thelightningpress.com

INFO2 SMARTBOOK

Second Edition (INFO2)

Information Advantage
(Defined & Described)

Information
in Joint Operations

OIE: Operations in the
Information Environment

Information Capabilities
(PA, CA, MILDEC, MISO,
OPSEC, CO, EW, Space, STO)

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

Information Preparation

Information Execution
(Working Group,
Intel Support)

Fires & Targeting

Information Assessment

information advantage

ACTIVITIES, TASKS & CAPABILITIES

The Lightning Press

Norman M Wade

thelightningpress.com

INFO2 SMARTBOOK

information advantage

ACTIVITIES, TASKS & CAPABILITIES

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

INFO2 SMARTbook: Information Advantage (Activities, Tasks & Capabilities)

We no longer regard information as a separate consideration or the sole purview of technical specialists. As a dynamic of combat power, Army forces fight for, defend, and fight with information to create and exploit information advantages—the use, protection, and exploitation of information to achieve objectives more effectively than enemies and adversaries do. INFO2 chapters and topics include information advantage (enable, protect, inform, influence, attack), information in joint operations (OIE: operations in the information environment), information capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO), information planning (information environment analysis, IPB, MDMP, JPP), information preparation, information execution, fires & targeting, and information assessment.

ISBN: 978-1-935886-97-6

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.

(INFO2) Notes to Reader

Information is central to everything we do—it is the basis of intelligence, a fundamental element of command and control, and the foundation for communicating thoughts, opinions, and ideas. Information is the building block for intelligence and is the basis for situational understanding, decision making, and actions across all warfighting functions. As a **critical resource**, Army forces fight for, defend, and fight with information while attacking a threat's (adversary or enemy) ability to do the same.

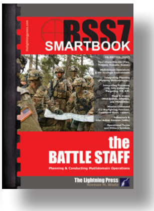
We **no longer regard information as a separate consideration** or the sole purview of technical specialists. Instead, we view information as **a resource that is integrated into operations** with all available capabilities in a **combined arms approach** to **enable** command and control; **protect** data, information, and networks; **inform** audiences; **influence** threats and foreign relevant actors; and **attack** the threat's ability to exercise command and control.

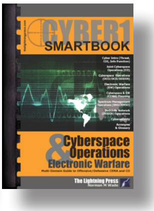
Army forces create and exploit **informational power** similarly to the joint force through five **information activities** (enable, protect, inform, influence, and attack). Army forces also consider information as a dynamic of combat power employed with mobility, firepower, survivability, and leadership to achieve objectives during armed conflict. As a **dynamic of combat power**, Army forces fight for, defend, and fight with information to create and exploit **information advantages**—the use, protection, and exploitation of information to achieve objectives more effectively than enemies and adversaries do.

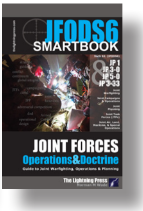
The **joint force** uses information to perform many simultaneous and integrated activities. The joint force employment of information is of central importance because it may provide an operational advantage.

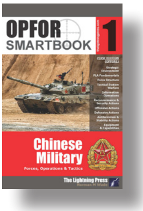
The elevation of information as a **joint function** impacts all operations and signals a fundamental appreciation for the military role of information at the strategic, operational, and tactical levels within today's complex operational environment (OE).

Operations in the information environment (OIE) are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by **informing** audiences; **influencing** foreign relevant actors; **attacking and exploiting** relevant actor information, information networks, and information systems; and by **protecting** friendly information, information networks, and information systems.







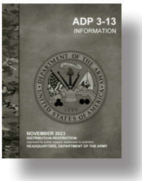


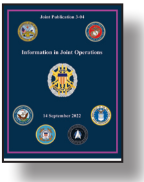
SMARTbooks - Intellectual Fuel for the Military!

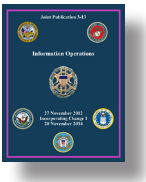
SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)! Recognized as a "whole of government" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive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

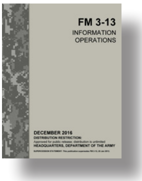
SMARTbooks can be used as quick reference guides during actual operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training. Visit **www.TheLightningPress.com**!

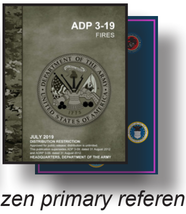
INFO2: Information Advantage SMARTbook (Activities, Tasks, & Capabilities), 2nd Ed.

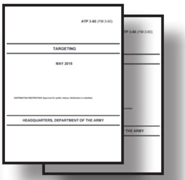

ADP 3-13


JP 3-04


JP 3-0


FM 3-13





Plus more than a dozen primary references on information capabilities & more!

