thelightningpress.com

INFO1

SMARTBOOK

First Edition (INFO1)

Information Operations (IO Defined & Described)

Information in Joint Operations

Information Roles & Responsibilities

Info-Related Capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO)

Information Planning (IE Analysis, IPB, MDMP, JPP)

Information Preparation

Information Execution (IO Working Grp, Weighted Efforts, Enabling Actions)

Fires & Targeting

Information Assessment

IO

information OPERATIONS&CAPABILITIES

Guide to Information Operations & the IRCs

The Lightning Press

Norman M Wade

INFO1

SMARTBOOK

IO information OPERATIONS&CAPABILITIES

Guide to Information Operations & the IRCs

The Lightning Press

Norman M Wade

The Lightning Press

2227 Arrowhead Blvd.
Lakeland, FL 33813
24-hour Order/Voicemail: 1-800-997-8827
E-mail: SMARTbooks@TheLightningPress.com
www.TheLightningPress.com

(INFO1) The Information Operations & Capabilities SMARTbook

Guide to Information Operations & the IRCs

Over the past two decades, information operations (IO) has gone through a number of doctrinal evolutions, explained, in part, by the rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment. INFO1: The Information Operations & Capabilities SMARTbook examines the most current doctrinal references available and charts a path to emerging doctrine. INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

ISBN: 978-1-935886-60-0

Notice of Liability

The information in this SMARTbook and quick reference guide is distributed on an "As Is" basis, without warranty. While every precaution has been taken to ensure the reliability and accuracy of all data and contents, neither the author nor The Lightning Press shall have any liability to any person or entity with respect to liability, loss, or damage caused directly or indirectly by the contents of this book. If there is a discrepancy, refer to the source document. This SMARTbook does not contain classified or sensitive information restricted from public release. "The views presented in this publication are those of the author and do not necessarily represent the views of the Department of Defense or its components."

Credits: Cover image - Soldiers from A Co., 1st Bn, 111th Inf, 56th Stryker BCT conduct a night live-fire during Exercise Decisive Strike 2019 (U.S. Army photo by Staff Sgt. Frances Ariele Tejada). All other images courtesy Dept. of the Army and/or Dept. of Defense.

Printed and bound in the United States of America.

(INFO1) Notes to Reader

INFO1: The Information Operations & Capabilities SMARTbook

Over the past two decades, information operations (IO) has gone through a number of doctrinal evolutions, explained, in part, by the rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment. *INFO1: The Information Operations & Capabilities SMARTbook* examines the most current doctrinal references available, and charts a path to emerging doctrine on information operations.

Information is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. The **information element of combat powe**r is integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes.

Information Operations (IO) 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. The purpose of IO is to **create effects in and through the information environment** that provide commanders decisive advantage over enemies and adversaries.

The joint force commander (JFC) **leverages informational aspects of military activities to gain an advantage**; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes. The joint force **attacks and exploits information, information networks, and systems to affect the ability of relevant actors to leverage information** in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

An **information-related capability (IRC)** 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. IO brings together information-related capabilities (IRCs) at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander.

SMARTbooks - DIME is our DOMAIN!

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)! Recognized as a "whole of government" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive professional library.

SMARTbooks can be used as quick reference guides during actual operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training. Visit **www.TheLightningPress.com**!

INFO1: The Information Operations & Capabilities SMARTbook

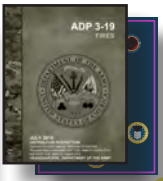
Over the past two decades, information operations (IO) has gone through a number of doctrinal evolutions, explained, in part, by the rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment. INFO1: The Information Operations & Capabilities SMARTbook examines the most current doctrinal references available and charts a path to emerging doctrine.

FM 3-13

ATP 3-13.1

JP 3-13 (Chg 1)

JP 3-0 (Chg 1)



Plus more than a dozen primary references on the IRCs and more!

INFO1 chapters and topics include information operations (IO defined and described), information in joint operations (joint IO), information-related capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution (IO working group, IO weighted efforts and enabling activities, intel support), fires & targeting, and information assessment.

Chap 1: Information Operations (Defined & Described)

Information is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. The **information element of combat powe**r is integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes.

Information Operations (IO) 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. The purpose of IO is to **create effects in and through the information environment** that provide commanders decisive advantage over enemies and adversaries.

Chap 2: Information in Joint Operations

The joint force commander (JFC) **leverages informational aspects of military activities to gain an advantage**; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes. The joint force **attacks and exploits information, information networks, and systems to affect the ability of relevant actors to leverage information** in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

Chap 3: Information-Related Capabilities (IRCs)

An **information-related capability (IRC)** 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. IO brings together information-related capabilities (IRCs) at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander.

All unit operations, activities, and actions affect the information environment. Even if they primarily affect the physical dimension, they nonetheless also affect the informational and cognitive dimensions. For this reason, whether or not they are routinely considered an IRC, a wide variety of unit functions and activities can be adapted for the purposes of conducting information operations or serve as enablers to its planning, execution, and assessment.

Chap 4: Information Planning

Planning is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. Commanders, supported by their staffs, ensure IO is fully integrated into the plan, starting with Army design methodology (ADM) and progressing through the military decisionmaking process (MDMP). The focal point for IO planning is the IO officer (or designated representative for IO). However, the entire staff contributes to planning products that describe and depict how IO supports the commander's intent and concept of operations.

Chap 5: Information Preparation

Preparation consists of those activities performed by units and Soldiers to improve their ability to execute an operation. Preparation creates conditions that improve friendly force opportunities for success. Because many IO objectives and IRC tasks require long lead times to create desired effects, preparation for IO often starts earlier than for other types of operations. Initial preparation for specific IRCs and IO units (such as 1st IO Command or a Theater IO Group) may begin during peacetime.

Chap 6: Information Execution

Execution of IO includes IRCs executing the synchronization plan and the commander and staff monitoring and assessing their activities relative to the plan and adjusting these efforts, as necessary. The primary mechanism for monitoring and assessing IRC activities is the **IO working group.** There are two variations of the IO working group. The first monitors and assesses ongoing planned operations and convenes on a routine, recurring basis. The second monitors and assesses unplanned or crisis situations and convenes on an as-needed basis.

Chap 7: Fires & Targeting

The **fires warfighting function** is the related tasks and systems that **create and converge effects in all domains** against the threat to enable actions across the range of military operations. These tasks and systems create **lethal and nonlethal effects** delivered from both Army and Joint forces, as well as other unified action partners.

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). IO is integrated into the targeting cycle to produce effects in and through the information environment that support objectives.

Chap 8: Information Assessment

Assessment precedes and guides the other activities of the operations process. It is also part of targeting. In short, assessment occurs at all levels and within all operations and has a role in any process or activity. The purpose of assessment is to improve the commander's decision making and make operations more effective. Assessment is a key component of the commander's decision cycle, helping to determine the results of unit actions in the context of overall mission objectives.

(INFO1) References

The following references were used in part to compile *INFO1: The Information Operations & Capabilities SMARTbook*. All military references used to compile SMARTbooks are in the public domain and are available to the general public through official public websites and designated as approved for public release with unlimited distribution. The SMARTbooks do not contain ITAR-controlled technical data, classified, or other sensitive material restricted from public release. SMARTbooks are reference books that address general military principles, fundamentals and concepts rather than technical data or equipment operating procedures.

Joint Publications

JP 3-0	Oct 2018	Joint Operations (w/Change 1)
JP 3-12	Jun 2019	Cyberspace Operations
JP 3-13	Nov 2014	Information Operations (w/Change 1)
JP 3-13.1	Feb 2012	Electronic Warfare
JP 3-13.2	Dec 2011	Military Information Support Operations (w/Change 2)
JP 3-13.3	Jan 2012	Operations Security
JP 3-14	Oct 2020	Space Operations
JP 3-57	Sep 2013	Civil-Military Operations
JP 3-61	Aug 2016	Public Affairs (w/Change 1)

Army Doctrine Publications (ADPs)

ADP 3-19	Jul 2019	Fires

Army Techniques Publications (ATPs)

ATP 3-13.1	Oct 2018	The Conduct of Information Operations
ATP 3-13.3	Jul 2019	Army Operations Security for Division and Below
ATP 3-60	May 2015	Targeting
ATP 3-36	Dec 2014	Electronic Warfare Techniques

Field Manuals (FMs)

FM 3-0	Dec 2017	Operations (w/Change 1)
FM 3-12	Apr 2017	Cyberspace and Electronic Warfare Operations
FM 3-13	Dec 2016	Information Operations
FM 3-14	Oct 2019	Space Operations
FM 3-61	Apr 2014	Public Affairs Operations
FM 6-0	Apr 2016	Commander and Staff Organization and Operations (w/Change 2)

Other Publications

PAM 525-3-1	Dec 2018	The U.S. Army in Multi-Domain Operations 2028
JDN 2-13	Dec 2013	Commander's Communication Synchronization

(INFO1) Table of Contents

Chap 1

Information Operations (IO)

Chap 2

Information in Joint Operations

Chap 3

Information-Related Capabilities (IRCs)

Chap 4 (Information Operations) PLANNING

Chap 5 (Information Operations) PREPARATION

Chap 6 (Information Operations) EXECUTION

Chap 7 Fires & Targeting

Chap 8 (Information Operations) ASSESSMENT

I. Information Operations (Defined & Described)

Ref: FM 3-13, Information Operations (Dec '16), pp. 1-2 to 1-6.

I. Information Operations (IO)

Information Operations (IO) 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).

FM 3-13 uses the term IO comprehensively to capture all activity employed to affect the information environment and contribute to operations in and through the information environment. IO includes:

- Integration and synchronization of information-related capabilities.
- Planning, preparing, execution, and assessment.
- The capability and capacity that ensures the accomplishment of IO, to include the units and personnel responsible for its conduct.

Breaking down the definition into constituent parts helps to understand its meaning and implications for land forces:

Information Operations (IO) is the...

Integrated Employment of Information-Related Capabilities (IRCs)...

IO brings together IRCs at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander. While IRCs create individual effects, IO stresses aggregate and synchronized effects as essential to achieving operational objectives.

See p. 1-5 (and chap. 3) for an overview and further discussion of the IRCs.

During Military Operations...

Army forces, as part of a joint force, conduct operations across the conflict continuum and range of military operations. Whether participating in security cooperation efforts or conducting major combat operations, IO is essential during all phases (0 through V) of a military operation.

In Concert with Other Lines of Operation...

Commanders use lines of operations and lines of effort to visualize and describe operations. A line of operations is a line that defines the directional orientation of a force in time and space in relation to the enemy and that links the force with its base of operations and objectives (ADRP 3-0). Lines of operations connect a series of decisive points that lead to control of a geographic or force-oriented objective. A line of effort is a line that links multiple tasks using the logic of purpose rather than geographical reference to focus efforts toward establishing operational and strategic conditions (ADRP 3-0). Lines of effort are essential to long-term planning when positional references to an enemy or adversary have little relevance. Commanders may describe an operation along lines of operations, lines of effort, or a combination of both. Commanders, supported by their staff, ensure information operations

are integrated into the concept of operation to support each line of operation and effort. Based on the situation, commanders may designate IO as a line of effort to synchronize actions and focus the force on creating desired effects in the information environment. Depending on the type of operation or the phase, commanders may designate an IO-focused line of effort as decisive.

To Influence, Disrupt, Corrupt, or Usurp...

IO seeks to create specific effects at a specific time and place. Predominantly, these effects occur in and through the information environment. Immediate effects (disrupt, corrupt, usurp) are possible in the information environment's physical and informational dimensions through the denial, degradation, or destruction of adversarial or enemy information-related capabilities. However, effects in the cognitive dimension (influence) take longer to manifest. It is these cognitive effects—as witnessed through changed behavior—that matter most to achieving decisive outcomes.

The Decision Making of Enemies and Adversaries...

While there are differences among the terms adversaries, threats, and enemies, all three refer to those individuals, organizations, or entities that oppose U.S. efforts. They therefore must be influenced in some fashion to acquiesce or surrender to or otherwise support U.S. national objectives by aligning their actions in concert with commanders' intent. [The joint phrasing "adversaries and potential adversaries" is revised to "enemies and adversaries" to better align with Army terminology.]

While Protecting Our Own...

Friendly commanders, like enemy and adversary leaders, depend on an array of systems, capabilities, information, networks, and decision aids to assist in their decision making. Gaining operational advantage in the information environment is equally about exploiting and protecting the systems, information, and people that speed and enhance friendly decision making, as it is about denying the same to the threat.

II. The Purpose of Information Operations

The purpose of IO is to **create effects in and through the information environment that provide commanders decisive advantage over enemies and adversaries.** Commanders achieve this advantage in several ways: preserve and facilitate decision making and the impact of decision making, while influencing, disrupting or degrading enemy or adversary decision making; get required information faster and with greater accuracy and clarity than the enemy or adversary; or influence the attitudes and behaviors of relevant audiences in the area of operations having an impact on operations and decision making.

To support achievement of these various ways, **IO employs and synchronizes IRCs** to affect the will, awareness, understanding, and capability of these audiences, while protecting our own. Will, awareness, understanding, and capability all contribute to and sustain decision making and, if compromised, can impair that decision making. In terms of will, awareness, understanding, and capability, advantage is achieved when commanders preserve their will to fight, as well as their situational understanding and their full capacity and ability to prosecute operations. Further, commanders achieve advantage when they preserve their freedom of action in the information environment while degrading enemy or adversary freedom of action.

See following pages (pp. 1-4 to 1-5) for an overview and further discussion.

Positions of Relative Advantage (Gaining the "Information Advantage")

Ref: FM 3-0 (w/Chg 1), Operations (Dec '17), pp. 1-18 to 1-19.

Gaining the "information advantage" to achieve "decision dominance" is an emerging doctrinal concept with regard to operations in the information environment. While not currently defined in joint or service doctrine, components of the concept are similar to those found in FM 3-0's discussion of "position of relative advantage":

See p. 7-7 (& 2-3) for related discussion of "leveraging information" from joint doctrine.

A **position of relative advantage** is a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage (ADRP 3-0). Positions of relative advantage **occur in all domains**, providing opportunities for units to exploit. Commanders maintain momentum through exploitation of opportunities to consolidate gains, and they continually assess and reassess friendly and enemy effects for future opportunities. A key aspect in achieving a position of advantage is maneuver, the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy (JP 3-0).

Positions of relative advantage are usually temporary and require initiative to exploit. While friendly forces are seeking positions of advantage, enemy forces are doing the same. There are multiple forms of positional advantage that provide opportunities to exploit. Some are considerations that should be understood when formulating tactical and operational concepts, while others are goals that can be worked towards as a means of destroying or defeating the enemy and achieving the overall purpose of the operation. Examples of positional advantage include—

- Physical and geographical (including strategic positioning, sanctuary, and control of key terrain)
- Combat power and warfighting function overmatch (including range, lethality, precision, and mass)
- **Relationships and influence** (including allies, interoperability, access, and indigenous forces)
- **Legitimacy, ideas, and popular perception** (including what is good versus bad, accepted versus opposed, and a believable narrative)
- Time (including speed of recognition, speed of decision making, speed of action, and operational tempo)
- Freedom of action (including secure lines of communications, standoff, depth, **access to cyberspace**, maritime and air enablers, and friendly A2 & AD measures)
- **Moral** (including alignment of words & deeds, just & unjust, international support)
- **Will** (including doing what must be done, continuing as long as it takes, and maintaining support from domestic leaders)

Relative positional advantage is something to gain, protect, and exploit across all domains. Combining positional advantages across multiple domains during each phase of operations provides opportunities for exploitation through maneuver. Physical or geographic positions of relative advantage are often identified first as decisive points and then depicted in operational graphics as objectives. The greater the number of positions of advantage a commander can generate, the increased number of dilemmas that commander can present to an enemy. The combination of positional advantages change over time relative to changes in the OE, and this change includes how the enemy reacts to friendly forces' activities. It is the exploitation of positions of advantage through maneuver which deters, defeats, or destroys an enemy.

II. Information (as an Element of Combat Power)

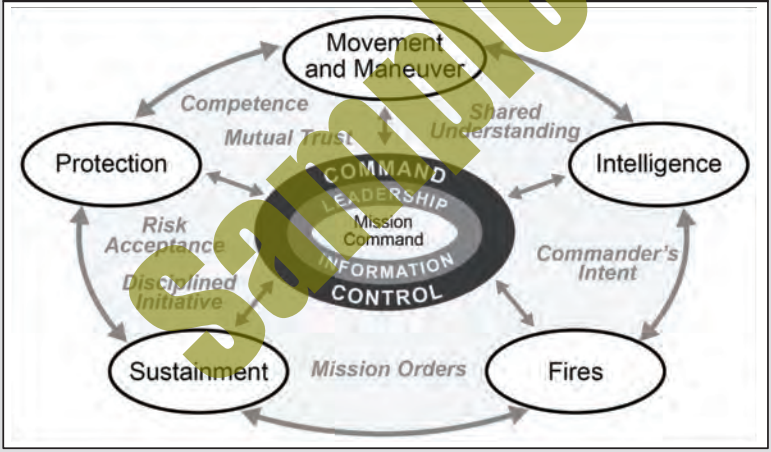
Ref: FM 3-13, Information Operations (Dec '16), pp. 1-7 to 1-8 and ADP 3-0, Operations (Jul '19), chap. 5.

Information is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. IO, along with knowledge management and information management, are the ways that units harness this resource and ensure its availability, as well as operationalize and optimize it.

The Information Element of Combat Power

The **information element of combat power i**s integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes. IO and the information element of combat power are related but not the same.

Elements of Combat Power



*Ref: ADP 3-0, Operations (Jul '19), fig. 5-1. The elements of combat power. Commanders apply combat power through the warfighting functions using leadership and **information**.*

Commanders apply leadership through **mission command**. Leadership is the multiplying and unifying element of combat power. An Army commander, by virtue of assumed role or assigned responsibility, inspires and influences people to accomplish organizational goals.

Information enables commanders at all levels to make informed decisions on how best to apply combat power.

IO, a component of the command and control* warfighting function, supports all other warfighting functions and makes each one more potent. The effects that IO achieves in the information environment amplify the effects of movement and maneuver, intelligence, fires, sustainment and protection, both constructive and destructive.

See pp. 2-1 to 2-6 for discussion of information (as one of the seven joint functions).

II. Information Operations and the Command & Control* Warfighting Function

Ref: FM 3-13, Information Operations, pp. 1-7 to 1-8.

The command and control warfighting function* enables commanders to balance the art of command and the science of control in order to integrate the other warfighting functions. It also enables a shared understanding of an operational environment and the commander's intent. IO's focus on protecting information, information systems, and decision making, enhances commanders' ability to integrate the other warfighting functions and create necessary shared understanding. At the same time, it seeks to degrade the enemy's decision-making ability.

IO supports the accomplishment of several mission command warfighting tasks, including inform and influence audiences inside and outside an organization, conduct knowledge management and information influencing are effects that occur in the cognitive dimension of the information environment. By effectively synchronizing IRCs and, when appropriate, conducting cyberspace electromagnetic activities, commanders tailor their influence and manner of informing to the situation and audience at hand. Information and knowledge management support the commander and staff's ability to access information quickly and completely, as well as segment and protect information, thereby enhancing their decision making and gaining advantage over adversaries and enemies.

Warfighting Function Tasks (FM 3-0*)

While staffs perform essential functions, commanders are ultimately responsible for accomplishing assigned missions. Throughout operations, commanders encourage disciplined initiative through a clear commander's intent while providing enough direction to integrate and synchronize the force at the decisive place and time. To this end, commanders perform three primary mission command warfighting function tasks. The commander tasks are—

- Drive the operations process through the activities of understanding, visualizing, describing, directing, leading, and assessing operations.
- Develop teams, both within their own organizations and with unified action partners.
- Inform and influence audiences, inside and outside their organizations.

Staffs support commanders in the exercise of mission command by performing four primary mission command warfighting function tasks. The staff tasks are—

- Conduct the operations process: plan, prepare, execute, and assess.
  (See following pages for specific discussion of IO and the operations process.)
- Conduct knowledge management, information management, and foreign disclosure.
- Conduct information operations.
- Conduct cyberspace electromagnetic activities.

Six additional tasks reside within the mission command warfighting function—

- Conduct CA operations.
- Conduct military deception.
- Install, operate, and maintain the DODIN.
- Conduct airspace control.
- Conduct information protection.
- Plan and conduct space activities.

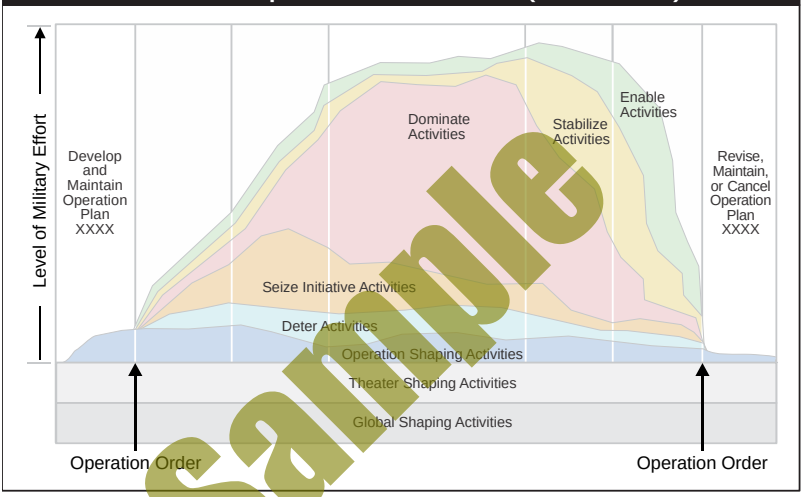
**Editor's Note: The "mission command" warfighting function tasks provided above are from FM 3-0 (w/Chg 1), Operations (Dec '17). The newer ADP 6-0, Mission Command (Jul '19) renamed and redefined the warfighting function formally called the "mission command warfighting function" as the "command and control warfighting function."*

III. IO & the Army Strategic Roles

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 7.

Army IO supports joint IO across the range of military operations and across all operational phases. In accordance with latest joint doctrine (JP 3-0 w/Chg 1, dated Oct '18), the joint operation model describes six general groups of activity as shown in figure V-4 as a convenient basis for thinking about a joint operation in notional phases.

Joint Combat Operation Model (Notional)



Ref: JP 3-0 (w/Chg 1), fig. V-4. A Notional Joint Combat Operation Model.

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.

U.S. Army Strategic Roles

Ref: FM 3-0 (Oct '17), fig. 1-4. Army strategic roles and their relationships to joint phases.

I. Shape

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.

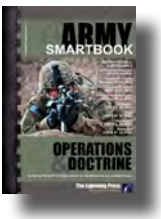
Although shaping operations are ongoing, they are specific to each theater and operational area in which they occur (although effects in one theater may well create effects or achieve objectives in another). The balance of defend, attack, and stabilize IO efforts varies based on the specific operational 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.

See following pages (pp. 1-20 to 1-21) for discussion of IO considerations for SHAPING.

II. Prevent

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.



Refer to AODS6-1 (w/SMARTupdate 1): The Army Operations & Doctrine SMARTbook (Guide to FM/ADP 3-0 Operations & the Elements of Combat Power), chap. 2 for complete discussion of the U.S. Army strategic roles from FM 3-0 (w/Chg 1). See pp. 2-37 to 2-42 for a description of Army forces, as part of a joint team, shape operational environments; pp. 2-43 to 2-60 discussion of prevent conflict; pp. 2-61 to 2-68 for discussion of large-scale ground combat; pp. 2-101 to 2-110 for discussion of consolidate gains; and p. 2-22 for discussion of paths to victory (win).

SHAPING Activities (IO Considerations)

Ref: FM 3-0 (w/Chg 1), Operations (Dec '17), chap. 3.

Operations to shape consist of various long-term military engagements, security cooperation, and deterrence missions, tasks, and actions intended to assure friends, build partner capacity and capability, and promote regional stability. Operations to shape typically occur in support of the geographic combatant commander's (GCC's) theater campaign plan (TCP) or the theater security cooperation plan. Ultimately, operations to shape focus on four purposes:

- Promoting and protecting U.S. national interests and influence.
- Building partner capacity and partnerships.
- Recognizing/countering adversary attempts to gain positions of relative advantage.
- Setting conditions to win future conflicts.