Intro: Nature of Information & the OE

Information is central to all activity Army forces undertake. It is fundamental to command and control (C2) and is the basis for situational understanding, decision making, and actions across all warfighting functions. Information is the building block for intelligence—the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. As a **critical resource**, Army forces fight for, defend, and fight with information while attacking a threat's (adversary or enemy) ability to do the same.

Chap 1: Information Advantage (ADP 3-13)

An **information advantage** is a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior. There are several forms of information advantage. The **information advantage framework** presents a framework for creating and exploiting information advantages. Within this framework, Army forces integrate all relevant military capabilities through the execution of five information activities (enable, protect, inform, influence, and attack).

We no longer regard information as a separate consideration or the sole purview of technical specialists. Instead, we **view information as a resource** that is integrated into operations with all available capabilities in a **combined arms approach** to **enable** command and control; **protect** data, information, and networks; **inform** audiences; **influence** threats and foreign relevant actors; and **attack** the threat's ability to exercise command and control.

Army forces create and exploit **informational power** similarly to the joint force through five information activities (enable, protect, inform, influence, and attack). Army forces also consider information as a **dynamic of combat power** employed with mobility, firepower, survivability, and leadership to achieve objectives during armed conflict.

Chap 2: Information in Joint Operations: OIE (JP 3-04)

Information is a resource of the informational instrument of national power at the strategic level. Information is also a critical military resource. The joint force uses information to perform many simultaneous and integrated activities. The joint force employment of information is of central importance because it may provide an operational advantage.

The elevation of information as a **joint function** impacts all operations and signals a fundamental appreciation for the military role of information at the strategic, operational, and tactical levels within today's complex operational environment (OE).

Operations in the information environment (OIE) are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by **informing** audiences; **influencing** foreign relevant actors; **attacking and exploiting** relevant actor information, information networks, and information systems; and by **protecting** friendly information, information networks, and information systems.

Chap 3: Information Capabilities (PA, CA, MILDEC, MISO, OPSEC, CO, EW, Space, STO)

In addition to planning all operations to benefit from the inherent informational aspects of physical power and influence relevant actors, the JFC also has additional means with which to leverage information in support of objectives. Leveraging information involves the generation and use of information through tasks to inform relevant actors; influence relevant actors; and/or attack information, information systems, and information networks.

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 information activities are fully integrated into plans and orders through the military decision-making process. This includes integrating information activities into the concept of operations and supporting schemes, to include schemes of intelligence, information collection, maneuver, fires, and protection.

Chap 5: Information Preparation

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. It requires commander, staff, and Soldier actions to ensure the force is ready to execute operations.

Chap 6: Information Execution

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). Commanders, staffs, and subordinate commanders focus their efforts on translating decisions into action. They direct action to apply combat power, of which information is a dynamic, to achieve objectives and accomplish missions.

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). Information is integrated into the targeting cycle to produce effects in and through the information environment that support objectives.

Chap 8: Information Assessment

Information activities and tasks must be continually assessed to judge whether they achieve the desired outcome. Assessment is not a discrete step of the operations process. Assessing information activities and tasks is continuous and informs the other activities of the operations process. Staffs assess information activities and tasks while working in functional and integrating cells, and while participating in cross-functional meetings such as working groups and boards. The purpose of assessing information activities and tasks is to equip the commander with the analysis necessary to make better decisions.

(INFO2) References

The following references were used in part to compile *INFO2: 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.

**** See Editor's Note on Changes in Information Terminology on p. 1-2.** Based on changes to joint information doctrine, Army forces will no longer use the terms information operations, information-related capabilities, or information superiority. The Army is currently revising all its doctrine, to include FM 3-13, to account for these changes and the Army's new information advantage framework. **As such, the INFO2 SMARTbook retains the original terminology as referenced from the original source, while recognizing this terminology is changing (references marked with an asterisk, where possible.)***

Joint Publications

JP 3-0	Jun 2022	Joint Campaigns and Operations
JP 3-04	Sept 2022	Information in Joint Operations
JP 3-12	Dec 2022	Joint Cyberspace Operations
JP 3-85	May 2020	Joint Electromagnetic Spectrum Operations
JP 3-13.2	Dec 2011	Military Information Support Operations (w/Change 2)
JP 3-13.3	Jan 2016	Operations Security
JP 3-14	Oct 2020	Space Operations
JP 3-57	Jul 2018	Civil-Military Operations
JP 3-60	Sept 2018	Joint Targeting
JP 3-61	Aug 2016	Public Affairs (w/Change 1)

Army Doctrine Publications (ADPs)

ADP 3-13	Nov 2023	Information

Army Techniques Publications (ATPs)

ATP 3-13.1*	Oct 2018	The Conduct of Information Operations
ATP 3-13.5	Dec 2021	Soldier and Leader Engagement

Field Manuals (FMs)