Army operations to shape align with military engagement and security cooperation activities. Army prevent activities align with deterrence and crisis response and limited contingency operations.

Optimally, shaping activities ensure regions remain stable, a crisis does not occur, and there is no need for an escalation of force. Upon activation of a joint operation order (OPORD) for a crisis or a limited contingency operation Army operations to shape occur simultaneously within a joint operations area (JOA) or designated theater of operations and across the GCC's area of responsibility (AOR). Shaping activities involving Army forces in support of the GCC to promote favorable access include—

- Key leader engagements.
- Bilateral and multinational exercises to improve multinational interoperability and operations.
- Missions to train, advise, and equip foreign forces.
- Negotiations to secure basing and transit rights, establish relationships, and formalize support agreements.
- The use of grants and contracts to improve relationships with and strengthen partner nations.
- Designing interoperability into acquisition programs.
- Electromagnetic spectrum (EMS) mapping of adversary capabilities.

Military engagement, security cooperation, and deterrence activities usually involve a combination of military forces and capabilities separate from, but integrated with, the efforts of interagency participants, and they are coordinated by ambassadors and country teams.

Military Engagement

Military engagement is the routine contact and interaction between individuals or elements of the Armed Forces of the United States and those of another nation's armed forces, or foreign and domestic civilian authorities or agencies to build trust and confidence, share information, coordinate mutual activities, and maintain influence (JP 3-0). Military engagement occurs as part of security cooperation, but it also extends to interaction with domestic civilian authorities. GCCs seek out partners and communicate with adversaries to discover areas of common interest and tension. This increases the knowledge base for subsequent decisions and resource allocation. Such military engagements can reduce tensions and may prevent conflict, or, if conflict is unavoidable, they may allow the U.S. to enter into it with greater access and stronger alliances or coalitions. Army forces support military engagement through key leader engagement and Soldier and leader engagement.

Security Cooperation

Security cooperation is all Department of Defense interactions with foreign security establishments to build security relationships that promote specific United States security interests, develop allied and partner nation military and security capabilities for self-defense and multinational operations, and provide United States forces with peacetime and contingency access to allied and partner nations (JP 3-20). These efforts may include Army forces participating in joint and multinational exercises and employing regionally aligned forces. Conducting security cooperation is one of the Army's primary stability tasks. Security cooperation is governed by various sections of Title 10, USC; Title 22, USC; and specific public laws addressing Department of Defense (DOD) interactions with other nations.

Commanders and staffs conduct security cooperation to develop allied and friendly military capabilities for self-defense and multinational operations, to improve information exchange and intelligence sharing, to provide U.S. forces with peacetime and contingency access, and to mitigate conditions that could lead to a crisis. Security cooperation activities include—

- Security assistance.
- Security force assistance (SFA).
- Foreign internal defense.
- Security sector reform.

Other Shaping Activities

As part of operations to shape, Army forces participate in and conduct numerous other activities in support of the combatant commander's TCP. These include developing intelligence, countering weapons of mass destruction (CWMD), providing support to humanitarian efforts, conducting information operations, and organizing and participating in combined training and exercises.

- **Intelligence**. Identifying threat capabilities, strengths, weaknesses, and intent accurately is critical to providing commanders the timely indications and warnings necessary to ensure operational success.
- **Countering Weapons of Mass Destruction.**
- **Humanitarian Efforts.** The United States Agency for International Development is the lead U.S. government agency, responsible to the Secretary of State, for administering civilian foreign aid and providing humanitarian assistance and disaster relief. The United States Agency for International Development often works in concert with Army forces when Soldiers are tasked to provide assistance.
- **Information Operations.** The primary stability mechanisms Army units employ during operations to shape are influence and support. By influencing regional perceptions and improving the ability of partner nations to secure themselves through unilateral security partnerships and regional alliances, Army forces can isolate adversaries and thwart behavior that runs counter to U.S. interests.
- **Combined Training and Exercises**. Combined training and exercises with multinational partners play a key role in shaping an OE. Through training and exercises, Army forces build partner combat readiness and set conditions for future operations.

Refer to TAA2: Military Engagement, Security Cooperation & Stability SMARTbook (Foreign Train, Advise, & Assist) for further discussion. Topics include the Range of Military Operations (JP 3-0), Security Cooperation & Security Assistance (Train, Advise, & Assist), Stability Operations (ADRP 3-07), Peace Operations (JP 3-07.3), Counterinsurgency Operations (JP & FM 3-24), Civil-Military Operations (JP 3-57), Multinational Operations (JP 3-16), Interorganizational Cooperation (JP 3-08), and more.

IV. IO Across the Range of Military Operations

Ref: FM 3-13, Information Operations (Dec '16), pp. 1-5 to 1-7 and JP 3-0 (w/Chg 1), Joint Operations (Oct '18), chap. V.

Army forces conduct IO within joint force parameters. From peace to war, and across the range of military operations, commanders integrate and synchronize IO to focus combat power and gain advantage in the information environment. In all situations, Army forces do not act in isolation. Army forces conduct operations in support of a larger joint or multinational plan. Figure V-2 from JP 3-0 depicts the three main categories of military operations within the range of military operations construct:

See pp. 1-17 to 1-26 for related discussion of IO and the Army strategic roles.

Ref: JP 3-0 (w/Chg 1), fig. V-2. Notional Operations Across the Conflict Continuum.

A. Military Engagement, Security Cooperation, and Deterrence

Military engagement, security cooperation, and deterrence operations are ongoing and recurring military activities that establish, shape, maintain, and refine relations with other nations and domestic civil authorities. The general objective is to protect U.S. interests at home and abroad. IO contributes significantly to military engagement, security cooperation, and deterrence. Military engagement and security cooperation depend heavily on influencing partners and potential partners to align with U.S. interests and, thereby, prevent threats from achieving objectives in or through these same partners and the countries and regions they inhabit. Military engagement and security cooperation are themselves forms of deterrence, but other forms are possible. Deterrence is not only the actual capacity to harm another state or non-state entity who fails to comply with or accommodate U.S. demands, but also the perception of that entity that the U.S. has the ability to do harm, if provoked. IO provides essential support to the shaping and maintaining of this perception through, among other things, the protection of friendly information (OPSEC).

Complementing IO support to military engagement, security cooperation, and deterrence, as well as crisis response, contingency operations and major operations and campaigns is the Attack the Network framework. This framework consists of activities that employ lethal and nonlethal means to support friendly networks, influence neutral

V. IO Roles, Responsibilities, & Organizations

Ref: FM 3-13, Information Operations, chap. 3.

Every member of a unit—from the commander, to the staff, to the IO officer or representative, to individual Soldiers and Army civilians—contributes to IO. Also essential to mission success are the IRCs supporting the unit's IO efforts, as well as any augmenting IO units. Each has a specific role and important responsibilities to fulfill or undertake, as well as vital relationships to forge and sustain, in order to achieve advantage in and through the information environment.

I. The Commander

Commanders, at all levels, are responsible for knowing what threats their units face and how to exploit or defeat them. They are their unit's chief influencers and engage relevant audiences and actors, as necessary, to shape the information environment to their advantage. Commanders rely on their staff and IO officer, in particular, to assist in planning, preparing, executing, and assessing IO. They also personally direct and review analysis of the information environment, issue guidance on the employment and synchronization of IRCs, and direct adjustments based on assessment results.

Cognizant of the pervasive impact of the information environment on operations and the need to affect this environment to their advantage, commanders are mindful of the following:

- Every operation has, to some degree, an effect on the information environment.
- IO planning is integral to operations from the start.
- Effects in and through the information environment, if essential to success, are part of the commander's intent.
- Combat power cannot be optimized without IO.
- The warfighting functions (particularly movement and maneuver and fires) produce effects in the information environment, whether intentional or not.
- IO is essential to operational success at all levels, whether or not the unit has an assigned IO officer.
- All communication can quickly become global and have strategic consequences.
- IRCs can have lengthy lead times to coordinate and employ, as well as lengthy lag times before their effects are realized.
- The alignment of words, deeds, and images is essential to building trust and confidence with relevant audiences in the area of operations.
- IO requires prioritized intelligence support.
- Effects in the information environment are not always caused as expected; assessment is difficult and benefits from commanders' interest, prioritization and support.
- U.S. IO can be constrained by policy and law, while the threat is often unconstrained in its use of information.

II. The Staff

Ref: FM 3-13, Information Operations (Dec '16), pp. 3-1 to 3-4.

Each staff section collaborates routinely, but to varying degrees, with the IO officer to plan, synchronize, support, and assess IO. Representatives from the G-2 (S-2), G-3 (S-3), assistant chief of staff, plans G-5 (S-5), assistant chief of staff, signal G-6 (S-6) and assistant chief of staff, civil affairs operations (G-9/S-9), in particular, serve as core members of the IO working group.

ASSISTANT CHIEF OF STAFF, G-1 (S-1), PERSONNEL

The G-1 (S-1) is the principal staff officer for personnel functions. The G-1 (S-1) processes requirements for individual, team and unit augmentation or attachment. It coordinates reception of these individuals, teams, or units and validates their requirements. It also builds manning documents, as required. Additional IO-related responsibilities include, but are not limited to:

- Designating a representative to the IO working group.
- Providing IO-focused instructions in the personnel appendix of the sustainment annex.
- Reviewing the IO mission and mission, enemy, terrain and weather, troops and support available,time available, and civil considerations from a personnel support perspective.

ASSISTANT CHIEF OF STAFF, G-2 (S-2), INTELLIGENCE

The G-2 (S-2) is the principal staff officer for all matters concerning military intelligence, security operations, and military intelligence training. The G-2 (S-2) produces the intelligence used by the IO officer, element, working group and IRCs. IO-related responsibilities of the G-2 (S-2) include, but are not limited to:

- Participating as a core member of the IO working group and providing intelligence briefings or updates.
- Providing IO-focused instructions in the intelligence annex.
- Including requests for information from the IO officer in intelligence reach.
- Answering information requirements (IRs) submitted by the IO officer.
- Coordinating with counterintelligence; law enforcement; and information system developers, providers, administrators, and users to ensure timely sharing of relevant information.
- Preparing a threat assessment of enemy command and control systems, including:
  - Political, economic, social, and cultural influences.
  - Targets and methods for offensive operations.
  - Enemy decision-making processes.
  - Biographical backgrounds of key threat leaders, decision makers, and communicators, and their advisors. Including motivating factors and leadership styles.
  - A comprehensive comparison of enemy offensive information capabilities against friendly IO vulnerabilities.
- Collecting data to establish an electronic warfare database and command and control target list.
- Providing intelligence support to military deception operations; specifically:
  - Helping the G-6 (S-6) plan use of friendly information systems as deception means.
  - Establishing counterintelligence measures to protect the military deception operation from detection.

ASSISTANT CHIEF OF STAFF, G-3 (S-3), OPERATIONS

The G-3 (S-3) is the principal staff officer for all matters concerning training and leader development, operations and plans, and force development modernization. IO-related responsibilities include, but are not limited to:

- Exercising primary responsibility for IO staff functions and overseeing the IO officer, who is part of the movement and maneuver cell.
- With assistance from the IO officer, integrating IO planning into the military decisionmaking process.
- Validating or approving, as necessary, IO officer inputs, actions and outputs. Among the inputs and outputs, the mission statement, scheme of IO, and IO objectives require G-3 (S-3) review,refinement, and emphasis.
- If additional IRCs or IO units are required, prioritizing and facilitating the augmentation requestor request for forces.
- Tasking units and assets necessary to achieve IO objectives.

III. The IO Officer

The IO officer (who heads the IO element at division and higher) or representative (at brigade and below) is the staff focal point for IO. The IO officer is responsible for the following specific tasks, among others:

- Analyzing the information environment to discern impacts it will have on unit operations and to exploit opportunities to gain an advantage over threat forces.
- Identifying the most effective IRCs to achieve objectives.
- Synchronizing IRCs to achieve objectives in the information environment.
- Assessing the risk, typically described as risk to mission and risk to force, associated with the employment of any capability, product, program or message.
- Providing input to the synchronization matrix for the use of available IRCs in support of unit operations.
- Identifying IRC gaps not resolvable at the unit level.
- Coordinating with other Army, Service, or joint forces to use IRCs to augment existing unit capability shortfalls.
- Providing information as required in support of operations security (OPSEC) at the unit level.
- Providing information as required in support of military deception at the unit level.
- Leading the IO working group.
- Assessing the effectiveness of employed IRCs.

The IO officer contributes to the overall intelligence preparation of the battlefield (IPB) by assisting the G-2 (S-2) in identifying and evaluating threat information capabilities, as well as the means to influence the population. Additionally, the IO officer submits to the G-2 (S-2) any IRs regarding intelligence shortfalls about the information environment and coordinates with the G-2 (S-2) in developing templates, databases, and other relevant products, including but not limited to:

- Religion, language, and culture of key groups and decision makers.
- Agendas of nongovernmental organizations.
- Size and location of threat IO or information warfare forces and assets.
- Military and civilian communication infrastructures and connectivity.
- Population demographics, linkages, and related information.
- Audio, video, and print media outlets and centers and the populations they service.
- Location and types of electromagnetic systems and emitters.
- Network vulnerabilities of friendly, neutral, and threat forces.

Additional tasks for which the IO officer is responsible include, but are not limited to:

- Participating in the military decisionmaking process.
- Developing IRs.
- Producing information and combined information overlays.
- Developing the scheme of IO.
- Through commander's communication synchronization, contribute to development of the commander's narrative.
- Integrating IO into the unit's targeting process.
- Deconflicting the employment of IRCs.
- Ensuring IO-related information is updated in the common operational picture.
- Integrating external augmentation.

I. Information in Joint Operations

Ref: JP 3-0 (w/Chg 1), Joint Operations (Oct '18), chap. III.

I. Information (as a Joint Function)

All military activities produce **information**. Informational aspects are the features and details of military activities observers interpret and use to assign meaning and gain understanding. Those aspects affect the perceptions and attitudes that drive behavior and decision making. The JFC leverages informational aspects of military activities to gain an advantage; failing to leverage those aspects may cede this advantage to others. Leveraging the informational aspects of military activities ultimately affects strategic outcomes.

The **information function** encompasses the management and application of information and its deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired behaviors and to support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of military activities to achieve the commander's objectives and attain the end state.

See p. 2-6 for discussion of information as related to the seven joint functions.

The **instruments of national power** (diplomatic, informational, military, and economic) provide leaders in the US with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments.

Regardless of its mission, the joint force considers the likely impact of all operations on **relevant actor** perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that create desired effects that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the employment of specialized capabilities -- e.g., **information-related capabilities (IRCs)** -- to reinforce the JFC's efforts.

Inform activities involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda. Inform activities help to assure the trust and confidence of the US population, allies, and partners and to deter and dissuade adversaries and enemies.

The joint force **attacks and exploits information, information networks, and systems** to affect the ability of relevant actors to leverage information in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

II. Information Function Activities

Ref: JP 3-0 (w/Chg 1), Joint Operations (Oct '18), pp. III-17 to III-22.

The information function includes activities that facilitate the JFC's understanding of the role of information in the OE, facilitate the JFC's ability to leverage information to affect behavior, and support human and automated decision making.

A. Understand Information in the Operational Environment (OE)

In conjunction with activities under the intelligence joint function, this activity facilitates the JFC's understanding of the pervasive nature of information in the OE, its impact on relevant actors, and its effect on military operations. It includes determining relevant actor perceptions, attitudes, and decision-making processes and requires an appreciation of their culture, history, and narratives, as well as knowledge of the means, context, and established patterns of their communication.

Information affects the perceptions and attitudes that drive the behavior and decision making of humans and automated systems. In order to affect behavior, the JFC must understand the perceptions, attitudes, and decision-making processes of humans and automated systems. These processes reflect the aggregate of social, cultural, and technical attributes that act upon and impact knowledge, understanding, beliefs, world views, and actions.

The human and automated systems whose behavior the JFC wants to affect are referred to as relevant actors. Relevant actors may include any individuals, groups, and populations, or any automated systems, the behavior of which has the potential to substantially help or hinder the success of a particular campaign, operation, or tactical action. For the purpose of military activities intended to inform audiences, relevant actors may include US audiences; however, US audiences are not considered targets for influence.

See pp. 1-6 to 1-7 for related discussion of the operational environment (OE).

Language, Regional, and Cultural Expertise

Language skills, regional knowledge, and cultural awareness enable effective joint operations. Deployed joint forces should understand and effectively communicate with HN populations; local and national government officials; multinational partners; national, regional, and international media; and other key stakeholders, including NGOs. This capability includes knowledge about the human aspects of the OE and the skills associated with communicating with foreign audiences. Knowledge about the human aspects of the OE is derived from the analysis of national, regional, and local culture, economy, politics, religion, and customs. Consequently, commanders should integrate training and capabilities for foreign language and regional expertise in contingency, campaign, and supporting plans and provide for them in support of daily operations and activities. Commanders should place particular emphasis on foreign language proficiency in technical areas identified as key to mission accomplishment.

For specific planning guidance and procedures regarding language and regional expertise, refer to CJCSI 3126.01, Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning, and Sourcing.

B. Leverage Information to Affect Behavior

Tasks aligned under this activity apply the JFC's understanding of the impact information has on perceptions, attitudes, and decision-making processes to affect the behaviors of relevant actors in ways favorable to joint force objectives.

Influence Relevant Actors

Regardless of its mission, the joint force considers the likely impact of all operations on relevant actor perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that create desired effects that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the employment of specialized capabilities (e.g., KLE, CO, military information support operations [MISO], EW, CA) to reinforce the JFC's efforts. Since some relevant actors will be located outside of the JFC's OA, coordination, planning, and synchronization of activities with other commands or mission partners is vital.

Inform Domestic, International, and Internal Audiences

Inform activities involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda. Inform activities help to assure the trust and confidence of the US population, allies, and partners and to deter and dissuade adversaries and enemies.

Attack & Exploit Information, Information Networks, & Systems

The joint force attacks and exploits information, information networks, and systems to affect the ability of relevant actors to leverage information in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

C. Support Human & Automated Decision Making

The management aspect of the information joint function includes activities that facilitate shared understanding across the joint force and that protect friendly information, information networks, and systems to ensure the availability of timely, accurate, and relevant information necessary for JFC decision making.

Facilitating Shared Understanding

Facilitating shared understanding is related to building shared understanding in the C2 joint function. Where building shared understanding is an element of C2 and focuses on purpose (i.e., the commander's objective), facilitating shared understanding is concerned with process (i.e., the methods). Key components of facilitating understanding are collaboration, KS, and IM.

Protecting Friendly Information

Information Networks, and Systems. The information function reinforces the protection function and focuses on protecting friendly information, information networks, and systems. This aspect of the information function includes the preservation of friendly information across the staff and the joint force and any information shared with allies and partners. These activities reinforce the requirement to assure the flow of information important to the joint force, both by protecting the information and by assessing and mitigating risks to that information. The preservation of information includes both passive and active measures to prevent and mitigate adversary collection, manipulation, and destruction of friendly information, to include attempts to undermine the credibility of friendly information.

II. Joint Information Operations (JP 3-13)

Ref: JP 3-13 w/change 1, Information Operations (Nov '14), chap. I & exec. summary.

The instruments of national power (diplomatic, informational, military, and economic) provide leaders in the US with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use **information-related capabilities (IRCs)** to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. As the strategic environment continues to change, so does **information operations (IO).**

Based on these changes, the Secretary of Defense now characterizes **IO as the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.**

Joint force commanders (JFCs) may establish an IO staff to provide command-level oversight and collaborate with all staff directorates and supporting organizations on all aspects of IO. Most combatant commands (CCMDs) include an IO staff to serve as the focal point for IO. Faced with an ongoing or emerging crisis within a geographic combatant commander's (GCC's) area of responsibility, a JFC can establish an IO cell to provide additional expertise and coordination across the staff and interagency.

IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process. These include: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations (CO), information assurance, space operations, military information support operations (MISO), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement.

The Information and Influence Relational Framework and the Application of Information-Related Capabilities (IRCs)

IRCs are the tools, techniques, or activities that affect any of the three dimensions of the information environment. The joint force (means) employs IRCs (ways) to affect the information provided to or disseminated from the target audience (TA) in the physical and informational dimensions of the information environment to affect decision making.

The change in the TA conditions, capabilities, situational awareness, and in some cases, the inability to make and share timely and informed decisions, contributes to the desired end state. Actions or inactions in the physical dimension can be assessed for future operations. The employment of IRCs is complemented by a set of capabilities such as operations security (OPSEC), information assurance (IA), counterdeception, physical security, electronic warfare (EW) support, and electronic protection. These capabilities are critical to enabling and protecting the JFC's C2 of forces.

The relational framework describes the application, integration, and synchronization of IRCs to influence, disrupt, corrupt, or usurp the decision making of TAs to create a desired effect to support achievement of an objective.

See following pages for further discussion of the relational framework and the IRCs.

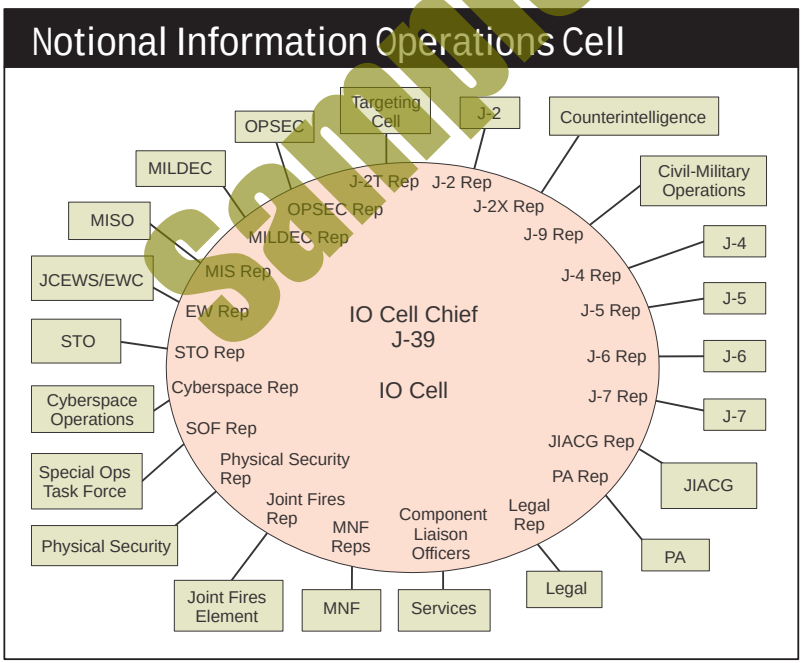
III. Integrating / Coordinating Functions of IO

Ref: JP 3-13 w/change 1, Information Operations (Nov '14), chap. II.

This section addresses how the integrating and coordinating functions of IO help achieve a JFC's objectives. Through the integrated application of IRCs, the relationships that exist between IO and the various IRCs should be understood in order to achieve an objective.

1. Information Operations and the Information-Influence Relational Framework

Influence is at the heart of diplomacy and military operations, with integration of IRCs providing a powerful means for influence. The relational framework describes the application, integration, and synchronization of IRCs to influence, disrupt, corrupt, or usurp the decision making of TAs to create a desired effect to support achievement of an objective. Using this description, the following example illustrates how IRCs can be employed to create a specific effect against an adversary or potential adversary.



Ref: JP 3-13 (with change 1), Information Operations, fig. II-3, p. II-6.

III. IO Phasing and Synchronization

Ref: JP 3-13 w/change 1, Information Operations (Nov '14), fig. IV-1, p. IV-3.

Through its contributions to the GCC's TCP, it is clear that joint IO is expected to play a major role in all phases of joint operations. This means that the GCC's IO staff and IO cell must account for logical transitions from phase to phase, as joint IO moves from the main effort to a supporting effort.

Shape

Joint IO planning should focus on supporting the TCP to deter adversaries and potential adversaries from posing significant threats to US objectives. Joint IO planners should access the JIACG through the IO cell or staff. Joint IO planning during this phase will need to prioritize and integrate efforts and resources to support activities throughout the interagency. Due to competing resources and the potential lack of available IRCs, executing joint IO during phase 0 can be challenging. For this reason, the IO staff and IO cell will need to consider how their IO activities fit in as part of a whole-of-government approach to effectively shape the information environment to achieve the CCDR's information objectives.

Deter

During this phase, joint IO is often the main effort for the CCMD. Planning will likely emphasize the JFC's flexible deterrent options (FDOs), complementing US public diplomacy efforts, in order to influence a potential foreign adversary decision maker to make decisions favorable to US goals and objectives. Joint IO planning for this phase is especially complicated because the FDO typically must have a chance to work, while still allowing for a smooth transition to phase II and more intense levels of conflict, if it does not. Because the transition from phase I to phase II may not allow enough time for application of IRCs to create the desired effects on an adversary or potential adversary, the phase change may be abrupt.

Seize Initiative

In phase II, joint IO is supporting multiple lines of operation. Joint IO planning during phase II should focus on maximizing synchronized IRC effects to support the JFC's objectives and the component missions while preparing the transition to the next phase.

Dominate

Joint IO can be a supporting and/or a supported line of operation during phase III. Joint IO planning during phase III will involve developing an information advantage across multiple lines of operation to execute the mission.

Stabilize

CMO, or even IO, is likely the supported line of operation during phase IV. Joint IO planning during this phase will need to be flexible enough to simultaneously support CMO and combat operations. As the US military and interagency information activity capacity matures and eventually slows, the JFC should assist the host-nation security forces and government information capacity to resume and expand, as necessary. As host nation information capacity improves, the JFC should be able to refocus joint IO efforts to other mission areas. Expanding host-nation capacity through military and interagency efforts will help foster success in the next phase.

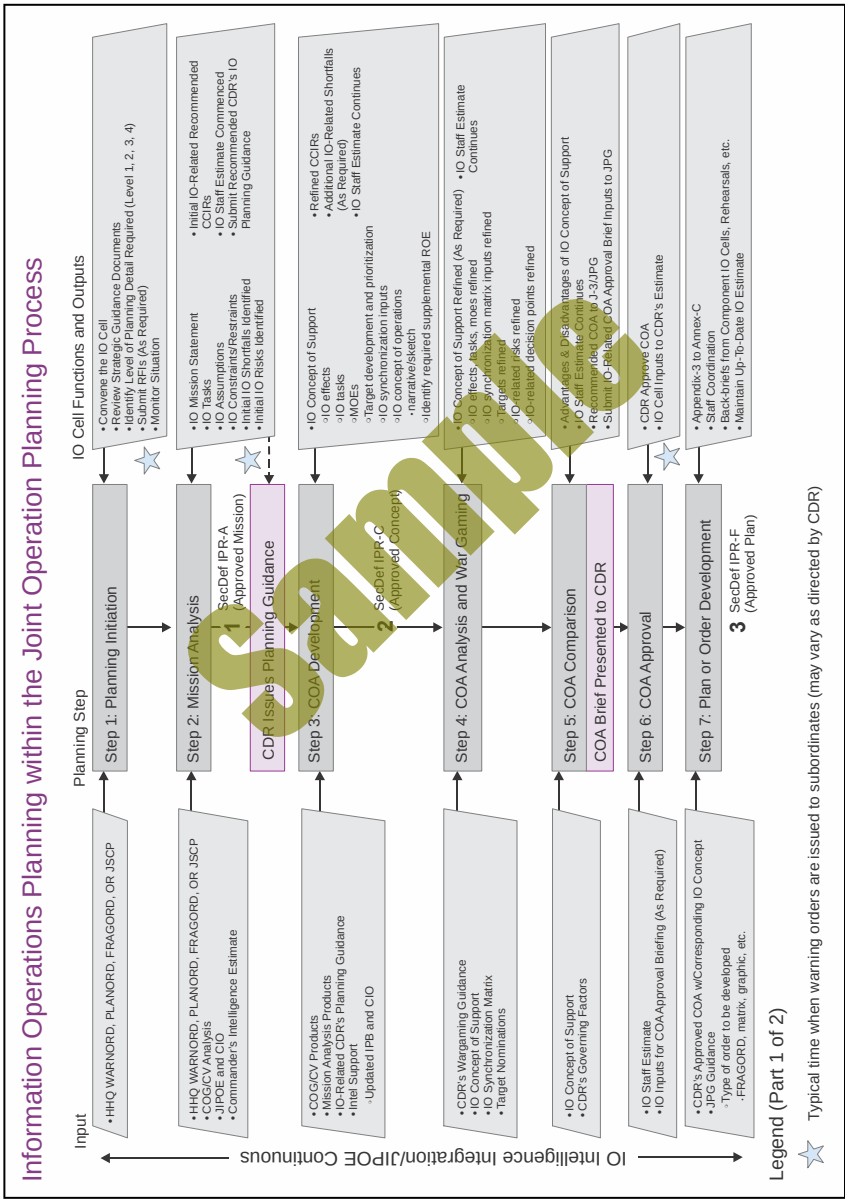
Enable Civil Authority

During this phase, joint IO planning focuses on supporting the redeployment of US forces, as well as providing continued support to stability operations. IO planning during phase V should account for interagency and country team efforts to resume the lead mission for information within the host nation territory. The IO staff and cell can anticipate the possibility of long term US commercial and government support to the former adversary's economic and political interests to continue through the completion of this phase.

Information Operations Planning (Within the Seven Steps of the JPP*)

Ref: JP 3-13 w/change 1, Information Operations (Nov '14), fig. IV-1, p. IV-3.

Throughout JOPP, IRCs are integrated with the JFC's overall CONOPS (see Figure IV-1). An overview of the seven steps of JOPP follows:



Step 1 - Planning Initiation

Integration of IRCs into joint operations should begin at step 1, planning initiation. Key IO staff actions during this step include the following:

a. Review key strategic documents

b. Monitor the situation, receive initial planning guidance, and review staff estimates from applicable operation plans (OPLANs) and concept plans (CONPLANs).

c. Alert subordinate and supporting commanders of potential tasking with regard to IO planning support.

d. Gauge initial scope of IO required for the operation.

e. Identify location, standard operating procedures, and battle rhythm of other staff organizations that require integration and divide coordination responsibilities among the IO staff.

f. Identify and request appropriate authorities.

g. Begin identifying information required for mission analysis and course of action (COA) development.

h. Identify IO planning support requirements (including staff augmentation, support products, and services) and issue requests for support according to procedures established locally and by various supporting organizations.

i. Validate, initiate, and revise PIRs and RFIs, keeping in mind the long lead times associated with satisfying IO requirements.

j. Provide IO input and recommendations to COAs, and provide resolutions to conflicts that exist with other plans or lines of operation.

k. In coordination with the targeting cell, submit potential candidate targets to JFC or component joint targeting coordination board (JTCB). For vetting, validation, and deconfliction follow local targeting cell procedures because these three separate processes do not always occur at the JTCB. Integrating Information-Related Capabilities Into the Joint Operation Planning Process

l. Ensure IO staff and IO cell members participate in all JFC or component planning and targeting sessions and JTCBs.

Step 2 - Mission Analysis

The purpose of step 2, mission analysis, is to understand the problem and purpose of an operation and issue the appropriate guidance to drive the remaining steps of the planning process. The end state of mission analysis is a clearly defined mission and thorough staff assessment of the joint operation. Mission analysis orients the JFC and staff on the problem and develops a common understanding, before moving forward in the planning process. During mission analysis, all staff sections, including the IO cell, will examine the mission from their own functional perspective and contribute the results of that analysis to the JPG. As IO impacts each element of the operational environment, it is important for the IO staff and IO cell during mission analysis to remain focused on the information environment. Key IO staff actions during mission analysis are:

a. Assist the J-3 and J-2 in the identification of friendly and adversary center(s) of gravity and critical factors (e.g., critical capabilities, critical requirements, and critical vulnerabilities).

b. Identify relevant aspects of the physical, informational, and cognitive dimensions (whether friendly, neutral, adversary, or potential adversary) of the information environment.

c. Identify specified, implied, and essential tasks.

d. Identify facts, assumptions, constraints, and restraints affecting IO planning.

Continued on next page

Continued on next page

Information-Related Capabilities (IRCs)

Ref: FM 3-13, Information Operations (Dec '16), pp. 1-2 to 1-6 and ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 3.

IO brings together information-related capabilities (IRCs) at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander. While IRCs create individual effects, IO stresses aggregate and synchronized effects as essential to achieving operational objectives.

An **information-related capability (IRC)** 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 1-02). The formal definition of IRCs encourages commanders and staffs to employ all available resources when seeking to affect the information environment to operational advantage. For example, if artillery fires are employed to destroy communications infrastructure that enables enemy decision making, then artillery is an IRC in this instance. In daily practice, however, the term IRC tends to refer to those tools, techniques, or activities that are inherently information-based or primarily focused on affecting the information environment.

IRC's include—

- Public affairs
- Civil affairs operations
- Military deception
- Military information support operations (MISO)
- Operations security (OPSEC)
- Cyberspace electromagnetic activities
- Electronic warfare
- Cyberspace operations
- Space operations
- Soldier and leader engagement (SLE), to include police engagement
- Combat camera
- Special technical operations

All unit operations, activities, and actions affect the information environment. Even if they primarily affect the physical dimension, they nonetheless also affect the informational and cognitive dimensions. For this reason, whether or not they are routinely considered an IRC, a wide variety of unit functions and activities can be adapted for the purposes of conducting information operations or serve as enablers to its planning, execution, and assessment. Some of these include, but are not limited to:

- Commander's communications strategy or communication synchronization.
- Presence, profile, and posture
- Foreign disclosure
- Physical security
- Physical maneuver
- Special access programs
- Civil military operations
- Intelligence
- Destruction and lethal actions

II. Overview of IRCs (INFO1 SMARTbook)

The INFO1 SMARTbook discusses the following IRCs in greater detail:

Public Affairs *See pp. 3-5 to 3-16.*
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.

Civil Affairs & Civil-Military Operations *See pp. 3-17 to 3-26.*
Civil affairs operations encompass actions planned, executed, and assessed by civil affairs forces. 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.

Military Deception (MILDEC) *See pp. 3-27 to 3-32.*
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.

Military Information Support Operations (MISO) *See p. 3-33.*
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).

Operations Security (OPSEC) *See pp. 3-39 to 3-44.*
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).

Cyberspace Electromagnetic Activities (CEMA) *See p. 3-45.*
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 Operations (CO) *See pp. 3-47 to 3-54.*
Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0).

Electronic Warfare (EW) *See pp. 3-55 to 3-60.*
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).

Space Operations *See pp. 3-61 to 3-70.*
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.

Additional IRCs *See pp. 3-71 to 3-74.*
Additional IRCs discussed include integrated joint special technical operations (IJSTO); special access programs (SAP); personnel recovery (PR); physical attack; physical security; presence, profile, and posture (PPP); soldier and leader engagement (SLE); police engagement; and social media.

I. Public Affairs (PA)

Ref: JP 3-61 (w/Chg 1), Public Affairs (Aug '16) and FM 3-61, Public Affairs Operations (Apr '14).

Public affairs (PA) doctrine and principles apply across the range of military operations. PA is a command responsibility and should not be delegated or subordinated to any other staff function below the command group. The public should perceive information communicated by PA as accurate.

Public Affairs Guidance (PAG)

Public affairs guidance (PAG) supports the public discussion of defense issues and operations and serves as a source document when responding to media representatives and the public. PAG also outlines planning guidance for related public affairs responsibilities, functions, activities, and resources. The development and timely dissemination of PAG ensures that all information is in consonance with policy when responding to the information demands of joint operations. PAG also conforms to operations security and the privacy requirements of the members of the joint forces.

The US military has an obligation to communicate with its members and the US public, and it is in the national interest to communicate with international publics. The proactive release of accurate information to domestic and international audiences puts joint operations in context, facilitates informed perceptions about military operations, undermines adversarial propaganda, and helps achieve national, strategic, and operational objectives.

Over the past two decades, there have been dramatic changes in the information environment. Notably, traditional media is no longer the only voice influencing key publics. The abundance of information sources, coupled with technology such as smart phones, digital cameras, video chat, and social media enterprises, allows information to move instantaneously around the globe. As such, it is imperative for PA personnel to rapidly develop themes and messages to ensure that facts, data, events, and utterances are put in context. Coordination and synchronization of themes and messages take place to ensure unity of effort throughout the information environment.

These tools provide the US military the ability to reach various audiences without mass media, as well as create the opportunity to join the conversation (as opposed to simply delivering a message) with an audience. Two-way conversation permits greater transparency and clarity. Joint operations will be supported by tailored communication that addresses friendly, neutral, and adversarial audiences. Often, these audiences want to both listen to and be heard by US forces. PA personnel will focus their communication efforts to a given public or publics. The speed of modern communications and the disparity of multiple audiences increase the importance of quickly and agilely synchronizing communication.

The First Amendment guarantees freedom of the press, but within the Department of Defense (DOD) this right must be balanced against the military mission that requires operations security (OPSEC) at all levels of command to protect the lives of US or multinational forces and the security of ongoing or future operations. These competing goals sometimes lead to friction between the media and the military. The Privacy Act of 1974 prevents the release of certain personal information to the media, but

does not forbid individuals from releasing information about themselves in social media. In addition, stringent restrictions exist for protecting personally identifiable information, and there are strict reporting requirements if personally identifiable information is released, even inadvertently.

The tempo of military operations, OPSEC concerns, and the number and variety of other information sources competing for the attention of the populace complicate the joint force commanders' (JFCs') ability to provide information to diverse publics at the same pace as the media and other sources. The ability of anyone with Internet access to share information and provide graphic visuals without validating facts as an event unfolds further complicates the military's effort to accurately inform the media and populace. JFCs and public affairs officers (PAOs) should evaluate missions to identify public information and visual information (VI) requirements, as well as the means to acquire and move those products in a timely manner. PA planning should include considerations to reduce the time lag between an event and when information about it, if any, can be shared.

The public can get information about the military and its operations from official DOD and unofficial sources (e.g., information disseminated by Service members, distributed by the public, the media, or by groups hostile to US interests). Regardless of the source, intention, or method of distribution, information in the public domain either contributes to or undermines the achievement of operational objectives. Official information can help create, strengthen, or preserve conditions favorable for the advancement of national interests and policies and mitigate any adverse effects from unofficial, misinformed, or hostile sources.

PA is a command responsibility. Official communication with US and international audiences will have a significant impact on the operational environment (OE). Effective PA is a key enabler for the commander to build and maintain essential relationships.

Public support for the US military's presence or operations is likely to vary. The PAO, in conjunction with others on the staff, must be able to quickly and accurately assess the information environment to provide valuable guidance and courses of action (COAs) to the commander. Such assessments enable the commander to better inform relevant audiences about ongoing operations and engender their support.

I. Public Affairs and the Operational Environment (OE)

Information in the public domain affects the OE and influences operations. Commanders should carefully evaluate how various friendly, enemy, adversary, and neutral actions, images, and words impact planned and ongoing operations. PA understands that various audiences have differing information needs and works closely with other information providers to ensure consistency of messaging and accuracy of content. By conveying the facts about joint force activities in a proactive manner, PA helps the JFC to impact the information environment, particularly as it relates to public support. The joint force must coordinate all of its messages; further, it must integrate those messages with its partner nations' message as part of the ongoing alignment to maintain unity of effort and stand out in a saturated information environment. The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

For additional discussion of the OE, see pp. 1-6 to 1-7. See facing page for a discussion of public perception.

Effective PA contributes to:

Enhanced Morale and Readiness

PA activities enable military personnel, DOD civilians, and their family members to better understand their roles by explaining the legitimacy of policies, programs, and operations affecting them. PA activities can help alleviate uncertainty and concern

V. Narrative, Themes, and Messages

Ref: JP 3-61 (w/Chg 1), Public Affairs (Aug '16), pp. I-11 to 1-14

Narrative

A narrative is a short story used to underpin operations and to provide greater understanding and context to an operation or situation.

- **Narrative in National Security Strategy.** The national security narrative is formed primarily by broad national policies, as articulated in strategic documents like the National Security Strategy and National Military Strategy. More specific national strategy is developed in National Security Council (NSC) meetings and executed by the relevant departments. For every military operation, the President or NSC staff may create the national/strategic narrative to explain events in terms consistent with national policy.
- **Conflicting Narratives.** Across areas of responsibility (AORs) and during operations within a specified operational area, there can be a struggle to define the prevailing narrative at all levels (internationally, nationally, and within the operational area) on favorable terms. To gain superiority over the adversary's narrative, diminish its appeal and followership, and supplant it or make it irrelevant, the USG needs to establish the reasons for and desired outcomes of the conflict, in terms understandable and acceptable to all relevant publics.

Supporting Themes and Messages

Themes are developed by the NSC staff, Department of State (DOS), DOD, and other USG departments and agencies. JFCs support strategic themes by developing themes appropriate to their mission and authority. Figure I-3 depicts how United States Forces Korea established a theater-strategic narrative linked to a long-term campaign plan. Themes at each level of command should support the themes of the next higher level, while also supporting USG strategic themes.

Operational-level themes are often created for each phase of an operation. Operational themes are nested with strategic themes and enduring national narratives to mitigate the risk that phase-by-phase themes appear to give conflicting messages.

Messages support themes by delivering tailored information to a specific public and can also be tailored for delivery at a specific time, place, and communication method. While messages are more dynamic, they must always support the more enduring themes up and down the chain of command. The more dynamic nature and leeway inherent in messages provide joint force communicators and planners more agility in reaching publics.

Theater and operational themes should nest within the CCDR's and USG's strategic themes. Theater and operational-level messages must also support themes at their level. This enables consistent communications to local and international audiences, which supports strategic objectives.

Sources of information for the national narrative include Presidential speeches and White House communications (www.whitehouse.gov), Secretary of State speeches and DOS communications (www.state.gov and rapid response unit products), Secretary of Defense speeches and DOD communications (www.defense.gov), Chairman of the Joint Chiefs of Staff (CJCS) speeches and communications (www.jcs.mil), and CCDR speeches and combatant command (CCMD) communications. Sources of information for the joint force themes should include the mission, commander's intent, and any other guidance contained within the warning order, planning order, operation order (OPORD), and execute order (EXORD). This is not an exhaustive list; other official sources providing national strategic narratives can contribute to a joint force's narrative. The Defense Press Office (DPO) can help joint force communications with strategic guidance. The DPO routinely coordinates DOD communications with the NSC staff and participating USG departments and agencies.

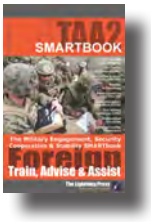
II. Civil Affairs and Civil-Military Operations (CMO)

Ref: JP 3-57, Civil-Military Operations (Sept '13), chap. 1.

I. Civil Affairs and Civil-Military Operations

In carrying out their civil-military operations (CMO) responsibilities, commanders use civil affairs operations (CAO). The relationship between CMO and CAO is best considered within the broad context of unified action that involves the synchronization, coordination, or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. JFCs seek this synergy by several means, one of the more prominent being through the conduct of CMO that bring together the activities of joint forces and multinational forces (MNFs) and nonmilitary organizations to achieve common objectives.

Ref: JP 3-57, Civil-Military Operations, fig I-4, p. I-17.



Refer to TAA2: Military Engagement, Security Cooperation & Stability SMARTbook (Foreign Train, Advise, & Assist) for further discussion. Topics include the Range of Military Operations (JP 3-0), Security Cooperation & Security Assistance (Train, Advise, & Assist), Stability Operations (ADRP 3-07), Peace Operations (JP 3-07.3), Counterinsurgency Operations (JP & FM 3-24), Civil-Military Operations (JP 3-57), Multinational Operations (JP 3-16), Interorganizational Cooperation (JP 3-08), and more.

III. Civil-Military Operations and the Levels of War

Ref: JP 3-57, Civil-Military Operations (Sept '13), pp. I-4 to I-6.

The levels of war are doctrinal perspectives that clarify the links between strategic objectives and tactical actions. The national strategic objectives facilitate theater strategic planning. Military strategy, derived from policy, is the basis for all operations (refer to JP 3-0, Joint Operations). CMO are applicable at the strategic, operational, and tactical levels of war. Specific actions at one level of war may affect all three levels simultaneously but with different effects at each level. CMO guidance should therefore include higher headquarters objectives and end states presented by USG policy and guidance. Individuals and units conducting CMO must understand the interrelationships of the levels of war.

Engaged civilian organizations likely will be more concerned with a predetermined agenda and not distinguish between the various levels of war. NGO or IGO members who communicate with US forces may report conversations to foreign officials at the highest level, who may then discuss them directly with the USG officials. Misperceptions of CMO actions by nonmilitary agencies can cause a commander to be distracted from the mission. Most civilian agencies are not organized with distinct operational, tactical, or strategic levels. NGO and IGO representatives collocated with forward-deployed joint forces often do not have the authority to make decisions that may change their original mission. As such, it is important that JFCs conducting CMO should understand the civilian participant's organizational and hierarchical relationships as they relate to decision making. This will help clarify working relationships and reduce friction with all parties concerned.

CMO are conducted at multiple levels. The effort at each level may be focused on different objectives, but the activities should be mutually supporting.

A. Strategic

At the strategic level, CMO focus on larger and long-term issues that may be part of a Department of Defense (DOD) global campaign, or USG reconstruction, economic development initiatives, and stability operations in failing or recovering nations. CMO are a component of a geographic combatant commander's (GCC's) theater security cooperation guidance within the theater campaign plan (TCP). As such, the GCC's TCP objectives must align with national strategic objectives.

B. Operational

At the operational level, CMO integrate and synchronize interagency, IGO and NGO activities with joint force operations. Interagency, IGO, and NGO activities generally support security cooperation and feature programs to build relationships and mitigate the need for military force. Consequently, CMO focus on immediate or near-term issues such as health service infrastructure; movement, feeding, and sheltering of dislocated civilians (DCs); police and security programs; promoting government legitimacy; and coordination for CMO support to tactical commanders.

Joint force planners and interagency partners should identify civil-military objectives early in the planning process. CMO are integrated into plans and operations through interagency coordination, multinational partnerships, and coordination with IGOs and NGOs. Coordination of CMO for current and future operations is conducted at the operational level. Information is valuable to interorganizational coordination, to efficiently and effectively marshall and distribute resources (to include funding), and to assess success in an OE where success may not be measured by traditional operational indicators. Information management (IM) enables CMO for operational commanders and facilitates the required interorganizational coordination necessary.

C. Tactical

Often, a civil-military team or civil-military operations center (CMOC) may facilitate tactical-level CMO among the military, the local populace, NGOs, and IGOs. Commanders derive tactical-level CMO from the core tasks of support to civil administration (SCA), populace and resources control (PRC), foreign humanitarian assistance (FHA), nation assistance (NA), and CIM. Tactical-level CMO normally are more sharply focused and have more immediate effects. Often, a civilian-military team or CMOC will facilitate these actions between the military, the local populace, and NGOs/IGOs. During certain contingency operations, the Secretary of State and SecDef will integrate stabilization and reconstruction contingency plans with military contingency plans and will develop a general framework for fully coordinating stabilization and reconstruction activities and military operations at all levels where appropriate. The DOS Bureau of Conflict and Stabilization is tasked to implement policy requirements from NSPD-44, Management of Interagency Efforts Concerning Reconstruction and Stabilization. This could provide a framework at the national strategic level for stabilization and reconstruction planning and coordination. SecDef, through the Chairman of the Joint Chiefs of Staff (CJCS), provides direction to combatant commanders (CCDRs) and subordinate JFCs to implement joint operation planning for the NSPD-44, Management of Interagency Efforts Concerning Reconstruction and Stabilization, process.

Annex G (Civil Affairs) promulgates CMO requirements in a formal plan or operation order. CMO require coordination among CA, maneuver, health support, MP, engineer, transportation, and SOF. CMO involve cross-cutting activities across staff sections and subordinate units. Annex G identifies, consolidates, and deconflicts the activities of the various sections and units. Planning and coordination at lower echelons require significantly more details than discussed in annex G.

Changes in the military or political situation, as well as natural or man-made disasters, can divert the joint force's main effort from CMO to combat operations. The JFC should identify early indicators and warnings of changes in the OE and allocate resources to monitor these changes in order to anticipate changes in force requirements. Branch and sequel planning and preventive action may mitigate disruption of CMO. Possible Escalation Indicators include:

- Political activities and movements
- Food or water shortages
- Outbreaks of disease
- Military setbacks
- Natural disasters
- Crop failures
- Fuel shortages
- Onset of seasonal changes (winter may exacerbate fuel and food shortages, for example)
- Police force and corrections system deterioration
- Judicial system shortcomings
- Insurgent attacks
- Sharp rise in crime
- Terrorist bombing
- Disruption of public utilities, e.g., water, power, sewage, and economic strife due to socioeconomic imbalance
- Increase in local government corruption

III. Military Deception (MILDEC)

Ref: FM 6-0 (C2), Commander and Staff Organization and Operations (Apr '16), chap. 11.

This section provides information on military deception. Initially this section addresses the principles of military deception. It then discusses how commanders use military deception to shape the area of operations in support of decisive action. The section concludes with a discussion of how to plan, prepare, execute, and assess military deception.

I. Military Deception Process and Capability

Modern military deception is both a process and a capability. As a process, military deception is a methodical, information-based strategy that systematically, deliberately, and cognitively targets individual decisionmakers. The objective is the purposeful manipulation of decisionmaking. As a capability, military deception 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.

Refer to JP 3-13 for a discussion in information operations and JP 3-13.4 for a more detailed discussion on military deception.

II. Principles of Military Deception

Military deception is applicable during any phase of military operations in order to create conditions to accomplish the commander's intent. The Army echelon that plans a military deception often determines its type. The levels of war define and clarify the relationship between strategic and tactical actions. The levels have no finite limits or boundaries. They correlate to specific levels of responsibility and military deception planning. They help organize thought and approaches to a problem. Decisions at one level always affect other levels. Common to all levels of military deception is a set of guiding principles:

- Focus on the target
- Motivating the target to act
- Centralized planning and control
- Security
- Conforming to the time available
- Integration

Focus on the Target

Leaders determine which targeted decisionmaker has the authority to make the desired decision and then can act or fail to act upon that decision. Many times it is one, key individual, or it could be a network of decisionmakers who rely on each other for different aspects of their mission or operation.

Motivating the Target to Act

Leaders determine what motivates the targeted decisionmaker and which information-related capabilities are capable of inducing the targeted decisionmaker to think a certain way. The desired result is that the targeted decisionmaker acts or fails to act as intended. This result is favorable to friendly forces. Often, the military objective is

III. Military Deception in Support of Operations

Ref: FM 6-0 (C2), Commander and Staff Organization and Operations (Apr '16), pp. 11-2 to 11-4.

Military deception often relies on the basic understanding that the complexities and uncertainties of combat make decisionmakers susceptible to deception. The basic mechanism for any deception is either to increase or decrease the level of uncertainty, or ambiguity, in the mind of the deception target (or targeted decisionmaker). Military deception and deception in support of operations security present false or misleading information to the targeted decisionmaker with the deliberate intent to manipulate uncertainty. The aim of deception is to either increase or decrease the targeted decisionmaker's ambiguity in order to manipulate the target to perceive friendly motives, intentions, capabilities, and vulnerabilities erroneously and thereby alter the target's perception of reality.

Ambiguity-Decreasing Deception

Ambiguity-decreasing deception reduces uncertainty and normally confirms the enemy decisionmaker's preconceived beliefs, so the decisionmaker becomes very certain about the selected course of action (COA). This type of deception presents false information that shapes the enemy decisionmaker's thinking, so the enemy makes and executes a specific decision that can be exploited by friendly forces. By making the wrong decision, which is the deception objective, the enemy could misemploy forces and provide friendly forces an operational advantage. For example, ambiguity-decreasing deceptions can present supporting elements of information concerning a specific enemy's COA. These deceptions are complex to plan and execute, but the potential rewards are often worth the increased effort and resources.

Ambiguity-Increasing Deception

Ambiguity-increasing deception presents false information aimed to confuse the enemy decisionmaker, thereby increasing the decisionmaker's uncertainty. This confusion can produce different results. Ambiguity-increasing deceptions can challenge the enemy's preconceived beliefs. These deceptions draw enemy attention from one set of activities to another, create the illusion of strength where weakness exists, create the illusion of weakness where strength exists, and accustom the enemy to particular patterns of activity that are exploitable at a later time. For example, ambiguity-increasing deceptions can cause the target to delay a decision until it is too late to prevent friendly mission success. They can place the target in a dilemma for which there is no acceptable solution. They may even prevent the target from taking any action at all. Deceptions in support of operations security (OPSEC) are typically executed as this type of deception.

Tactical Deception

Most often, Army commanders will be faced with deciding when and where to employ military deception in support of tactical operations. The intent of tactical deception is to induce the enemy decisionmakers to act in a manner prejudicial to their interests. This is accomplished by either increasing or decreasing the ambiguity of the enemy decisionmaker through the manipulation, distortion, or falsification of evidence. Military deception undertaken at the tactical level supports engagements, battles, and stability tasks. This focus is what differentiates tactical deception from other forms of military deception.

Refer to JP 3-13.4 for more information on military deception.

Strategic and Operational Military Deception

Less frequently, Army commanders will employ strategic and operational military deception to influence enemy strategic decisionmakers' abilities to successfully oppose U.S. national interests and goals or to influence enemy decisionmakers' abilities to conduct operations. These deceptions are joint or multinational efforts. In these cases, Army

IV. Military Information Support Operations (MISO)

Ref: JP 3-13.2 (w/Chg 1), Military Information Support Operations (Dec '11).

Today's global information environment is complex, rapidly changing, and requires integrated and synchronized application of the instruments of national power to ensure responsiveness to national goals and objectives. In the current operational environment, effective influence is gained by unity of effort in what we say and do, and how well we understand the conditions, target audiences (TAs), and operational environment. Within the military and informational instruments of national power, the Department of Defense (DOD) is a key component of a broader United States Government (USG) communications strategy. To be effective, all DOD communications efforts must inherently support the credibility, veracity, and legitimacy of USG activities.

Military information support operations (MISO) play an important role in DOD communications efforts through the planned use of directed programs specifically designed to support USG and DOD activities and policies. MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. Military information support (MIS) professionals follow a deliberate process that aligns commander's objectives with an analysis of the environment; select relevant TAs; develop focused, culturally, and environmentally attuned messages and actions; employ sophisticated media delivery means; and produce observable, measurable behavioral responses.

The employment of MIS units is governed by explicit legal authorities that direct and determine how their capability is utilized. This legal foundation establishes MISO as a communications means and allows their integration with those strategies that apply the instruments of national power. Leaders and planners interpret relevant laws and policies to conduct MISO in any situation or environment, internationally and domestically.

Joint MISO support policy and commanders' objectives from strategic to tactical levels. Although military leadership and local key communicators are examples of TA engaged at the operational and tactical levels that are capable of affecting the accomplishment of a strategic objective.

MISO are used to establish and reinforce foreign perceptions of US military, political, and economic power and resolve. In conflict, MISO as a force multiplier can degrade the enemy's relative combat power, reduce civilian interference, minimize collateral damage, and maximize the local populace's support for operations.

MISO contribute to the success of both peacetime engagements and major operations. The combatant commander (CCDR) receives functional and theater strategic planning guidance from the Joint Strategic Capabilities Plan (JSCP), Unified Command Plan (UCP), and Guidance for Employment of the Force (GEF). These documents are derived from the Secretary of Defense (SecDef) National Defense Strategy, which interprets the President's national security policy and strategy, and the Joint Chiefs of Staff National Military Strategy.

III. Information Roles & Relationships

Ref: JP 3-13.2 (w/Chg 1), Military Information Support Operations (Dec '11), fig. II-1, p. II-9.

There are a variety of functions and capabilities that help a JFC formulate the command's message and communicate with local, international, and US domestic audiences as part of broader policy and in support of operational objectives. DOD information activities include IO, MISO, PA (to include visual information), and DSPD.

Dept of Defense Information Activities

INFORMATION ACTIVITY	PRIMARY TASK	FOCUS OF ACTIVITY	PURPOSE	DESIRED OUTCOME
US Government (USG) Strategic Communication (Department of State Lead)	Coordinate information, themes, plans, programs, and actions that are synchronized with other elements of national power	Understand and engage key audiences	Better enable the USG to engage foreign audiences holistically and with unity of effort	Create, strengthen, or preserve conditions favorable to advance national interests and objectives
Department of Defense (DOD) support to Strategic Communication	Use DOD operational and informational activities and strategic communication processes in support of Department of State's broader public diplomacy efforts	Key audiences	Improve the alignment of DOD actions and information with policy objectives	The conduct of military activities and operations in a shaped environment
Information Operations	Integrate information operations core, supporting, and related capabilities as part of a military plan	Adversary audiences	Influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.	Optimum application of capability to desired military outcome
Military Information Support Operations	Influence target audience perceptions, attitudes, and subsequent behavior	Approved foreign audiences	Shape, deter, motivate, persuade to act	Perceptions, attitudes, and behavior conducive to US/multinational partner objectives
Public Affairs	Provide truthful, timely, accurate information about DOD activities (inform)	US, allied, national, international, and internal audiences	Keep the public informed, counter adversary information activities, deter adversary actions, and maintain trust and confidence of US population, and friends and allies	Maintain credibility and legitimacy of US/multinational partner military operations with audience

PA and MISO are separate and unique activities that are governed by policy and practice in terms of audiences, focus, and scope. SC integrates various instruments of national power with other activities across the USG to synchronize crucial themes, messages, images, and actions. SC is policy driven and generally conducted under DOS lead. DOD SC activities are designed to support the continuity of DOD strategic- and operational-level messages and activities with overall USG policy and SC themes.

Continued on next page

V. Operations Security (OPSEC)

Ref: JP 3-13.3, Operations Security (Jan '12) and ATP 3-13.3, Army Operations Security for Division and Below (Jul '19).

Joint forces often display personnel, organizations, assets, and actions to public view and to a variety of adversary intelligence collection activities, including sensors and systems. Joint forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed to the field conducting actual operations. Frequently, when a force performs a particular activity or operation a number of times, it establishes a pattern of behavior. Within this pattern, certain unique, particular, or special types of information might be associated with an activity or operation. Even though this information may be unclassified, it can expose significant US military operations to observation and/or interdiction. In addition, the adversary could compile and correlate enough information to facilitate predicting and countering US operations.

I. Purpose of Operations Security

The purpose of OPSEC is to reduce the vulnerability of US and multinational forces from successful adversary exploitation of critical information. OPSEC applies to all activities that prepare, sustain, or employ forces.

The OPSEC process is a systematic method used to identify, control, and protect critical information and subsequently analyze friendly actions associated with military operations and other activities to:

- Identify those actions that may be observed by adversary intelligence systems.
- Determine what specific indications could be collected, analyzed, and interpreted to derive critical information in time to be useful to adversaries.
- Select countermeasures that eliminate or reduce vulnerability or indicators to observation and exploitation.
- Avoid patterns of behavior, whenever feasible, and thus preclude the possibility of adversary intelligence constructing an accurate model.
- Prevent the display or collection of critical information, especially during preparation for and execution of actual operations.
- Avoid drastic changes as OPSEC countermeasures are implemented. Changes in procedures alone will indicate to the adversary that there is an operation or exercise starting.

An **indicator** is data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities. Selected indicators can be developed into an analytical model or profile of how a force prepares and how it operates. An indication is an observed specific occurrence or instance of an indicator.

Adversary intelligence personnel continuously analyze and interpret collected information to validate and/or refine the model. As adversary analysts apply more information to the analytical model, the likelihood increases that the analytical model will replicate the observed force. Thus, current and future capabilities and courses of action (COA) can be revealed and compromised. **Critical information** consists of

V. Operations Security Indicators

Ref: ATP 3-13.3, Army Operations Security for Division and Below (Jul '19).

The indicator's signature is a characteristic that serves to set the indicator apart. A signature makes the indicator identifiable or causes it to stand out. Uniqueness and stability are properties of a signature. Uncommon or unique features reduce the ambiguity of an indicator.

Association. Association is the process of forming mental connections to an indicator. It is the key to interpretation. An enemy compares current data with previously gathered information to identify possible relationships. Continuity of actions, objects, or other indicators, which register as patterns, provides another association. For example, the presence of special operations aviation aircraft, such as the MH-6, MH-60, and MH-47,may be indicators of other special operations forces operating in the area. Certain items of equipment particular to specific units are indicators of the potential presence of related equipment. For instance, the sighting of an M-88A2 Hercules Recovery Vehicle likely indicates the presence of an armored unit equipped with M1A2-series tanks, as the M-88A2 is rated to recover and tow the M1A2-series tanks. Such continuity can result from repetitive practices or sequencing instead of from planned procedures. When detecting some components of symmetrically-arrayed organizations, the enemy can assume the existence of the rest. As another example, the adversary would suspect the presence of an entire infantry battalion when intelligence detects the headquarters company and one line company. When evaluated as a whole, the pattern can be a single indicator, which simplifies the enemy's analysis.

Profile. A profile is accumulated data that portray the significant features of an indicator. Profiles are linked to functional activity, which has a profile comprising unique indicators, patterns, and associations. This profile, in turn, has several sub-profiles for the functional activities needed to deploy the particular mission aircraft (for example, fuels, avionics, munitions,communications, air traffic control, supply, personnel, and transportation). If a functional profile does not appear to change from one operation to the next, it is difficult for an enemy to interpret. However, if it is distinct, the profile may be the key or only indicator needed to understand the operation. Unique profiles reduce the time needed to make accurate situational assessments. They are primary warning tools because they provide a background for contrasts.

Contrast. Contrast is the change in an indicator's established profile. The key to obtaining the contrast of an indicator lies in how it differs from what has been shown previously. Contrasts are the simplest and most reliable means of detection because they only need to be recognized, not understood. One question prompts several additional ones concerning contrasts in profile. The nature of the indicator's exposure is an important aspect when seeking profile contrasts. For example, if the adversary identifies items specific to special operations aviation at an airfield, this will contrast with what is "normal" at the airfield and will indicate the deployment of special operations aircraft to the airfield without having actually observed them.

Exposure. Exposure is the condition of being presented to view or made known—the condition of being unprotected. For an OPSEC indicator, exposure increases according to the duration, repetition, and timing of its appearance. The exposure of an indicator often reveals its relative importance and meaning. Limited duration and repetition reduces detailed observation and associations. An indicator that appears for a short time will likely fade into the background of insignificant anomalies. An indicator that appears over a long period of time, however, becomes part of a profile. Indicators exposed repeatedly present the biggest danger. Operations conducted the same way several times with little or no variation provide an adversary the information needed to determine where, when, how, and with what to attack. Repetitive operations cost many lives in wartime.

VI(a). Cyberspace Operations (CO)

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), chap. 1.

Superiority in cyberspace and the electromagnetic spectrum (EMS) provides a decisive advantage to commanders at all levels in modern combat. The Army's ability to exploit cyberspace and EW capabilities will prove critical to the success of unified land operations. As cyberspace and EW operations develop similar and complementary capabilities, the Army must plan, integrate, and synchronize these operations with unified land operations.

Employing cyberspace and EW capabilities under a single planning, integration, and synchronization methodology increases the operational commander's ability to understand the environment, project power, and synchronize multiple operations using the same domain and environment. Synchronizing offensive and defensive activities allows a faster response to enemy and adversary actions. The EMS is the common denominator for both cyberspace and EW operations, and also impacts every operation in the Army.

The distinctions between cyberspace and EW capabilities allow for each to operate separately and support operations distinctly. However, this also necessitates synchronizing efforts to avoid unintended interference. Any operational requirement specific to electronic transfer of information through the wired portion of cyberspace must use a cyberspace capability for affect. If the portion of cyberspace uses only the EMS as a transport method, then it is an EW capability that can affect it. Any operational requirement to affect an EMS capability not connected to cyberspace must use an EW capability.

The Department of Defense information network-Army (DODIN-A) is the Army's critical warfighting platform, which enables mission command, precision fires, intelligence, logistics, and tele-medicine, and supports all operations. Access to the DODIN-A allows commanders to project combat power, conduct support operations, and achieve joint and Army force commander objectives. Securing and operating this expansive network is one of the most complex and important operations the Army currently undertakes. A single vulnerability within this network can place units and operations at risk, potentially resulting in mission failure. Understanding how to operationalize cyberspace and the EMS is a fundamental staff proficiency and commander's priority.

Superiority in cyberspace and the EMS to support Army operations results from effectively synchronizing Department of Defense information network (DODIN) operations, offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), electronic attack, electronic protection, electronic warfare support, and spectrum management operations (SMO). 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). 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.

Cyberspace and the EMS will likely grow increasingly congested, contested, and critical to successful unified land operations. Success will be measured by the ability to execute operations freely in cyberspace and the EMS, while controlling the ability of others to operate in the domain.

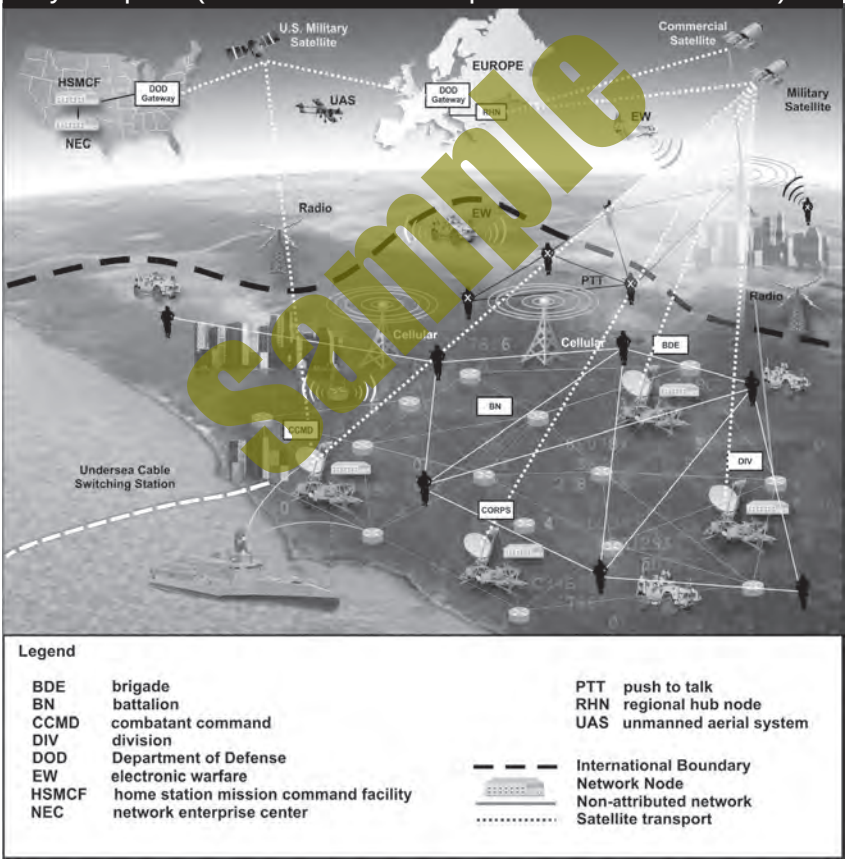
See following pages (p. 3-48 to 3-49) for a discussion of the cyberspace domain.

I. The Cyberspace Domain

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-2 to 1-4.

Cyberspace is 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. The Army performs cyberspace operations and supporting activities within this domain as part of joint and Army operations. Friendly, enemy, adversary, and host nation networks, communications systems, computers, cellular phone systems, social media Web sites, and technical infrastructures are all part of cyberspace. Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). The interrelated cyberspace missions are DODIN operations, DCO, and OCO. A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

Cyberspace (Visualization in an Operational Environment)



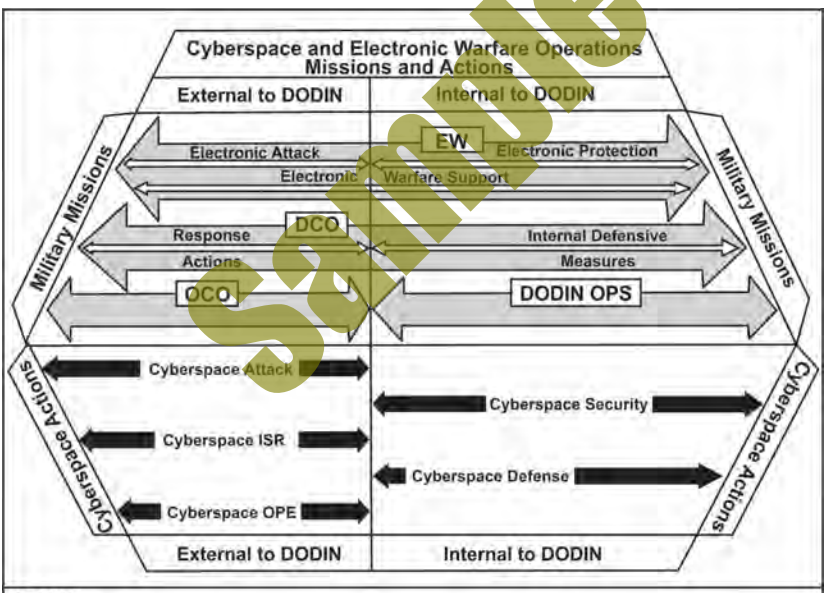
Ref: FM 3-12 (Apr '17), fig. 1-1. Visualization of cyberspace and the electromagnetic spectrum in an operational environment.

IV. Army Cyberspace Missions and Actions

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), pp. 1-6 to 1-7.

Cyberspace missions and actions are interrelated; synchronizing and supporting efforts among the cyberspace missions is imperative to maintaining freedom of maneuver in cyberspace. Supporting the cyberspace missions are the cyberspace actions: cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance (ISR); cyberspace OPE; cyberspace attack; and cyberspace security. Cyberspace actions support DODIN operations, DCO, OCO, or any combination thereof. Executing cyberspace actions at any echelon is dependent on authority, capability, and coordination. The actions are interrelated and a cyberspace mission may require more than one action to achieve mission success.

Army forces can execute cyberspace missions and actions under the proper authority. Since DODIN operations and some DCO tasks may overlap, Army forces may conduct multiple cyberspace missions or actions as part of their daily duties and responsibilities. Situational requirements may dictate the transition from cyberspace security to DCO internal defensive measures (DCO-IDM). Figure 1-3 below shows the relationship of the cyberspace missions and cyberspace actions both external and internal to the DODIN and the owned, leased, shared partner portions of cyberspace. EW can affect the cyberspace capabilities that use the EMS.



Ref: FM 3-12 (Apr '17), 1-3. Cyberspace & EW operations, missions and actions.

Refer to CYBER1: The Cyberspace Operations & Electronic Warfare SMARTbook (Multi-Domain Guide to Offensive/Defensive CEMA and CO). Topics and chapters include cyber intro (global threat, contemporary operating environment, information as a joint function), joint cyberspace operations (CO), cyberspace operations (OCO/DCO/DODIN), electronic warfare (EW) operations, cyber & EW (CEMA) planning, spectrum management operations (SMO/JEMSO), DoD information network (DODIN) operations, acronyms/abbreviations, and a cross-referenced glossary of cyber terms.

VI(b). Electronic Warfare (EW)

Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), pp. 1-25 to 1-35.

I. Electronic Warfare (EW)

Electronic warfare refers to 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 EMS to support the commander's intent and concept of operations.

Electronic Warfare (EW) Operations

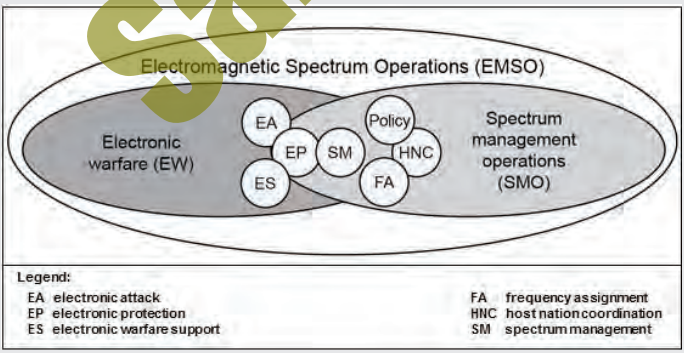
A **Electronic Attack (EA)**

B **Electronic Protection (EP)**

C **Electronic Warfare Support (ES)**

Electromagnetic Spectrum Operations (EMSO)

EMSO are comprised of EW and SMO. The importance of the EMS and its relationship to the operational capabilities of the Army is the focus of EMSO. EMSO include all activities in military operations to successfully control the EMS. Figure 1-8 illustrates EMSO and how they relate to SMO and EW.



Ref: FM 3-12 (Apr '17), fig. 1-8. Electromagnetic spectrum operations.

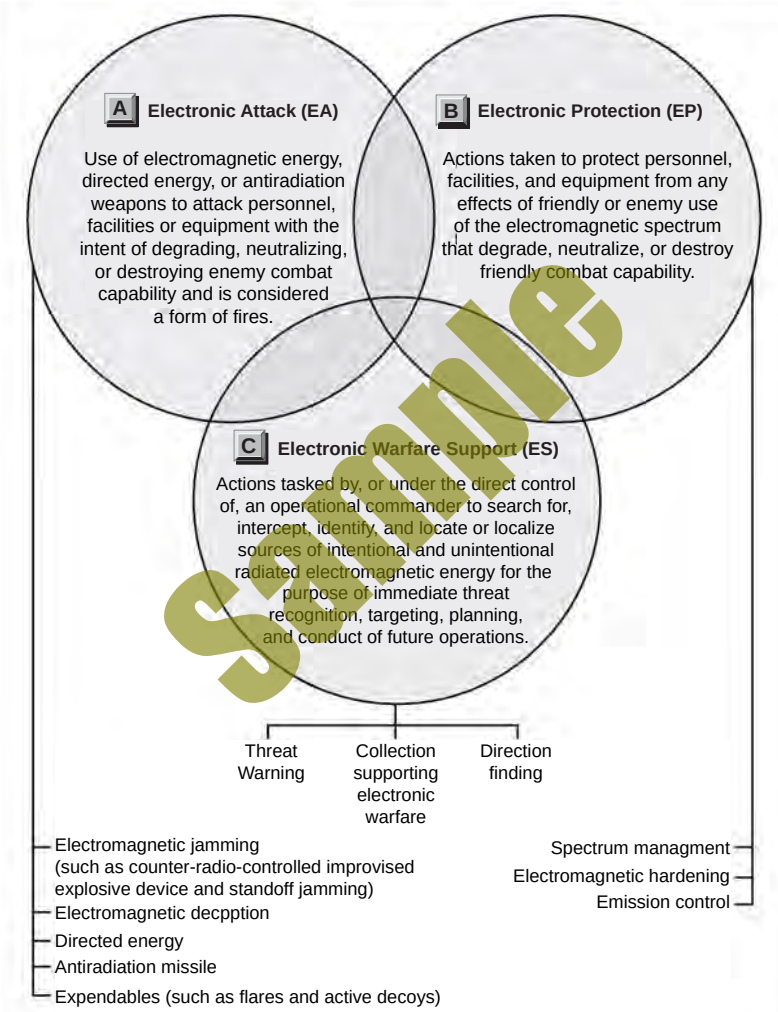
Throughout this document, the term EW operations refers to planning, preparing, execution, and continuous assessment of the electronic warfare activities of an operation. The term EMSO indicates the addition of those operationally related spectrum management operations activities.

II. Electronic Warfare Missions

Ref: FM 3-12, Cyberspace & Electronic Warfare Operations (Apr '17), fig. 1-9.

With proper integration and deconfliction, EW can create reinforcing and complementary effects by affecting devices that operate in and through wired and wireless networks.

Electronic Warfare (EW) Missions



Ref: FM 3-12, Cyberspace and Electronic Warfare Operations (Apr '17), fig. 1-9. Electronic warfare missions.

VII. Space Operations

Ref: JP 3-14 (w/Chg 1), Space Operations (Oct '20).

Access to space is vital to the collective security of the United States and its allies and partners. The Department of Defense (DOD) space policy is focused on deterring adversaries, defending against threats, and pursuing resilient space architectures that contribute to achieving space mission assurance and objectives. Further, the United States must sustain the ability to attribute malicious or irresponsible actions that jeopardize the viability of space for all. Sustained space access is vital to the collective security of the United States and its allies and partners.

Space Domain

The space domain is the area above the altitude where atmospheric effects on airborne objects become negligible. United States Space Command (USSPACECOM) area of responsibility (AOR) is the area surrounding the Earth at altitudes equal to, or greater than, 100 kilometers (54 nautical miles) above mean sea level. Like the air, land, and maritime domains, space is a physical domain within which military, civil, and commercial activities are conducted. The relationship between space and cyberspace is unique in that many space operations depend on cyberspace, and a critical portion of cyberspace can only be provided via space operations.

Proper planning and execution of military operations in space enables activities such as intelligence collection; early warning; environmental monitoring; satellite communications (SATCOM); and positioning, navigation, and timing (PNT). Activities conducted in space support freedom of action throughout the operational environment (OE), and operations in other domains may create effects in space.

I. Space Operations

Space operations are those operations impacting or directly utilizing space-and ground-based capabilities to enhance the potential of the United States and multinational partners. Joint space forces are the space and terrestrial systems, equipment, facilities, organizations, and personnel, or combination thereof, necessary to conduct space operations. Space systems consist of three related segments: space, link, and ground.

- The **ground segment** consists of ground-based facilities and equipment supporting command and control (C2) of space segment resources, as well as ground-based processing equipment, Earth terminals or user equipment, space situational awareness (SSA) sensors, and the interconnectivity between the facilities in which this equipment is housed.
- The **link segment** consists of signals connecting ground and space segments through the electromagnetic spectrum (EMS). This link normally includes telemetry, tracking, and commanding (TT&C) signals necessary for controlling the spacecraft and payload. Separate from the TT&C signals, the satellite payload may contribute to the link segment through the use of SATCOM signals between two terminals on the ground or a PNT signal enhancing air, ground, and naval maneuver.
- The **space segment** involves the operational spacecraft within the space domain.

II. Space Capabilities

Ref: JP 3-14 (w/Chg 1), Space Operations (Oct '20), chap. 2.

Due to the complexities of the operational environment (OE) and the required integration and coordination between elements of the joint force, a shared understanding of selected aspects of specific space capabilities is essential to foster and enhance unified action.

Space Situational Awareness (SSA)

Space situational awareness (SSA) is the requisite foundational, current, and predictive knowledge and characterization of space objects and the OE upon which space operations depend—including physical, virtual, information, and human dimensions—as well as all factors, activities, and events of all entities conducting, or preparing to conduct, space operations. Space surveillance capabilities include a mix of space-based and ground-based sensors. SSA is dependent on integrating space surveillance, collection, and processing; environmental monitoring; status of US and cooperative satellite systems; understanding of US and multinational space readiness; and analysis of the space domain.

Space Control

Space control includes offensive space control and defensive space control operations to ensure freedom of action in space and, when directed, defeat efforts to interfere with or attack US or allied space systems. Space control uses a broad range of response options to provide continued, sustainable use of space. Space control contributes to space deterrence by employing a variety of measures to assure the use of space; attributing enemy attacks; and being consistent with the right to self-defense, target-threat space capabilities.

See following page (p. 3-64) for further discussion of space control and superiority.

Positioning, Navigation, and Timing (PNT)

Military users depend on assured positioning, navigation, and timing (PNT) systems for precise and accurate geo-location, navigation, and time reference services. PNT information, whether from space-based global navigation satellite systems (GNSSs), such as Global Positioning System, or non-GNSS sources, is considered mission-essential for virtually every modern weapons system.

Intelligence, Surveillance, Reconnaissance

Space-based intelligence collection synchronizes and integrates sensors, assets, and systems for gathering data and information on an object or in an area of interest on a persistent, event-driven, or scheduled basis. Space-based intelligence, surveillance, and reconnaissance, which includes overhead persistent infrared (OPIR), is conducted by an organization's intelligence collection manager to ensure integrated, synchronized, and deconflicted operations of high-demand assets.

Satellite Communications (SATCOM)

Satellite communications (SATCOM) systems inherently facilitate beyond line-of-sight connectivity. Depending on its configuration, a robust SATCOM architecture provides either equatorial coverage (nonpolar) or high-latitude coverage (includes poles). This provides national and strategic leadership with a means to maintain situational awareness and convey their intent to the operational commanders responsible for conducting joint operations.

Environmental Monitoring

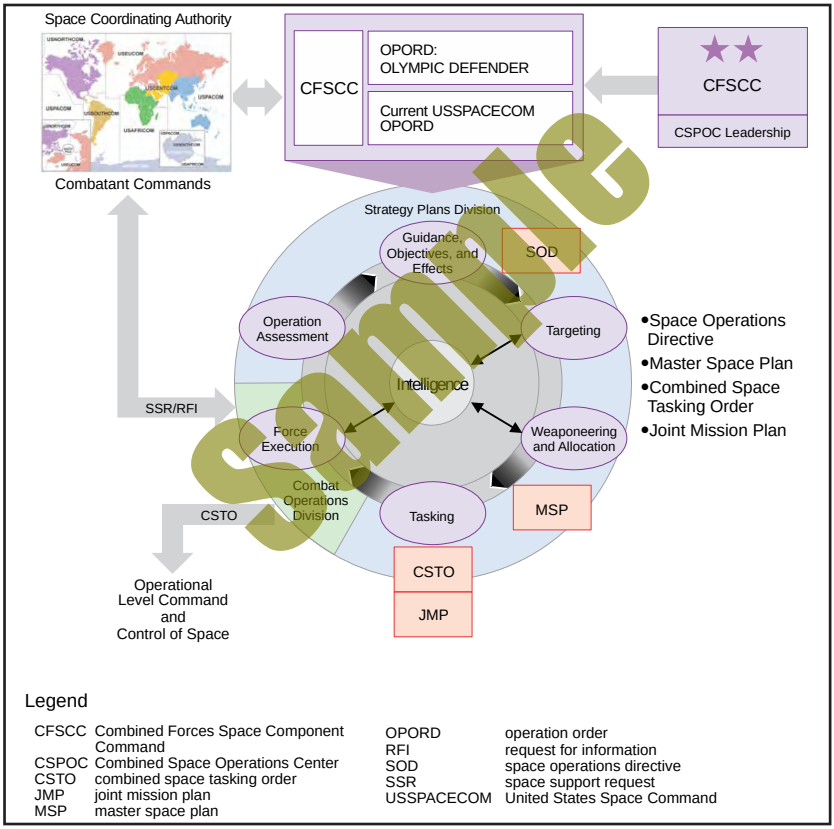
Terrestrial environmental monitoring provides information on meteorological and oceanographic factors that affect military operations. Space environmental monitoring provides data that supports forecasts, alerts, and warnings for the space environment that may

Combined Space Tasking Order (CSTO)

Ref: JP 3-14 (w/Chg 1), Space Operations (Oct '20), p. IV-7.

Specific to space operations, the CFSCC produces plans/orders for the management of assigned space forces through the CSTO. The CSTO and special instructions (SPINS) direct space forces, assign tasks to meet joint force operational objectives, and synchronize space operations with other CCMD operations (see Figure IV-1).

The operational planning cycle includes inputs into the joint targeting cycle, as depicted in Figure IV-1. The space operations directive captures the CFSCC's guidance and intent. The space operations directive conveys prioritization and apportionment guidance focused on the applicable execution period. This is then used to form the master space plan. The master space plan is used to allocate resources to each desired effect and serves as the source to generate unit tasking and coordination within the CSTO and SPINS. The CSTO tasks execution and the SPINS provide amplifying guidance.



Ref: JP 3-14 (w/Chg 1), fig. IV-1. Combined Space Tasking Order Process.

The planning process may significantly compress during a crisis or to support major combat operations. In periods of conflict, the CSTO cycle may compress from a 30¬day production cycle to synchronize with the supported CCDR's air tasking order cycle. The CSTO transmits the CFSCC's guidance and priorities for a short-duration timeframe, assigns tasks to meet operational objectives, and, when required, synchronizes and integrates CFSCC activities with other CCMD operations.

VIII. Additional IRCs

Ref: JP 3-14 (w/Chg 1), Space Operations (Oct '20).

In addition to the specific IRCs covered on the previous pages, FM 3-13 discusses additional capabilities as outlined below.

Additional IRCs

- **A** — **Integrated Joint Special Technical Operations (IJSTO)**
- **B** — **Special Access Programs (SAP)**
- **C** — **Personnel Recovery (PR)**
- **D** — **Physical Attack**
- **E** — **Physical Security**
- **F** — **Presence, Profile, and Posture (PPP)**
- **G** — **Soldier and Leader Engagement (SLE)**
- **H** — **Police Engagement**
- **I** — **Social Media**

All unit operations, activities, and actions affect the information environment. Even if they primarily affect the physical dimension, they nonetheless also affect the informational and cognitive dimensions. For this reason, whether or not they are routinely considered an IRC, a wide variety of unit functions and activities can be adapted for the purposes of conducting information operations or serve as enablers to its planning, execution, and assessment.

See p. 3-1 for additional discussion.

Chap 4

(Information Operations) PLANNING

Ref: FM 3-13, Information Operations (Dec '16), pp. 4-1 to 4-2.

Planning is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Planning helps commanders create and communicate a common vision between commanders, their staffs, subordinate commanders, and unified action partners. Planning results in a plan and orders that synchronize the action of forces in time, space, and purpose to achieve objectives and accomplish missions.

Commanders, supported by their staffs, ensure IO is fully integrated into the plan, starting with Army design methodology (ADM) and progressing through the military decisionmaking process (MDMP). The focal point for IO planning is the IO officer (or designated representative for IO). However, the entire staff contributes to planning products that describe and depict how IO supports the commander's intent and concept of operations. The staff also contributes to IO planning during IO working group meetings to include assessing the effectiveness of IO and refining the plan.

Commanders, supported by their staffs, ensure IO is fully integrated into the plan, starting with Army design methodology and progressing through the military decisionmaking process.

Army Design Methodology (ADM)

ADM helps commanders and staffs with the conceptual aspects of planning. These aspects include understanding, visualizing, and describing operations to include framing the problem and identifying an operational approach to solve the problem.

Military Decisionmaking Process (MDMP)

The MDMP helps commanders and staffs translate the commander's vision into an operations plan or operations order that synchronizes the actions of the force in time, space, and purpose to accomplish missions. Both the problem the commander needs to solve and the specific operation to advance towards its solution have significant information-related aspects.

See pp. 4-3 to 4-16 for discussion of commander, staff, and IO working group responsibilities for synchronizing information-related capabilities.

Planning activities occupy a continuum ranging from conceptual to detailed. **Conceptual planning** involves understanding operational environments and problems, determining the operation's end state, and visualizing an operational approach to attain that end state. **Detailed planning** translates the commander's operational approach into a complete and practical plan. Generally, detailed planning is associated with the science of control including synchronizing forces in time, space, and purpose to accomplish missions.

Refer to BSS6: The Battle Staff SMARTbook, 6th Ed. for further discussion. BSS6 covers the operations process (ADP 5-0); commander's activities; Army planning methodologies; the military decisionmaking process and troop leading procedures (FM 7-0 w/Chg 2); integrating processes (IPB, information collection, targeting, risk management, and knowledge management); plans and orders; mission command, C2 warfighting function tasks, command posts, liaison (ADP 6-0); rehearsals & after action reviews; and operational terms and military symbols (ADP 1-02).

I. Synchronization of Info-Related Capabilities

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 4.

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.

I. Commanders' Responsibilities

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.

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.

See following pages (pp. 4-4 to 4-5) for an overview and further discussion.

II. Staff Responsibilities

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.

Key IO Planning Tools and Outputs

Key staff outputs include the:

- IO running estimate (*See pp. 4-6 to 4-7.)*
- Logic of the effort (*See p. 4-8.)*
- Commander's critical information requirements (CCIRs) and CCIRs and essential elements of friendly information (EEFIs) (*See p. 4-9.)*
- Combined Information Overlay (CIO) (*See pp. 4-32 to 4-33.)*

Information operations input to base orders and plans include:

- Mission Statement (*See p. 4-11.)*
- Scheme of information operations (*See pp. 4-12 to 4-13.)*
- IO Objectives & IRC tasks (*See pp. 4-14 to 4-15.)*
- IO Synchronization Matrix (*See p. 4-16.)*
- Battle drills (*See pp. 4-65 to 4-68.)*
- Other products as needed

See p. 6-3 for related discussion of the IO working group inputs and outputs (fig. 4-1) and chap. 7 for fires and targeting products.

A. IO Running Estimate *See also pp. 4-37.*

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 4-3 to 4-6.

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. 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. 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. *(Fig. 4-2, below).*

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.

Variations on this format, such as the example provided in Figure 4-3 below 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.

Example Graphical IO Running Estimate

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

Ref: ATP 3-13.3, fig. 4-3. Example graphical information operations running estimate.

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.

See related discussion of the running estimate on p. 4-37.

B. Scheme of Information Operations

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 4-9 to 4-11.

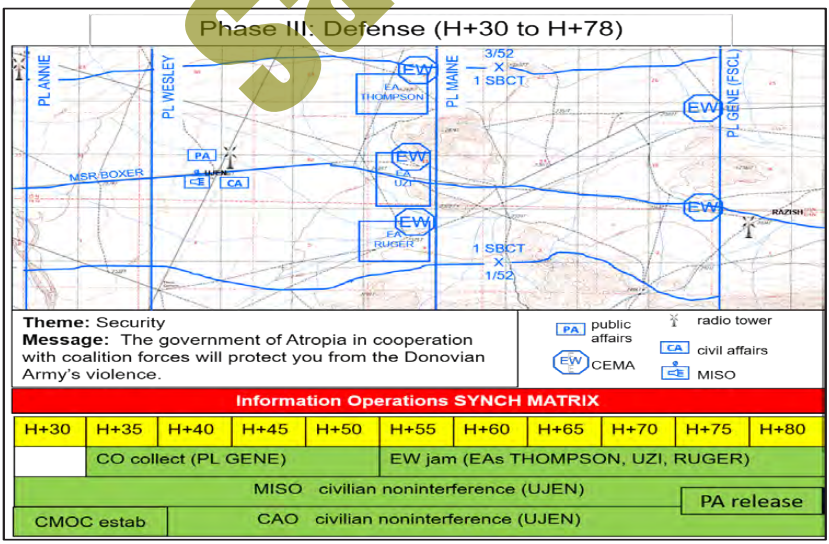
The scheme of IO begins with a clear, concise statement of where, when, and how the commander intends to employ synchronized IRCs to create effects in and through the information environment to support the overall operation and accomplish the mission. Based on the commander's planning guidance, the IO 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 provides a sample scheme of an IO statement. Figure 4-6 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		

Ref: ATP 3-13.1, fig. 4-5. Sample scheme of information operations statement.



Ref: ATP 3-13.1, fig. 4-6. Example scheme of information operations sketch.

D. IO Synchronization Matrix

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 4-14 to 4-16.

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.

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

Ref: ATP 3-13.1, table 4-2. Example 2 – 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.

Ref: ATP 3-13.1, table 4-1. Example 1 – Information operations synchronization matrix.

II. Information Environment Analysis

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 2.

IO and Intelligence Preparation of the Battlefield (IPB)

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.

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.

Analyze and Depict the Information Environment

To achieve advantage in the information environment, commanders, with specialized advice and support from the IO officer, ensure that IO planning is fully integrated into the operations process. This begins with analysis to understand, visualize, and describe the information environment.

A significant part of what makes the operational environment complex is the information environment because it includes such components as cyberspace, the electromagnetic spectrum, data flow, encryption and decryption, the media, biases, perceptions, decisions, key leaders and decision makers, among many others. What occurs in the physical dimension of the information environment and, more broadly, the operational environment, always has second- and third-order effects in the informational and cognitive dimensions of the information environment. Thus, there must be holistic and nuanced understanding of how these various components and dimensions interrelate and the whole operates.

This understanding is depicted through a series of information overlays and comprehensive combined information overlays, which vary depending on commanders' priorities, the nature of the operation, and the type of analysis being conducted. Modeling or mapping social or human networks also enhances this understanding. While complex, the information environment still needs to be captured in a way that the commander can visualize and understand it, draw necessary insights and conclusions, and make informed decisions. The IO officer should not be locked into any specific method for analyzing and depicting the information environment but develop a process and overlays that best serve the commander and, as appropriate, follow unit standard operating procedures. As new technologies and interactive capabilities emerge, they should be incorporated as tools to facilitate the visualization and understanding processes.

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 pp. 4-6 to 4-7 for discussion of running estimates and pp. 4-32 to 4-33 for discussion of the combined information overlay.

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 (IPB):

Step 1: Define the Information Environment

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)

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

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

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

Examples of Operational Variables Crosswalked with Civil Considerations

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-5 to 2-6.

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.

	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
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

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

Example Overlay

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-7 to 2-11.

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).

The following figures 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.

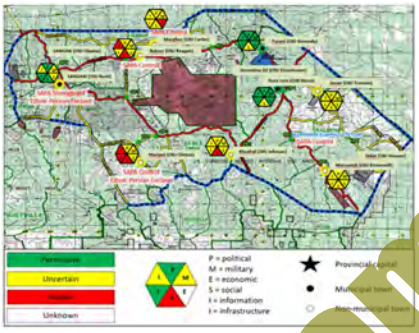


Figure 2-1. Example overlay that depicts relevant information about the populace in the area of operations.

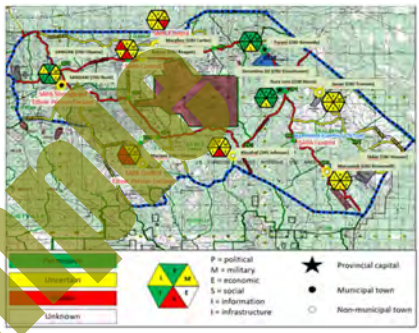


Figure 2-2. Example overlay that depicts relevant information about communications infrastructure in the area of operations.

Sangari:	***Turani:***	***Janan:***
• 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	• 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)	• 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

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).

Combined Information Overlay (CIO)

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-16 to 2-17.

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.

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.

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 (refer to ATP 2-22.9 for more on this topic).

A thorough understanding of the current state of the information environment, local communications means, methods, trusted sources, key influencers, established cognitive patterns, cultural norms, perspectives, historical narrative, system of opposition, and adversary and HN IRCs is critical to the development of the commander's communication synchronization effort.

Significant characteristics, further analyzed within the physical, informational, and cognitive dimensions, can be graphically represented on a **combined information overlay.** The analyst can use this overlay to identify strengths and/or vulnerabilities of the information environment that can be exploited by friendly or adversary forces. The adversary mindset should be evaluated to determine the probable state of morale in both the civil and military population. Morale is a significant factor not only in assessing the overall capability of a military force, but also in evaluating the extent to which the civil populace will support military operations. The degree of regime loyalty should be assessed not only for the populace but also, if possible, for individual leaders. Depending on the situation, factors such as ethnic, religious, political, or class grievances or differences may be exploitable for military information support operations (MISO) purposes. Psychological profiles on military and political leaders may facilitate understanding an adversary's behavior, evaluating an adversary's vulnerability to deception, and assessing the relative probability of an adversary's adopting various COAs.

- JP 2-01.3, Joint Intelligence Preparation of the Operational Environment (May '14), pp. III-23 to III-24.

Figure 2-5 below 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.

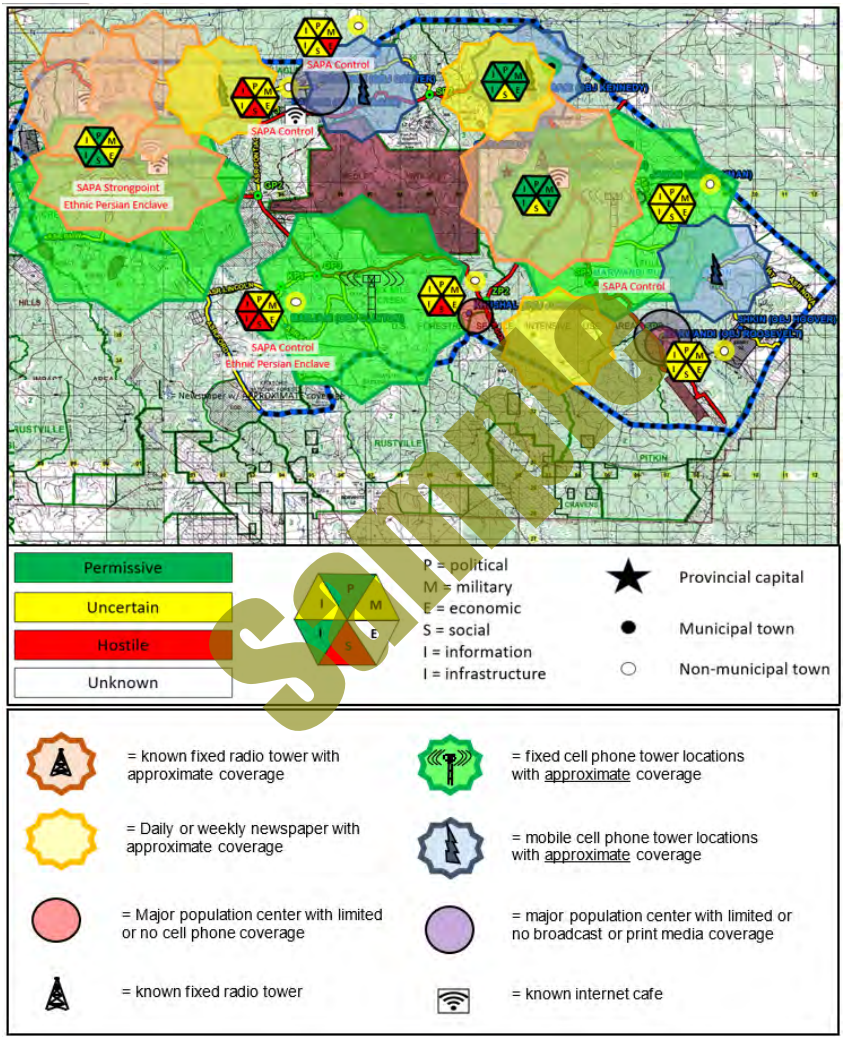


Figure 2-5. Example of combined information overlay.

III. IO & the MDMP

Ref: FM 3-13, Information Operations (Dec '16), pp. 4-2 to 4-29.

Commanders use the MDMP to understand the situation and mission confronting them and make informed decisions resulting in an operations plan or order for execution. Their personal interest and involvement is essential to ensuring that IO planning is integrated into MDMP from the beginning and effectively supports mission accomplishment.

See pp. 2-22 to 2-25 for related discussion of IO planning as related to the joint planning process (JPP).

IO planning is integral to several other processes, to include intelligence preparation of the battlefield (IPB) and targeting. The G-2 (S-2) and fire support representatives participate in the IO working group and coordinate with the IO officer to integrate IO with their activities and the overall operation.

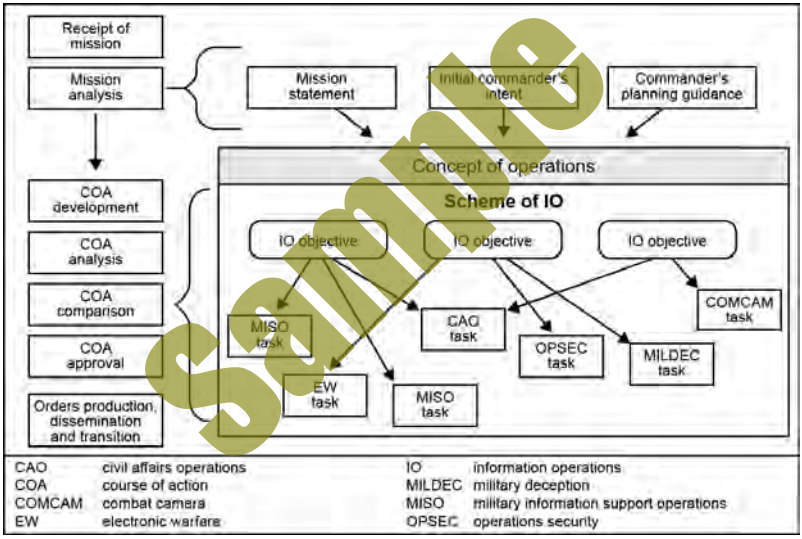


Figure 4-1. Relationship among the scheme of IO, IO objectives, and IRC tasks.

Commanders use their mission statement for the overall operation, the IO mission statement, scheme of IO, IO objectives, and IRC tasks to describe and direct IO, as seen in fig. 4-1. *See pp. 4-3 to 4-16 for in-depth discussion IO mission statement, scheme of IO, IO objectives, and IRC tasks (synchronization of IRCs).*

Refer to BSS6: The Battle Staff SMARTbook, 6th Ed. for further discussion. BSS6 covers the operations process (ADP 5-0); commander's activities; Army planning methodologies; the military decisionmaking process and troop leading procedures (FM 7-0 w/Chg 2); integrating processes (IPB, information collection, targeting, risk management, and knowledge management); plans and orders; mission command, C2 warfighting function tasks, command posts, liaison (ADP 6-0); rehearsals & after action reviews; and operational terms and military symbols (ADP 1-02).

Scheme of IO *See pp. 4-12 to 4-13.*

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 support overall operations and achieve the mission. Based on the commander's planning guidance, to include IO weighted efforts, the IO officer develops a separate scheme of IO for each course of action (COA) the staff develops. IO schemes of support are written in terms of IO objectives—and their associated weighted efforts—and IRC tasks required to achieve these objectives. For example, the overall scheme may be oriented primarily on defending friendly information but also include attack and stabilize objectives.

IO Objectives *See pp. 4-14 to 4-15.*

IO objectives express specific and obtainable outcomes or effects that commanders intend to achieve in and through the information environment. In addition to be being specific, these objectives are measurable, achievable, relevant, and time-bounded (or SMART), which facilitates their attainment and assessment (see chapter 8). IO objectives serve a function similar to that of terrain or force-oriented objectives in maneuver operations. They focus the IO effort on achieving synchronized IRC effects, at the right time and place, to accomplish the unit's mission and support the commanders' intent and concept of the operation.

Accurate situational understanding is key to establishing IO objectives. Operational- and tactical-level IO objectives must nest with strategic theater objectives. Joint and component staffs develop IO objectives to help integrate and synchronize their campaigns and major operations.

The IO officer develops objectives as part of developing the scheme of IO during COA development. These objectives help the staff determine tasks to subordinate units during COA development and analysis.

IRC Tasks *See pp. 4-14 to 4-15.*

Tasks are developed to support accomplishment of one or more IO objectives. These tasks are developed specifically for a given IRC. In concert with IRC representatives, the IO officer develops tasks during COA development and finalizes them during COA analysis. During COA development and COA analysis, tasks are discussed in general terms but not assigned to a subordinate unit. During orders production, these tasks are assigned to IRC units.

Step I. Receipt of Mission

Upon receipt of a mission, the commander and staff perform an initial assessment. Based on this assessment, the commander issues initial guidance and the staff prepares and issues a warning order (WARNORD). Between receiving the commander's initial guidance and issuing the WARNORD, the staff performs receipt of mission actions.

See pp. 4-48 to 4-49 for a summary of the inputs, actions and outputs required of the IO officer during mission analysis.

During receipt of mission, the IO officer—

- Reviews and updates the running estimate.
- Participates in the initial assessment.
- Provides input to the commander's initial guidance.
- Provides input to the warning order.
- Prepares for subsequent planning.

See facing page for an overview of the running estimate. See also pp. 4-6 to 4-7 for more in-depth discussion.

A. Review and Update the Running Estimate

Ref: FM 3-13, Information Operations (Dec '16), p. 4-4. (See also pp. 4-6 to 4-7.)

Running estimates are integral to IO planning. A running estimate is the continuous assessment of the current situation, and is 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.

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 WARNORDs as required during planning and ultimately to draft applicable IO sections of the operation order (OPORD) or operation plan (OPLAN).

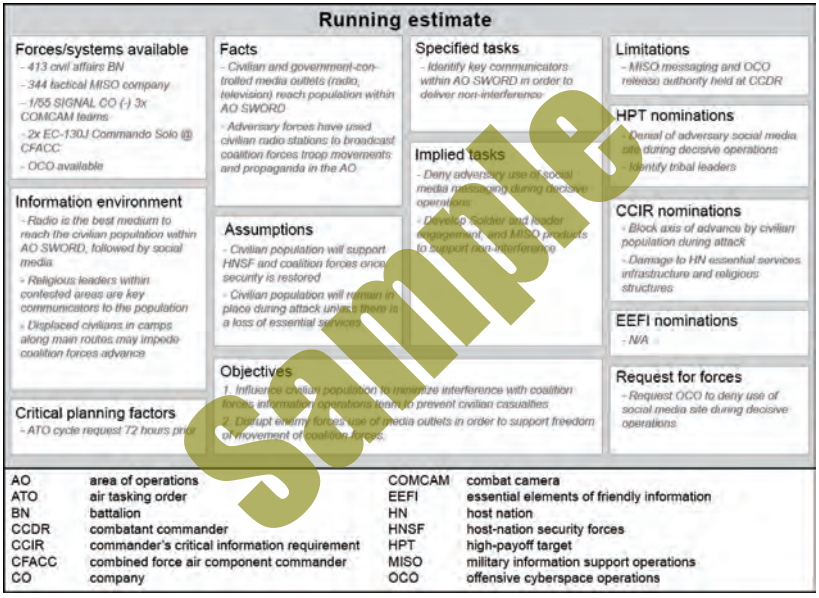


Figure 4-2. Example graphical IO running estimate.

Variations on the standard, narrative format, such as the example provided in figure 4-2, 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 graphical 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 graphical format enables the element to brief the commander and staff with a single slide.

Running estimate development never stops. The IO officer continuously 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. If regionally aligned, the unit prepares its estimate based on research and analysis of the information environment within its region and anticipated mission sets.

B. Participate in Commander's Initial Assessment

Initial assessment primarily focuses on time and resources available to plan, prepare and begin execution of an operation. The IO officer assesses readiness to participate in ADM and MDMP, as well as what external support might be necessary to ensure effective IO planning.

During the initial assessment, the IO officer establishes a battle rhythm, including locations, times, preparation requirements, and the anticipated schedule. Upon receiving a new mission, the IO officer begins gathering planning tools, including a copy of the higher command OPLAN or OPORD, maps of the area of operations, appropriate references, and the running estimate. During initial assessment, the IO officer also coordinates with organic, assigned, and available IRCs and subordinate units to gauge their planning readiness.

Initial time allocation is important to IO because some operations and activities require significant time to produce effects or for assessment. The time available may be a limiting factor for some IRCs. The IO officer identifies activities for which this is the case and includes these limitations in estimates and recommendations.

The commander determines when to execute time-constrained MDMP. Under time-constrained conditions, the IO officer relies on existing tools and products, either his or her own or those of higher headquarters. The lack of time to conduct reconnaissance requires planners to rely more heavily on assumptions and increases the importance of routing combat information and intelligence to the people who need it. A current running estimate is essential to planning in time-constrained conditions.

C. Provide Input to Commander's Initial Guidance

Commanders include IO-specific guidance in their initial guidance, as required. Examples include authorized movements of IRCs, initiation of information collection necessary to support IO, and delineation of IRs.

D. Provide Input to the Initial Warning Order

A WARNORD is issued after the commander and staff have completed their initial assessment and before mission analysis begins. It includes, at a minimum, the type and general location of the operation, initial timeline, and any movements or reconnaissance that need to be initiated. When they receive the initial WARNORD, subordinate units begin parallel planning.

Parallel planning and collaborative planning are routine MDMP techniques. The time needed to achieve and assess effects in the information environment makes it especially important to successful IO. Effective parallel or collaborative planning requires all echelons to share information fully as soon as it is available. Information sharing includes providing higher headquarters plans, orders, and guidance to subordinate IO officers or representatives.

Because some IRCs require a long time to plan or must begin execution early in an operation, follow-on WARNORDs may include detailed IO information. Although the MDMP includes three points at which commanders issue WARNORDs, the number of WARNORDs is not fixed. WARNORDs serve a purpose in planning similar to that of a fragmentary order (FRAGORD) during execution. Commanders issue both, as the situation requires. Possible IO officer input to the initial WARNORD includes:

- Tasks to subordinate units and IRCs for early initiation of approved IO actions, particularly for military deception operations and MISO.
- Essential elements of friendly information (EEFIs) to facilitate defend weighted efforts and begin the OPSEC process.
- Known hazards and risk guidance.
- Military deception guidance and priorities.

Mission Analysis (Summary of IO Inputs, Actions & Outputs)

Ref: FM 3-13, Information Operations (Dec '16), table 4-1, pp. 4-14 to 4-18.

Table 4-1 provides a summary of the inputs, actions and outputs required of the IO officer. Only those sub-steps within mission analysis with significant IO activity are listed.

MDMP Sub Step	Inputs	IO Officer Actions	IO Officer Outputs
Conduct IPB	• Higher HQ IPB • Higher HQ running estimates • Higher HQ OPLAN or OPORD • Higher HQ combined information overlay	• Develop IPB products • Analyze and describe the information environment in the unit's area of operations and its effect on friendly, neutral, adversary, and enemy information efforts • Identify threat information capabilities and vulnerabilities • Identify gaps in current intelligence on threat information efforts • Identify IO-related high-value targets • Determine probable threat information-related COAs • Assess the potential effects of IO on friendly, neutral, adversary, and enemy operations • Determine threat's ability to collect on friendly critical information • Determine additional EEFIs (OPSEC)	• Input to IPB products • IRs to G-2 (S-2), as well as the foreign disclosure officer • Refined EEFIs (OPSEC)
Determine Specified, Implied, and Essential Tasks	• Specified tasks from higher HQ OPLAN or OPORD • IPB and combined information overlay products	• Identify specified tasks in the higher HQ OPLAN or OPORD • Develop implied tasks • Determine if there are any essential tasks • Develop input to the command targeting guidance • Assemble critical and defended asset lists, especially low density delivery systems • Determine additional EEFIs (OPSEC)	• Specified, implied and essential tasks • List of IRCs to G-3 (S-3) • Input to command targeting guidance • Refined EEFIs (OPSEC)
Review Available Assets	• Current task organization for information related capabilities • Higher HQ task organization for information related capabilities • Status reports • Unit standard operating procedure	• Identify friendly IRCs (include capabilities that are joint, interorganizational, and multinational) • Analyze IRC command and support relationships • Determine if available IRCs can perform tasks necessary to support lines of operation or effort • Identify additional resources (such as air assets) needed to execute or support IO	• List of available IRCs [IO running estimate paragraph 1b(4)] • Request for additional IRCs, if required
Determine Constraints	• Commander's initial guidance • Higher HQ OPLAN or OPORD	• Identify IO-related constraints	• List of constraints (IO appendix to Annex C; scheme of IO or coordinating instructions)

MDMP Sub Step	Inputs	IO Officer Actions	IO Officer Outputs
Identify Critical Facts and Develop Assumptions	• Higher HQ OPLAN or OPORD • Commander's initial guidance • Observations and reports	• Identify facts and assumptions affecting IRCs • Submit IRs that will confirm or disprove assumptions • Identify facts and assumptions regarding OPSEC indicators that identify vulnerabilities	• List of facts and assumptions (IO running estimate paragraph 1c.) • IRs that will confirm or disprove facts and assumptions
Begin Risk Management	• Higher HQ OPLAN or OPORD • IPB • Commander's initial guidance	• Identify and assess hazards associated with IO • Propose controls • Identify OPSEC indicators • Assess risk associated with OPSEC indicators to determine vulnerabilities • Establish OPSEC measures	• List of assessed hazards • Input to risk assessment • Develop risk briefing matrix • List of provisional OPSEC measures
Develop Initial CCIRs and EEFIs	• IO IRs	• Determine information the commander needs in order to make critical decisions concerning IO efforts • Identify IRs to recommend as commander's critical information requirements	• Submit IRs
Determine Initial Information Collection Plan	• Initial IPB • PIRs or IO IRs	• Identify gaps in information needed to support planning, execution, and assessment of early initiation actions • Confirm that the initial information collection plan includes IRs concerning enemy capability to collect EEFIs	
Update Plan for the Use of Available Time	• Revised G-5 (S-5)/G-3 (S-3) plans timeline	• Determine time to accomplish IO planning requirements • Assess viability of planning timeline vis-à-vis higher HQ timeline and threat timeline as determined during IPB • Refine initial time allocation plan	• Timeline (provided to G-5 (S-5), with emphasis on the effect(s) of long-lead time events
Develop Initial Themes and Messages	• Public affairs themes and messages adjusted and refined from higher HQ • MISO actions and messages adjusted and refined from higher HQ	• Assess impact of initial themes and messages on the information environment • Assess whether planned IO effects will reinforce themes and messages • Contribute to development of talking points aimed at influencing perceptions and behaviors	• PA themes/ messages and MISO actions/ messages de-conflicted • Initial list of talking points • IRC actions to disseminate approved messages/ talking points
Issue a Warning Order	• Commander's intent and guidance • Approved restated mission and initial objectives • Mission analysis products	• Prepare input to the warning order. Input may include — - Early tasking to subordinate units - Initial mission statement - OPSEC planning guidance - Reconnaissance and surveillance tasking • Military deception guidance	• Input to mission, commander's intent, commander's critical information requirements, and concept of the operations

COA course of action
EEFI essential element of friendly information
G-2 assistant chief of staff, intelligence
G-3 assistant chief of staff, operations
G-5 assistant chief of staff, plans
HQ headquarters
IO information operations
IPB intelligence preparation of the battlefield
IR information requirements
IRC information related capability
MISO military information support operations
OPLAN operations plan
OPORD operations order
OPSEC operations security
PA public affairs
PIR priority intelligence requirement
S-2 battalion or brigade intelligence officer
S-3 battalion or brigade operations staff officer
S-5 battalion or brigade plans staff officer

Step VI. Course of Action Approval

After completing the COA comparison, the staff identifies its preferred COA and recommends it to the commander in a COA decision briefing, if time permits. The concept of operations for the approved COA becomes the concept of operations for the operation itself. The scheme of IO for the approved COA becomes the scheme of IO for the operation. Once a COA is approved, the commander refines the commander's intent and issues additional planning guidance. The G-3 (S-3) then issues a WARNORD and begins orders production.

The WARNORD issued after COA approval contains information that executing units require to complete planning and preparation. Possible IO input to this WARNORD includes:

- Contributions to the commander's intent/concept of operations.
- Changes to the CCIRs.
- Additional or modified risk guidance.
- Time-sensitive reconnaissance tasks.
- IRC tasks requiring early initiation.
- A summary of the scheme of IO and IO objectives.

During the COA decision briefing, the IO officer is prepared to present the associated scheme of IO for each COA and comment on the COA from an IO perspective. If the IO officer perceives the need for additions or changes to the commander's intent or guidance with respect to IO, they ask for it.

MDMP Step	*Inputs*	*IO Officer Actions*	*IO Officer Outputs*
Course of Action Approval	• Updated IO running estimate • Evaluated COAs • Recommended COAs • Updated assumptions	• Provide input to COA recommendation • Re-evaluate input to the commander's intent and guidance • Refine scheme of IO, objectives, and tasks for approved COA and update synchronization matrix • Prepare input to the WARNORD • Participate in the COA decision briefing • Recommend the COA that IO can best support • Request decision on executing any OPSEC measures that entail significant resource expenditure or high risk	• Finalized scheme of IO for approved COA • Finalized tasks based on approved COA • Input to WARNORD • Updated synchronization matrix
COA course of action **IO** information operations **MDMP** military decisionmaking process **WARNORD** warning order			

Step VII. Orders Production, Dissemination, and Transition

Based on the commander's decision and final guidance, the staff refines the approved COA and completes and issues the OPLAN/OPORD. Time permitting, the staff begins planning branches and sequels. The IO officer ensures input is placed in the appropriate paragraphs of the base order and its annexes, especially the IO appendix to the operations annex. When necessary, the IO officer or appropriate special staff officers prepare appendixes for one or more IRCs/

See p. 4-61 for table 4-6 (summary of IO inputs to orders production, dissemination and transition) along with an annotated format of appendix 15 (Information Operations) to Annex C (Operations).

Appendix 15 (IO) to Annex C (Operations)

Ref: FM 3-13, Information Operations (Dec '16), fig. A-1. Appendix 15 (IO) to Annex C (Operations).

[CLASSIFICATION]

Place the classification at the top and bottom of every page of the OPLAN or OPORD. Place the classification marking at the front of each paragraph and subparagraph in parentheses. Refer to AR 380-5 for classification and release marking instructions.

Copy ## of ## copies
Issuing headquarters
Place of issue
Date-time group of signature
Message reference number

Include heading if attachment is distributed separately from the base order or higher-level attachment.

APPENDIX 15 (INFORMATION OPERATIONS) TO ANNEX C (OPERATIONS) TO OPERATION PLAN/ORDER [number] [(code name)]- [issuing headquarters] [(classification of title)]

(U) **References**: Refer to higher headquarters· OPLAN or OPORD and identify map sheets for operation (optional). Add any other specific references to IO if needed.

1. (U) **Situation**. *Include information affecting information operations (IO) that paragraph 1 of the OPLAN or OPORD does not cover or that needs expansion.*

a. (U) Area of Interest. *Describe the information environment as it relates to IO. Refer to Tab 1 (Combined Information Overlay) to Appendix 15 (Information Operations) to Annex C (Operations) as required.*

b. (U) Area of Operations. *Refer to Appendix 2 (Operation Overlay) to Annex C (Operations).*

(I) (U) Information Environment. *Describe the physical. informational. and cognitive dimensions of the information environment that affect IO. Refer to Tab 1 (Combined Information Overlay) to Appendix 15 (Information Operations) to Annex C (Operations) as required.*

(2) (U) Weather. *Describe aspects of weather that impact information operations. Refer to Annex B (Intelligence) as required*

c. (U) Enemy Forces. *List known and templated locations and activities of enemy information unitsfor one echelon up and two echelons down. List enemy maneuver and information-related capabilities that will impact friendly operations. State probable enemy courses of action and employment of enemy information assets. Describe the informational and cognitive dimensions of the information environment that affect enemy actions. Refer to Tab 1 (Combined Information Overlay) to Appendix 15 (Information Operations) to Annex C (Operations) as required.*

d. (U) Friendly Forces. *Outline the higher headquarters· plan as it pertains to IO. List designation. location. and outline of plan of higher. adjacent. and other jUnctional area assets that support or impact the issuing headquarters or require coordination and additional support. Identify friendly IO/IRC assets and resources that affect subordinate commander IO planning. Identify friendly forces IO vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the information environment especially if conducting joint or multinational operations. Identijj; and deconflict IRC employment and information environment effects.*

[page number]
[CLASSIFICATION]

e. (U) Interagency Intergovernmental and Nongovernmental Organizations. *Identify and describe other organizations in the area of operations that may impact the conduct of IO or implementation of IO-specific equipment and tactics.*

f. (U) Civil Considerations. *Describe critical aspects of the civil situation that impact IO. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to Annex B (Intelligence) and Annex K (Civil Affairs Operations) as required Also refer to Tab 1 (Combined Information Overlay) to Appendix 15 (Information Operations) to Annex C (Operations) as required.*

g. (U) Attachments and Detachments. *List IRCs or IO units only as necessary to clarify task organization. Examples include Tactical MISO Teams, Mobile Public Affairs Detachments, and Visual Information Teams. Refer to Annex A (Task Organization) as required.*

h. (U) Assumptions. *List any IO-specific assumptions.*

2. (U) **Mission**. *State the IO mission.*

3. (U) **Execution**.

a. (U) Scheme of Support. *Describe how IO supports the commander's intent and concept of operations. Establish the priorities of support to unitsfor each phase of the operation. Establish IO objectives to employ IRCs to achieve the desired endstate. Describe how IO weighted efforts will support offense, defense, and stability tasks. Identify target sets and effects, by priority. Describe the general conceptfor the integration of IO. List the staff sections, elements, and working groups responsible for aspects of IO. Include IO collection methodsfor information developed in staff sections, elements, and working groups outside the IO element and working group. Ensure subordinate units and higher headquarters receive the IO synchronization plan. Describe the plan for the integration of unified action and nongovernmental partners and organizations. Refer to Annex C (Operations) as required This section is designed to provide insight and understanding a/how IO is integrated across the operational plan.*

b. (U) Assessment. *Describe the priorities for assessment and Identify the measures of performance and effectiveness and indicators used to assess information operations objectives against end state conditions. Refer to Annex M (Assessment) as required.*

c. (U) Tasks to Subordinate Units. *List IO tasks assigned to specific subordinate units not contained in the base order.*

d. (U) Coordinating Instructions. *List only IO instmctions applicable to two or more subordinate units not covered in the base order. Identify and highlight any IO-specific rules of engagement risk reduction control measures, environmental considerations, coordination requirements between units, and CCIRs and EEFIs that pertain to IO.*

4. (U) **Sustainment**. Identify priorities of sustainment for IO key tasks and speciJj; additional instructions as required Refer to Annex F (Sustainment) as required

a. (U) Logistics. *Use subparagraphs to Identify priorities and specific instruction for logistics pertaining to IO. See Appendix 1 (Logistics) to Annex F (Sustainment) and Annex P (Host-Nation Support) as required.*

b. (U) Personnel. *Use subparagraphs to Identify priorities and specific instruction for human resources support pertaining to IO. See Appendix 2 (personnel Services Support) to Annex F (Sustainment) as required.*

c. (U) Health System Support. *See Appendix 3 (Army Health System Support) to Annex F (Sustainment) as required*

Continued on next page

Continued on next page

(Information Operations) V. Battle Drills

Ref: FM 3-13, Information Operations (Dec '16), pp. 4-1 to 4-2.

FM 3-13 describes **battle drills as 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.

IO Battle Drills

Identify Critical Events

Define Information End State

Develop Battle Drill Scheme of Information Operations

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.

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.

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—

Chap 5

(Information Operations) PREPARATION

Ref: FM 3-13, Information Operations (Dec '16), chap. 5.

Preparation consists of those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0). Preparation creates conditions that improve friendly force opportunities for success. Because many IO objectives and IRC tasks require long lead times to create desired effects, preparation for IO often starts earlier than for other types of operations. Initial preparation for specific IRCs and IO units (such as 1st IO Command or a Theater IO Group) may begin during peacetime.

I. IO Preparation Activities

Peacetime preparation by units or capabilities involves building contingency plan databases about the anticipated area of operations. These databases can be used for IO input to IPB and to plan IO to defend friendly intentions, such as network protection and operations security (OPSEC). IO portions of contingency plans are continuously updated. Normal IO working group participants maintain their own data to provide the IO officer with the latest information.

During peacetime, IO officers prepare for future operations by analyzing anticipated area(s) of operations' information environment and likely threat information capabilities. Examples of factors to consider include, but are not limited to—

- Religious, ethnic, and cultural mores, norms, and values.
- Non-military communications infrastructure and architecture.
- Military communication and command and control infrastructure and architecture.
- Military training and level of proficiency (to determine susceptibility to denial, deception, and IO).
- Literacy rate.
- Formal and informal organizations exerting influence and leaders within these organizations.
- Ethnic factional relationships and languages.

Preparation includes assessing unit readiness to execute IO. Commanders and staffs monitor preparations and evaluate them against criteria established during planning to determine variances. This assessment forecasts the effects these factors have on readiness to execute the overall operation as well as individual IRC tasks.

Preparation for IO takes place at three levels: staff (IO officer), IRC units or elements, and individual. The IO officer helps prepare for IO by performing staff tasks and monitoring preparations by IRC units or elements. These units perform preparation activities as a group for tasks that involve the entire unit, and as individuals for tasks that each soldier and leader must complete.

Refer to BSS6: The Battle Staff SMARTbook, 6th Ed. (Plan, Prepare, Execute, & Assess Military Operations), pp. 1-48 to 1-51 for further discussion of preparation activities from ADP 5-0 (2019). Specific discussion includes preparation activities commanders, units, and Soldiers conduct to ensure the force is protected and prepared for execution. See also p. 5-7 for discussion of preparation fundamentals from ADP 5-0.

Chapter 3 of ADP 5-0 provides a comprehensive overview of preparation activities. The activities most relevant to conducting IO include—

- Improve situational understanding.
- Revise and refine plans and orders.
- Conduct coordination and liaison.
- Initiate information collection.
- Initiate security operations.
- Initiate troop movements.
- Initiate network preparation.
- Manage and prepare terrain.
- Conduct confirmation briefs.
- Conduct rehearsals.

A. Improve Situational Understanding

The IO officer/element must understand and share their understanding of the information environment with the commander and staff. During preparation, information collection begins, which helps to validate assumptions and improve situational understanding. Coordination, liaison, and rehearsals further enhance this understanding. Given the information environment's complexity, this task is never-ending and depends on everyone, not just the IO officer, to update and refine understanding of the information environment.

B. Revise and Refine Plans and Orders

Plans are not static; the commander adjusts them based on new information. This information may be the result of analysis of unit preparations, answers to IO IRs, and updates of threat information capacity and capability.

During preparation, the IO officer adjusts the relevant portions of the operation plan (OPLAN) or operation order (OPORD) to reflect the commander's decisions. The IO officer also updates the IO running estimate so that it contains the most current information about adversary information activities, changes in the weather or terrain, and friendly IRCs.

The IO officer ensures that IO input to IPB remains relevant throughout planning and preparation. To do this, they ensure that IO input to the information collection plan is adjusted to support refinements and revisions made to the OPLAN/OPORD.

IO preparation begins during planning. As the IO appendix begins to take shape, IO officer coordination with other staff elements is vital because IO affects every other warfighting function. For example, planning an attack on a command and control (C2) high-payoff target requires coordination with the targeting team. A comprehensive attack offering a high probability of success may involve air interdiction and therefore needs to be placed on the air tasking order. It may involve deep attack: rocket and missile fires have to be scheduled in the fire support plan. Army jammers and collectors have to fly the missions when and where needed. The IO officer ensures the different portions of the OPLAN/OPORD contain the necessary coordinating instructions for these actions to occur at the right time and place.

Effective IO is consistent at all echelons. The IO officer reviews subordinate unit OPLANs/OPORDs to ensure IO has been effectively addressed and detect inconsistencies. The IO officer also looks for possible conflicts between the command's OPLAN/OPORD and those of subordinates. When appropriate, the IO officer reviews adjacent unit OPLANs/OPORDs for possible conflicts. This review allows the IO officer to identify opportunities to mass IO effects across units.

Chap 6

(Information Operations) EXECUTION

Ref: FM 3-13, Information Operations (Dec '16), chap. 6.

Execution is the act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0). In execution, commanders, staffs, and subordinate commanders focus their efforts on translating decisions into actions. They direct action to apply combat power at decisive points and times to achieve objectives and accomplish missions. Inherent in execution is deciding whether to execute planned actions (such as phases, branches, and sequels) or to modify the plan based on unforeseen opportunities or threats.

Execution of IO includes IRCs executing the synchronization plan and the commander and staff monitoring and assessing their activities relative to the plan and adjusting these efforts, as necessary. The primary mechanism for monitoring and assessing IRC activities is the IO working group. There are two variations of the IO working group. The first monitors and assesses ongoing planned operations and convenes on a routine, recurring basis. The second monitors and assesses unplanned or crisis situations and convenes on an as-needed basis.

I. Information Operations Working Group

The IO working group is the primary means by which the commander, staff and other relevant participants ensure the execution of IO. The IO working group is a collaborative staff meeting led by the IO officer, and periodically chaired by the G-3 (S-3), executive officer, chief of staff or the commander. It is a critical planning event integrated into the unit's battle rhythm.

Purpose

The IO working group is the primary mechanism for ensuring effects in and through the information environment are planned and synchronized to support the commander's intent and concept of operations. This means that the staff must assess the current status of operations relative to the end state and determine where efforts are working well and where they are not. More specifically, they must ensure targets are identified and nominated at the right place and time to achieve decisive results. The IO working group occurs regularly in the unit's battle rhythm and always before the next targeting working group. The only exception is a crisis IO working group (also referred to as consequence management or crisis action working group), which occurs as soon as feasible before or after an event or incident that will significantly alter the information environment and give the threat operational advantage unless handled quickly and adeptly.

Inputs/Outputs

The example in figure 6-1 *(following page)* is not exhaustive. In terms of inputs, it identifies those documents, products, and tools that historically and practically have provided the IO working group the information necessary to achieve consensus and make informed recommendations to the G-3 (S-3) and commander. The outputs listed are those considered essential to ensuring the staff can effectively conduct IO.

One tool that the IO working group uses to affirm and adjust the synchronized employment of IRCs is the IO synchronization matrix. An updated synchronization matrix is the working group's key output and essential input to the next targeting meeting. *See p. 4-16.*

Information Execution

IO Working Group

Roles & Responsibilities

Ref: FM 3-13, Information Operations (Dec '16), table 6-1, pp. 6-3 to 6-4.

Representative	Responsibility
Information Operations	• Distribute read-ahead packets • Lead working group • Establish and enforce agenda • Lead information environment update • Recommend commander's critical information requirements • Keep records, track tasks, and disseminate meeting notes
Cyber Electromagnetic Activities	• Provide cyber electromagnetic activities-related information and capabilities to support information operations analysis and objectives • Coordinate, synchronize and deconflict information operations efforts with cyberspace electromagnetic activities efforts or cyberspace electromagnetic activities efforts with information operations efforts
Military Information Support Operations	• Advise on both psychological effects (planned) and psychological impacts (unplanned) • Advise on use of lethal and nonlethal means to influence selected audiences to accomplish objectives • Develop key leader engagement plans • Monitor and coordinate assigned, attached, or supporting military information support unit actions • Identify status of influence efforts in the unit, laterally, and at higher and lower echelons • Provide target audience analysis
G-2 (S-2)	• Provide an intelligence update • Brief information requirements and priority information requirements • Develop the initial information collection plan • Provide foreign disclosure-related guidance and updates
G-3 (S-3)	• Provide operations update and significant activity update • Task units or sections based on due outs • Update fragmentary orders • Maintain a task tracker
Subordinate unit information operations	• Identify opportunities for information operations support to lines of effort • Provide input to assessments • Provide input to information environment update
Public Affairs	• Develop media analysis products • Develop media engagement plan • Provide higher headquarters strategic communication plan • Provide changes to themes and messages from higher headquarters • Develop command information plan
G-9 (S-9)	• Provides specific country information • Ensures the timely update of the civil component of the common operational picture through the civil information management process • Advise on civil considerations within the operational environment • Identify concerns of population groups within the projected joint operational area/area of operations and potential flash points that can result in civil instability • Provide cultural awareness briefings • Advise on displaced civilians movement routes, critical infrastructure, and significant social, religious, and cultural shrines, monuments, and facilities • Advise on information impacts on the civil component • Identify key civilian nodes
Information-related capabilities (IRCs) representatives	• Serve as subject-matter expert for their staff function or capability • Identify opportunities for information-related capability support to lines of effort or operations

Agenda

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 4-3 to 4-4.

The IO working group has a purpose, agenda and proposed timing, inputs and outputs, and structure and participants. Figure 4-1 below 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.

IO Working Group (Agenda/Components)

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 } • Review and update synchronization matrix	6 min
	Part 3: Defend efforts } • Guidance and comments	12 min
	Part 4: Attack efforts }	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

Ref: ATP 3-13.1, fig. 4-1. Components of an information operations working group.

I. IO Weighted Efforts and Enabling Activities

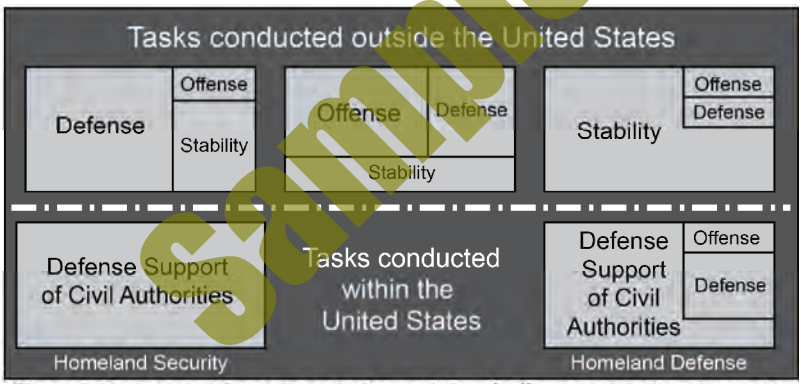
Ref: FM 3-13, Information Operations (Dec '16), chap. 2.

Unified Land Operations

Unified land operations applies land power as part of unified action to defeat the threat on land and establish conditions that achieve the joint force commander's end state. **Combat power** is the primary means by which Army forces apply land power. IO synchronization supports combat power by harnessing the information element to optimize the warfighting functions and leadership. In turn, this optimization enables commanders to seize the initiative through decisive action.

Unified land operations span the entire competition continuum. They are conducted to support all four **Army strategic roles**. The relative emphasis on the various elements of decisive action vary with the purpose and context of the operations being conducted.

See pp. 1-17 to 1-26 for discussion of how IO supports the four Army strategic roles from ADP 3-13.1 (Oct '18). See pp. 1-11 to 1-16 for discussion of information as an element of combat power.



The mission determines the relative weight of effort among the elements.

Ref: ADP 3-0, Operations (Jul '19), fig. 3-1. Decisive action.

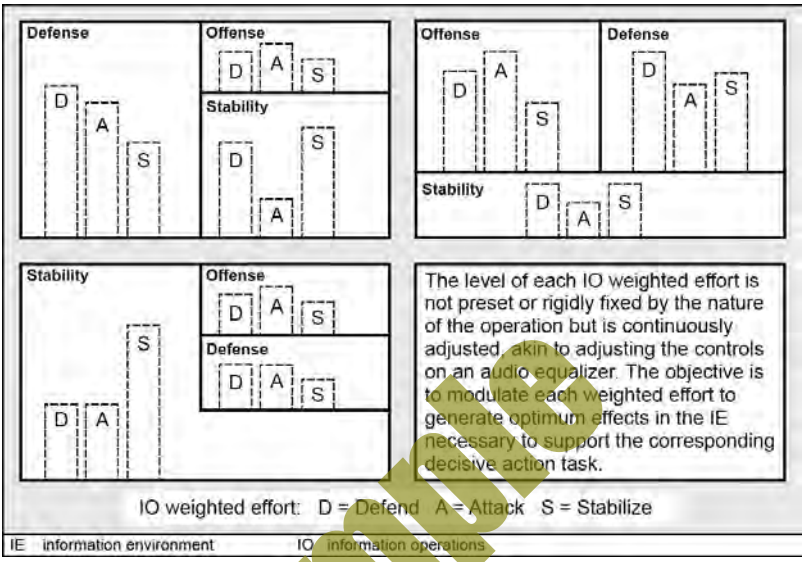
Decisive Action

Decisive action is the continuous, simultaneous combination of offensive, defensive, and stability or defense support of civil authorities tasks (ADRP 3-0). IO contributes to decisive action through the **continuous and simultaneous combination and synchronization of IRCs** in support of offense, defense, and stability tasks. IO itself is not offensive, defensive, or stabilizing, but contributes to all of these simultaneously by **weighting its efforts** in such a way that it achieves requisite effects in and through the information environment in support of the commander's intent.

See following pages for discussion of IO weighted efforts in decisive action.

I. Weighted Efforts

IO weighted efforts are broad orientations used to focus the integration and synchronization of IRCs to **create effects that seize, retain, and exploit the initiative in the information environment**. Commanders, supported by their staffs, visualize and describe how IO will support the concept of operations by aligning and balancing the efforts of **defend, attack, and stabilize** with corresponding decisive action tasks as shown below.



Ref: FM 3-12, fig. 2-1. IO weighted efforts. See following pages (pp. 6-11 to 6-13) for further discussion of IO weighted efforts: defend, attack, and stabilize.

IO and Defense Support of Civil Authorities (DSCA)

IO does not participate in defense support of civil authorities. However, if requested by civil authorities and approved by the Secretary of Defense, select IRCs may support civil authorities in the conduct of their operations.

To support decisive action effectively, the commander and staff undertake three enabling activities—analyze and depict the information environment, determine IRCs and IO organizations available, and optimize IRC effects. These activities start with understanding and visualizing the information environment in all its complexity. They progress to determining the array of IRCs and IO organizations available to affect the information environment. They culminate with optimizing IRC effects through effective planning, preparation, execution and assessment.

II. IO Enabling Activities

To support decisive action, as well as accomplish IO's purpose, commanders, staffs, and in particular, the IO officer or representative, undertake and accomplish three enabling activities:

- Analyze and depict the information environment in all its complexity.
- Determine the array of IRCs and IO organizations (such as Theater IO Groups) available to affect the information environment and the advantages each offers.
- Optimize the effects of IRCs through effective planning, preparation, execution, and assessment.

See p. 6-14 for further discussion of these IO enabling activities.

(IO Weighted Effort)
A. DEFEND

Ref: FM 3-13, Information Operations (Dec '16), pp. 2-1 to 2-2.

When the IO effort necessitates a defend orientation, it seeks to create effects in the information environment that accomplish any one or combination of the following (not all inclusive):

Physical Dimension

- Locking or otherwise physically securing documents, equipment and infrastructure that facilitate decision making.
- Protecting documents, equipment, and structures from destruction or degradation.
- Protecting key personnel from attack or exploitation.
- Using obscurants to mask movements.

Informational Dimension

- Encrypting communications.
- Preserving the free-flow of information and access to data and information sources.
- Employing knowledge management principles.
- Proactively identifying instances of social engineering or malware and keeping virus andother protections current.
- Using forensics to determine sources of attack.
- Countering enemy or adversary information efforts.

Cognitive Dimension

- Making decentralized decisions.
- Checking facts and assumptions.
- Using precedents or best practices.
- Using red teaming.

IRCs that are most often synchronized to achieve a defend orientation in the information environment include, but are not limited to:

- Cyberspace operations.
- Electronic warfare.
- Military deception.
- MISO.
- Operations security (OPSEC).
- Physical security.
- Destruction and lethal actions.
- Special technical operations.

Continued on next page

II. Coordination of Intelligence Support

ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 5-1 to 5-3.

I. Intelligence Support to Information Operations

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.

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.

Key Terms

• **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).

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.

Chap 7

I. Fires (IO Considerations)

Ref: ADP 3-19, Fires (Jul '19), chap. 1 and ADP 3-0, Operations (Jul '19), p. 5-5.

Success in large-scale combat operations is dependent on the Army's ability to employ fires. Fires enable maneuver. Over the past two decades, potential peer threats have invested heavily in long-range fires and integrated air defense systems, making it even more critical that the U.S. Army possess the ability to maneuver and deliver fires in depth and across domains.

I. The Fires Warfighting Function

The fires warfighting function is the related tasks and systems that create and converge effects in all domains against the threat to enable actions across the range of military operations (ADP 3-0). **These tasks and systems create lethal and nonlethal effects delivered from both Army and Joint forces, as well as other unified action partners.** The fires warfighting function does not wholly encompass, nor is it wholly encompassed by, any particular branch or function. Many of the capabilities that contribute to fires also contribute to other warfighting functions, often simultaneously. For example, an aviation unit may simultaneously execute missions that contribute to the movement and maneuver, fires, intelligence, sustainment, protection, and command and control warfighting functions. Additionally, air defense artillery (ADA) units conduct air and missile defense (AMD) operations in support of both fires and protection warfighting functions.

Commanders must execute and integrate fires, in combination with the other elements of combat power, to create and converge effects and achieve the desired end state. Fires tasks are those necessary actions that must be conducted to create and converge effects in all domains to meet the commander's objectives. The tasks of the fires warfighting function are:

Integrate Army, multinational, and joint fires through:

- Targeting.
- Operations process.
- Fire support.
- Airspace planning and management.
- **Electromagnetic spectrum management.**
- Multinational integration.
- Rehearsals.
- Air and missile defense planning and integration.

Execute fires across all domains and in the information environment, employing:

- Surface-to-surface fires.
- Air-to-surface fires.
- Surface-to-air fires.
- **Cyberspace operations and EW.**
- **Space operations.**
- Multinational fires.
- Special operations.
- **Information operations.**

See pp. 7-4 to 7-5 for an overview and further discussion.

IV. Joint Fires (IO Considerations)

Ref: JP 3-0 (w/Chg 1), Joint Operations (Oct '18), chap. III.

To employ fires is to use available weapons and other systems to create a specific effect on a target. Joint fires are those delivered during the employment of forces from two or more components in coordinated action to produce desired results in support of a common objective. Fires typically produce destructive effects, but various other tools and methods can be employed with little or no associated physical destruction. This function encompasses the fires associated with a number of tasks, missions, and processes, including:

- **Conduct joint targeting**. This is the process of selecting and prioritizing targets and matching the appropriate response to them, taking account of command objectives, operational requirements, and capabilities.
- **Provide joint fire support**. This task includes joint fires that assist joint forces to move, maneuver, and control territory, populations, space, cyberspace, airspace, and key waters.
- **Countering Air and Missile Threats.** This task integrates offensive and defensive operations and capabilities to achieve and maintain a desired degree of air superiority and force protection. These operations are planned to destroy or negate enemy manned and unmanned aircraft and missiles, both before and after launch.
- **Interdict Enemy Capabilities**. Interdiction diverts, disrupts, delays, or destroys the enemy's military surface capabilities before they can be used effectively against friendly forces or to otherwise achieve their objectives.
- **Conduct Strategic Attack**. This task includes offensive action against targets—whether military, political, economic, or other—which are selected specifically in order to achieve national or military strategic objectives.
- **Employ IRCs**. IRCs are tools, techniques, or activities employed within the information environment to create effects and operationally desirable conditions. In the context of the fires function, this task focuses on the integrated employment of IRCs in concert with other LOOs and LOEs, to **influence, disrupt, corrupt, or usurp an enemy's decision making**.
- **Assess the Results of Employing Fires**. This task includes assessing the effectiveness and performance of fires as well as their contribution to the larger operation or objective.

Joint Fires (Key Considerations Related to IO)

Capabilities That Can Create Nonlethal Effects. Some capabilities can generate nonlethal effects that limit collateral damage, reduce risk to civilians, and may reduce opportunities for enemy or adversary propaganda. They may also reduce the number of casualties associated with excessive use of force, limit reconstruction costs, and maintain the good will of the local populace. Some capabilities are nonlethal by design and include, but are not limited to, blunt impact and warning munitions, acoustic and optical warning devices, and vehicle and vessel stopping systems.

Cyberspace Attack. Cyberspace attack actions create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains.

Electronic Attack (EA). EA involves the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment to degrade, neutralize, or destroy enemy combat capability.

Military Information Support Operations (MISO). MISO convey selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning, and ultimately induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Leveraging Information

Ref: JP 3-0, Joint Operations, w/Chg 1 (Oct '18), pp. III-17 to III-22.

All military activities produce **information**. Informational aspects are the features and details of military activities observers interpret and use to assign meaning and gain understanding. Those aspects affect the perceptions and attitudes that drive behavior and decision making. The JFC leverages informational aspects of military activities to gain an advantage; failing to leverage those aspects may cede this advantage to others. **Leveraging the informational aspects of military activities** ultimately affects strategic outcomes.

Regardless of its mission, the joint force considers the likely impact of all operations on **relevant actor** perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that **create desired effects** that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the **employment of specialized capabilities** -- e.g., key-leader engagements (KLE), cyberspace operations (CO), military information support operations (MISO), electronic warfare (EW), and civil affairs (CA) -- to reinforce the JFC's efforts.

Tasks aligned under this activity apply the JFC's understanding of the impact information has on perceptions, attitudes, and decision-making processes to affect the behaviors of relevant actors in ways favorable to joint force objectives.

Influence Relevant Actors

Regardless of its mission, the joint force considers the likely impact of all operations on relevant actor perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation in ways that create desired effects that include maintaining or inducing relevant actor behaviors. These ways may include the timing, duration, scope, scale, and even visibility of an operation; the deliberately planned presence, posture, or profile of assigned or attached forces in an area; the use of signature management in deception operations; the conduct of activities and operations to similarly impact behavioral drivers; and the employment of specialized capabilities (e.g., KLE, CO, military information support operations [MISO], EW, CA) to reinforce the JFC's efforts. Since some relevant actors will be located outside of the JFC's OA, coordination, planning, and synchronization of activities with other commands or mission partners is vital.

Inform Domestic, International, and Internal Audiences

Inform activities involve the release of accurate information to domestic and international audiences to put joint operations in context; facilitate informed perceptions about military operations; and counter adversarial misinformation, disinformation, and propaganda. Inform activities help to assure the trust and confidence of the US population, allies, and partners and to deter and dissuade adversaries and enemies.

Attack and Exploit Information, Information Networks, and Systems

The joint force attacks and exploits information, information networks, and systems to affect the ability of relevant actors to leverage information in support of their own objectives. This includes the manipulation, modification, or destruction of information or disruption of the flow of information for the purpose of gaining a position of military advantage. This also includes targeting the credibility of information.

See p. 1-19 for related discussion of "information advantage" (positions of relative advantage) and also pp. 2-1 to 2-6, information (as one of the joint functions).

II. Targeting (IO Integration)

Ref: FM 3-13, Information Operations (Dec '16), chap. 7 and ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 5.

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). IO is integrated into the targeting cycle to produce effects in and through the information environment that support objectives. The targeting cycle facilitates the engagement of the right target with the right asset at the right time. The IO officer or representative is a part of the targeting team, responsible to the commander and staff for all aspects of IO.

Targeting Methodology

Army targeting methodology is based on four functions: decide, detect, deliver, and assess (D3A) *(see figure 7-1)*. The decide function occurs concurrently with planning. The detect function occurs during preparation and execution. The deliver function occurs primarily during execution, although some IO-related targets may be engaged while the command is preparing for the overall operation. The assess function occurs throughout.

	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 high priority target list Establish target selection standards Develop AGM Determine criteria of • Successful BDA • Requirements **Orders Production** Finalize high-payoff target list Finalize target selection standards Finalize AGM Submit IO information requirements/requests for information to G-2 (S-2)
	PREPARATION / EXECUTION	DETECT	• Execute collection plan • Update PIRs/IO IRs as they are answered • Update high-payoff target 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; BDA battle damage assessment; COA course of action; HPT high-payoff target; HVT high-value target; IO Information operations; PIR priority intelligence requirements

Ref: FM 3-13, fig. 7-1. The operations process, targeting cycle and IO-related tasks.

The targeting process is cyclical. The command's battle rhythm determines the frequency of targeting working group meetings. IO-related target nominations are developed by the IO officer and by the IO working group, which validates all IO-related targets before they are nominated to the targeting working group. Therefore, the IO working group is always scheduled in advance of the targeting working group.

II. Decide, Detect, Deliver, Assess (D3A)

Army targeting methodology is based on four functions: decide, detect, deliver, and assess (D3A). The decide function occurs concurrently with planning. The detect function occurs during preparation and execution. The deliver function occurs primarily during execution, although some IO-related targets may be engaged while the command is preparing for the overall operation. The assess function occurs throughout.

D - Decide

The decide function is part of the planning activity of the operations process. It occurs concurrently with the military decisionmaking process (MDMP). During the decide function, the targeting team focuses and sets priorities for intelligence collection and attack planning. Based on the commander's intent and concept of operations, the targeting team establishes targeting priorities for each phase or critical event of an operation. The following products reflect these priorities—

- High-payoff target list.
- Information collection plan.
- Target selection standards.
- Attack guidance matrix.
- Target synchronization matrix.

The high-payoff target list is a prioritized list of targets whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets (HPTs) are those high-value targets (HVTs) identified during COA development and validated in subsequent steps that must be acquired and successfully attacked for the success of the friendly commander's mission. Examples of IO-related HPTs are threat command and control nodes and intelligence collection assets/capabilities.

The information collection plan, prepared by the G-3 (S-3) and coordinated with the entire staff, synchronizes the four primary means information collection to provide intelligence to the commander. The G-2 (S-2) ensures all available collection assets provide the required information. Information requirements submitted by the IO officer can require longer lead times to detect targets and dwell times to assess the effects of IRCs directed against these targets.

Target selection standards establish criteria for deciding when targets are located accurately enough to attack. These criteria are often more complicated for IO, especially when attempting to identify actors and audiences with precision.

The attack guidance matrix addresses how and when targets are to be engaged and desired effects of the engagement. For IO-related targets, effects are diverse, running the gamut from destruction of assets to changed behaviors.

The target synchronization matrix is a list of HPTs by category and the agencies responsible for detecting them, attacking them, and assessing the effects of the attacks. It combines data from the high-payoff target list, information collection plan and attack guidance matrix.

The targeting team develops or contributes to these products throughout the MDMP. The commander approves them during COA approval. The IO officer ensures they include information necessary to engage IO-related targets. IO-related vulnerability analyses done by the G-2 (S-2) and IO officer provide a basis for deciding which IO-related targets to attack.

See following pages (pp. 7-16 to 7-21) for further discussion of "Decide" targeting tasks during the MDMP.

D - Detect

This function involves locating HPTs accurately enough to engage them. It primarily entails execution of the information collection plan. All staff agencies, including the IO officer, are responsible for passing to the G-2 (S-2) information collected by their assets that answer IRs. Conversely, the G-2 (S-2) is responsible for passing combat information and intelligence to the agencies that identified the IRs. Sharing information allows timely evaluation of attacks, assessment of IO, and development of new targets. Effective information and knowledge management are, therefore, essential.

The information collection plan focuses on identifying HPTs and answering PIRs. These are prioritized based on the importance of the target or information to the commander's concept of operation and intent. When designated by the commander, PIRs can include requirements concerning IO; obtaining answers to these requirements will assist the IO officer in assessing IO. Thus, there is some overlap between detect and assess functions. Detecting targets for nonlethal attacks may require information collection support from higher headquarters. The targeting team adjusts the high-payoff target list and attack guidance matrix to meet changes as the situation develops. The IO officer submits new IO IRs/RFIs as needed.

During the detect function, the IO officer updates the high-payoff target list and target synchronization matrix. In addition to the information collection plan, the IO officer will use other information sources, particularly culturally-attuned ones that have unique access to or knowledge of the information environment and its various audiences. Examples include atmospheric teams; cultural attaches or advisors; joint, interorganizational or multinational partner cultural experts; interpreters, or indigenous leaders.

D - Deliver

This function occurs primarily during execution, although some IO-related targets may be engaged while the command is preparing for the overall operation. The key to understanding the deliver function is to know which assets are available to perform a specific function or deliver a specific effect and to ensure these assets are ready and capable. Examples of delivery methods include but are not limited to: corps/division/brigade commander, provincial reconstruction team member or other unified action partner, host nation government leader, loudspeaker, media broadcast., social media posts and videos, and patrols.

During this step, the IO officer executes relevant portions of the target synchronization matrix. As IO-related delivery means and methods are multi-faceted and often involve human interaction, this step includes recording the delivery act and keeping detailed accounts or notes of actions taken or the proceedings, discussions, and commitments involved. The IO officer will ensure that required reporting procedures are explained and disseminated in the operations order or as part of the unit's standard operating procedures.

A - Assess

There are multiple types and levels of assessment. Assessment within D3A specifically focuses on whether the commander's targeting guidance was met for a specific target. From an IO perspective, such guidance may speak in terms of influence or degraded decision making, which are difficult to quantify. In the case of engagements, for example, assessment will help determine whether messages were retained by the target, whether these messages resulted in changed behavior, and whether reengagement may be necessary. An ongoing consideration in the information environment is that there may be a significant lag between the time of delivery, the effect taking place, and determination of an effect.

During this step, the IO officer and IRCs evaluate measures of effectiveness and performance to determine if desired effects were achieved. If not, it recommends re-engagement or other actions.

III. Targeting Tasks during the MDMP

Ref: FM 3-13, Information Operations (Dec '16), pp. 7-2 to 7-6.

A. Mission Analysis

The two targeting-related IO products of mission analysis are a list of IO-related HVTs and recommendations for the commander's targeting guidance. The IO officer works with the G-2 (S-2) during IPB to develop IO-related HVTs, and with other members of the targeting team to develop IO targeting guidance recommendations.

Intelligence Preparation of the Battlefield (IPB)

IPB includes preparing templates that portray threat forces and assets unconstrained by the environment. The intelligence cell adjusts threat templates based on terrain and weather to create situational templates that portray possible threat COAs. These situational templates allow the intelligence to identify HVTs. The IO officer works with the intelligence cell throughout IPB to identify threat information-related capabilities and vulnerabilities and other key groups in the area of operations. These capabilities and vulnerabilities become IO-related HVTs.

See pp. 4-17 to 4-34 for related discussion of IO & IPB (information environment analysis).

Targeting Guidance

Issued within the commander's guidance is targeting guidance. This guidance describes the desired effects the commander wants to achieve. IO targeting focuses on HVTs that support critical, information-related threat capabilities that underpin their objectives and are vulnerable to friendly IO exploitation.

The IO officer develops input to targeting guidance based on the initial mission and available and anticipated IRCs. The IO officer identifies the functions, capabilities, or units to be attacked; the effects desired; and the purpose for the attack. The IO officer uses the targeting guidance to select IO-related HPTs from among identified HVTs. These HPTs are confirmed during COA analysis.

Targeting guidance is developed separately from IO objectives. IO objectives are generally broad in scope. They encompass all IO weighted efforts (attack, defend, stabilize). The IO officer develops recommendations for targeting guidance that supports achieving objectives.

When developing IO input to the targeting guidance, the IO officer considers the time required to achieve effects and the time required to determine results. Some IRCs require targeting guidance that allows for the acquisition, engagement, and assessment of targets while the unit is preparing for the overall operation. For example, the commander may want to psychologically and electronically isolate the enemy's reserve before engaging it with fires. Doing this requires electronic attack of threat command and control systems and military information support operations (MISO) directed at the threat 24 to 48 hours before lethal fires are initiated. Successfully achieving IO objectives for this phase of the operation requires targeting guidance that gives IO-related targets the appropriate priority.

B. COA Development

Feasible COAs, that integrate the effects of all elements of combat power, are developed by the staff. The IO officer prepares a scheme of IO that identifies objectives and IRC tasks for each COA. The IRC tasks are correlated with targets on the HVT list. A single IRC or multiple IRCs can be planned against a single HVT.

For each COA, the IO officer identifies HVTs that will support attainment of an IO objective. IO-related HVTs that subsequently support friendly IO objectives, and that can be engaged by IRCs, become HPTs. The targeting team also performs target value analysis, coordinates and deconflicts targets, and establishes assessment criteria. The IO officer participates in each of these tasks.

Target Value Analysis (TVA)

The targeting team performs target value analysis for each COA the staff develops. The initial sources for target value analysis are target spreadsheets and target sheets. Target spreadsheets (target folders) identify target sets associated with adversary functions that could interfere with each friendly COA or that are key to adversary success. IO-related targets can be analyzed as a separate target set or incorporated into other target sets. The IO officer establishes any IO-specific target sets. Each target set is assigned a priority based on its contribution to the success of a friendly objective, its impact on an enemy or adversary COA, and friendly capability to service the target.

The targeting team uses target spreadsheets during the war game to determine which HVTs to attack. The IO officer ensures that target spreadsheets include information on threat capabilities and IO-related HVTs and that the IO target set, if designated, is assigned a value appropriate to IO's relative importance to each friendly COA. If an IO target set is not designated, the IO officer ensures that IO-related targets are assigned an appropriate priority within the target sets used.

Target sheets contain the information required to engage a specific target. Target sheets state how attacking the target affects the threat's operation. The IO officer prepares target sheets for HVTs to analyze them from an IO planning perspective. These HVTs are expressed as target subsets, such as decision makers. Information requirements include:

- What influences these decision makers.
- How they communicate.
- With whom they communicate.
- Weaknesses, susceptibilities, accessibility, feasibility, and pressure points.

Deconflicting and Coordinating Targets

The IO officer and working group consider the possible consequences of attacking any target or target set. Their purpose is to identify possible duplication or attenuation of effects. The attack of physical targets always has second- and third-order effects (informational and cognitive) that could diminish or enhance their value to the overall operation. For example, fires that result in the collateral deaths of civilian non-combatants can have a negative cognitive effect, while using fires to destroy the enemy's fiber network so that it relies on radio communications vulnerable to jamming can have a positive informational effect. Also, the effects achieved by one IRC might compete with or diminish the effects of another IRC. Thus, IRC synchronization and the integration of IO into other lines of effort requires methodical coordination and deconfliction efforts.

IO working group members consider all targets from their various perspectives. Deconfliction in this context means ensuring that engaging a target does not produce effects that interfere with the effects of other IRC tasks or IO-related targets, or otherwise inhibit mission accomplishment. Coordination ensures that the effects of engaging different targets complement each other and further the commander's intent.

IO officers at different echelons may seek to engage the same targets and, possibly, desire different effects. Therefore, IO-focused targeting includes coordinating and deconflicting targets with higher and subordinate units before the targeting working group meets. Some IO-related targets may also be nominated by other staff elements. The IO officer presents the effects required to accomplish the IO objective associated with those targets when the targeting team determines how to engage them. IO officers must also coordinate and deconflict targets with unified action partners whose doctrinal use of IRCs and policies governing their employment differ. Such coordination extends the planning horizon and may limit how IRCs are integrated.

One way to achieve this coordination and deconfliction is by beginning parallel planning as early as possible in the MDMP. This means that the IO officer and the targeting team should share all pertinent information with subordinate units and adjacent and higher headquarters.

Continued on next page

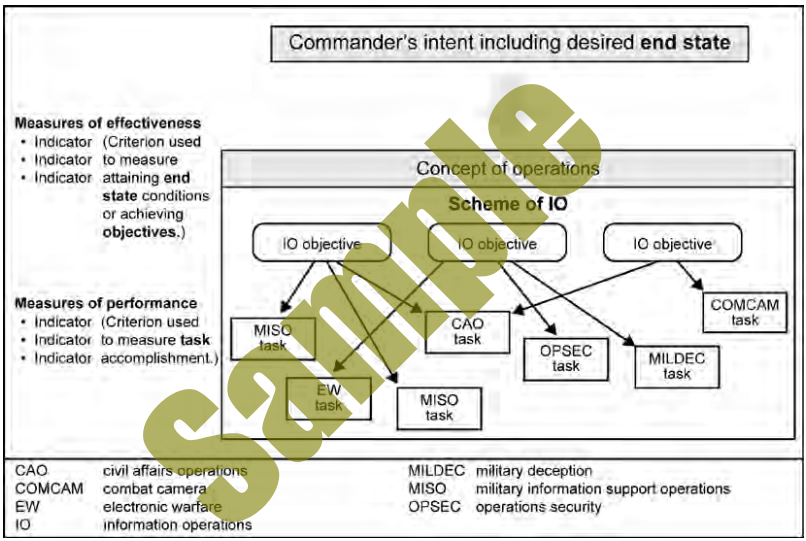
Chap 8

(Information Operations) ASSESSMENT

Ref: ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 6 and FM 3-13, Information Operations (Dec '16), chap. 8.

I. Assessment Framework

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.



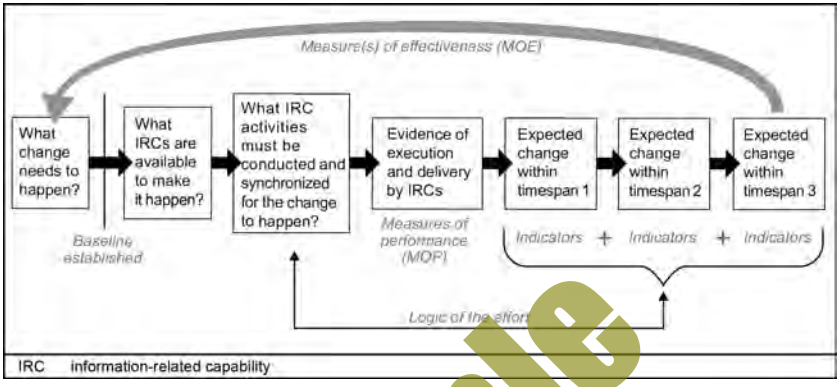
Ref: ATP 3-13.1, fig. 6-1. Framework for assessment.

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.

II. IO Assessment Considerations

Ref: FM 3-13, Information Operations (Dec '16), pp. 8-3 to 8-5. See also pp. 8-7 to 8-9.

Assessment of IO in general and of specific effects in the information environment require careful development of measures of effectiveness and performance, as well as identification of indicators that will best signal achievement of these measures and desired outcomes. Assessment in the information environment is not easy and adherence to the following considerations will aid in making IO assessment more effective.



Ref: FM 3-13, fig. 8-2. Logic flow and components of an IO objective. Figure 8-2 portrays the relationship between objectives (the change that needs to happen) and measures of performance, indicators, and measures of effectiveness. The logic of the effort is shown as a relationship between 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 unique to every objective and combination of IRCs.

Measures of Effectiveness (MOEs)

A measure of effectiveness is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0). Measures of effectiveness help measure changes in conditions, both positive and negative. They are commonly found and tracked in formal assessment plans.

Time is a factor when assessing IO and developing measures of effectiveness. The attainment of IO objectives leading to the commander's desired end state often requires days or months to realize. It is essential, therefore, to have a baseline from which to measure change and also to time-bound the change. Time-bounding makes clear how long it will take before the change is observed. It helps to set necessary expectations, foster patience, and avoid a rush to judgment. If a behavioral objective is anticipated to take considerable time, assessment planning may choose to break the objective into smaller increments, each with more immediate observable outcomes. Finally, it is also important to analyze and understand the cultural relevance of time in the area of operations and account for and adapt to it.

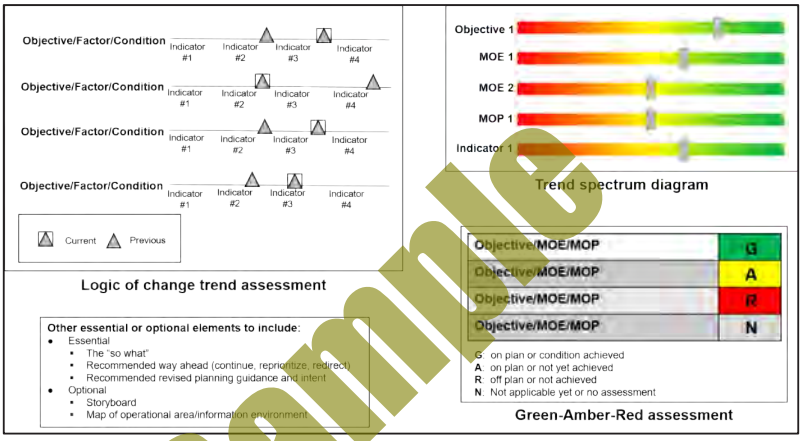
Developing informational, behavioral and sentiment baselines often requires significant time and resource investments. Sentiment baselines, such as those determined through surveys or interviews, may require contracted labor to accomplish. The IO officer must factor in the lead time necessary to contract a third-party, provide it time to develop the survey instrument, administer the survey, and tabulate and report on the results.

Commanders and staffs, particularly the IO officer, must account for the order of effects when assessing IO or, more broadly, any effect. For example, an effect in the physical dimension (1st order) can resonate in unexpected ways in the informational and cogni-

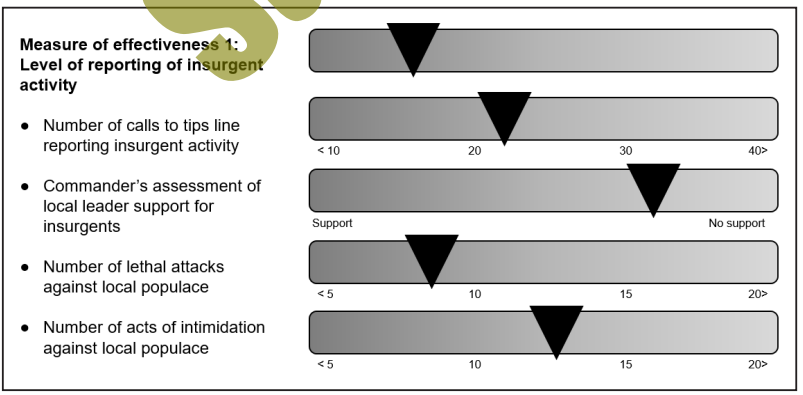
VIII. Assessment Products

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. Campaign assessments are substantially fuller or richer in terms of the scope of information presented than is a task assessment.

As figure 6-5 depicts below, 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. Figure 6-6 illustrates several common methods for depicting trends or the status of a given condition in an information environment. Figure 6-7 provides a counterinsurgency example that depicts indicator trends supporting an MOE.



Ref: ATP 3-13.1, fig. 6-6. Sample assessment product templates



Ref: ATP 3-13.1, fig. 6-7. Example counterinsurgency MOE assessment.

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."

(INFO1) Index

F

G

I

J

S

T

U

V

W

SMARTbooks

INTELLECTUAL FUEL FOR THE MILITARY

Recognized as a "**whole of government**" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a **comprehensive professional library** designed with all levels of Soldiers, Sailors, Airmen, Marines and Civilians in mind.

The SMARTbook reference series is used by **military, national security, and government professionals** around the world at the organizational/ institutional level; operational units and agencies across the full range of operations and activities; military/government education and professional development courses; combatant command and joint force headquarters; and allied, coalition and multinational partner support and training.

SMARTbooks
INTELLECTUAL FUEL FOR THE MILITARY

MILITARY REFERENCE: SERVICE-SPECIFIC

Recognized as a "whole of government" doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.

MILITARY REFERENCE: MULTI-SERVICE & SPECIALTY

SMARTbooks can be used as quick reference guides during operations, as study guides at professional development courses, and as checklists in support of training.

JOINT STRATEGIC, INTERAGENCY, & NATIONAL SECURITY

The 21st century presents a global environment characterized by regional instability, failed states, weapons proliferation, global terrorism and unconventional threats.

The Lightning Press is a **service-disabled, veteran-owned small business,** DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

THREAT, OPFOR, REGIONAL & CULTURAL

In today's complicated and uncertain world, the military must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats.

HOMELAND DEFENSE, DSCA, & DISASTER RESPONSE

Disaster can strike anytime, anywhere. It takes many forms—a hurricane, an earthquake, a tornado, a flood, a fire, a hazardous spill, or an act of terrorism.

DIGITAL SMARTBOOKS (eBooks)

In addition to paperback, SMARTbooks are also available in digital (eBook) format. Our digital SMARTbooks are for use with Adobe Digital Editions and can be used on up to **six computers and six devices**, with free software available for **85+ devices and platforms—including PC/MAC, iPad and iPhone, Android tablets and smartphones, Nook, and more**! Digital SMARTbooks are also available for the **Kindle Fire** (using Bluefire Reader for Android).

Download FREE samples and SAVE 15% everyday at:

www.TheLightningPress.com

Purchase/Order

www.TheLightningPress.com

SMARTsavings on SMARTbooks! Save big when you order our titles together in a SMARTset bundle. It's the most popular & least expensive way to buy, and a great way to build your professional library. If you need a quote or have special requests, please contact us by one of the methods below!

View, download FREE samples and purchase online:

www.TheLightningPress.com

Order SECURE Online

Web: www.TheLightningPress.com

Email: SMARTbooks@TheLightningPress.com

24-hour Order & Customer Service Line

Place your order (or leave a voicemail) at 1-800-997-8827

Phone Orders, Customer Service & Quotes

Live customer service and phone orders available Mon - Fri 0900-1800 EST at (863) 409-8084

Mail, Check & Money Order

2227 Arrowhead Blvd., Lakeland, FL 33813

Government/Unit/Bulk Sales

The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered—to include the SAM, WAWF, FBO, and FEDPAY.

We accept and process both **Government Purchase Cards** (GCPC/GPC) and **Purchase Orders** (PO/PR&Cs).

Keep your SMARTbook up-to-date with the latest doctrine! In addition to revisions, we publish incremental "**SMARTupdates**" when feasible to update changes in doctrine or new publications. These SMARTupdates are printed/produced in a format that allow the reader to insert the change pages into the original GBC-bound book by simply opening the comb-binding and replacing affected pages. Learn more and sign-up at: **www.thelightningpress.com/smartupdates/**

INFO1

thelightningpress.com

(INFO1) The Information Operations & Capabilities SMARTbook

Guide to Information Operations & the IRCs

Over the past two decades, **information operations (IO)** has gone through a number of doctrinal evolutions, explained, in part, by the rapidly changing nature of information, its flow, processing, dissemination, impact and, in particular, its military employment. *INFO1: The Information Operations & Capabilities SMARTbook* examines the most current doctrinal references available and charts a path to emerging doctrine on information operations.

Information is a resource. As a resource, it must be obtained, developed, refined, distributed, and protected. The **information element of combat power** is integral to optimizing combat power, particularly given the increasing relevance of operations in and through the information environment to achieve decisive outcomes.

Information Operations (IO) 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.

An **information-related capability (IRC)** 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. IO brings together information-related capabilities (IRCs) at a specific time and in a coherent fashion to create effects in and through the information environment that advance the ability to deliver operational advantage to the commander.