FM 3-0	Oct 2022	Operations
FM 3-12	Aug 2021	Cyberspace and Electromagnetic Warfare
FM 3-13*	Dec 2016	Information Operations
FM 3-13.4	Feb 2019	Army Support to Military Deception
FM 3-14	Oct 2019	Army Space Operations
FM 3-57	Jul 2021	Civil Affairs Operations
FM 3-61	Feb 2022	Communication Strategy and Public Affairs Operations

(INFO2) Table of Contents

Intro

(INTRO) Nature of Information & the OE

Chap 1

Information Advantage

Chap 2 Information in Joint Operations (OIE)

Chap 3

(Information) CAPABILITIES

Chap 4

(Information) PLANNING

Chap 5 (Information) PREPARATION

Chap 6 (Information) EXECUTION

Chap 7

Fires & Targeting

Chap 8

(Information) ASSESSMENT

Intro

(INTRO) Nature of Information & the OE

Ref: ADP 3-13, Information (Nov '23), chap. 1.

I. Information Explained

Information is central to all activity Army forces undertake. It is fundamental to command and control (C2) and is the basis for situational understanding, decision making, and actions across all warfighting functions. Information is the building block for intelligence—the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (JP 2-0). As a critical resource, Army forces fight for, defend, and fight with information while attacking a threat's (adversary or enemy) ability to do the same.

A. Data and Information

The effective use of information to create and exploit information advantages begins with a common understanding of the terms data and information. Data is any signal or observation from the environment. An observation of an enemy force or a radar sounding are examples of data. A series of facts used for statistical analysis is also referred to as data. It can include facts such as lists of daily fuel and ammunition expenditures of subordinate units. In the context of computer science, data is electromagnetic encoded information for repeatability, meaning, and procedural use by automated means. Data can be collected, quantified, stored, and transmitted in electronic or other tangible forms; however, data is most useful when processed and assigned meaning by humans or human-designed algorithms (programs).

Information is data in context to which a receiver (human or automated system) assigns meaning.

Information is data in context to which a receiver processes and assigns meaning. Receivers include humans and automated systems that acquire data in a variety of ways—observations, spoken or written words, database retrieval, or other sensing mechanisms. Humans assign meaning to contextual data and use that information to understand, make decisions, communicate, and act. Automated systems—a combination of hardware and software—process and assign meaning to contextual data to support decision making, control their own functions, or control the functions of other systems.

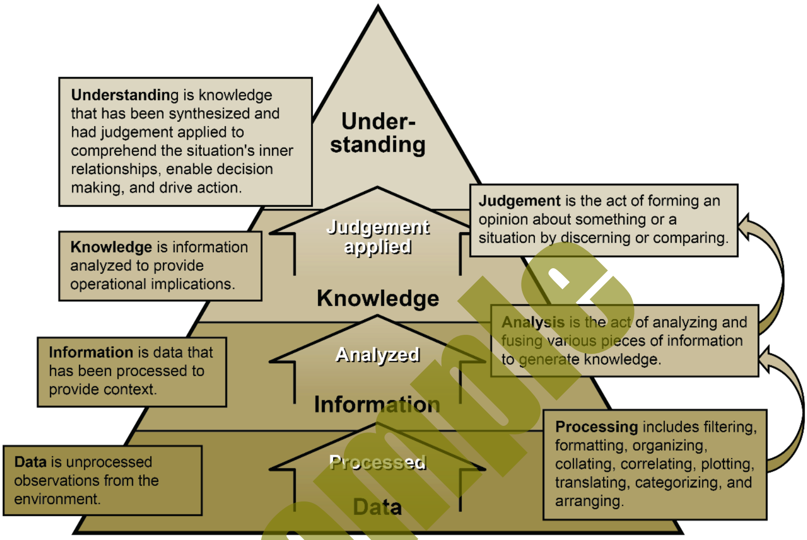
B. Assignment of Meaning

The assignment of meaning to data is receiver centric. For example, a company commander may interpret an enemy platoon moving into an assault position as the lead element of the enemy's main attack. The battalion commander may interpret the same observation differently, discerning the enemy platoon is a feint based on other reporting from the area of operations. A multitude of factors influences how a receiver interprets data to make sense of a situation or activity. For humans, factors range from education and experience to culture and beliefs. Automated systems assign meaning to data based on human programming, and in some cases, artificial intelligence and machine learning.

How Humans Assign Meaning to Data

Ref: ADP 3-13, Information (Nov '23), pp. 1-2 to 1-4.

How humans progressively assign meaning to data into understanding can be visualized as a hierarchy as shown in Figure 1-1. At the lowest level of the hierarchy is data. At the highest level is understanding. Processing transforms data into information. Analysis then refines information into knowledge. Humans then apply judgement to transform knowledge into understanding. It is this understanding that informs decision making and ultimately behavior.



Understanding is knowledge that has been synthesized and had judgement applied to comprehend the situation's inner relationships, enable decision making, and drive action.

Knowledge is information analyzed to provide operational implications.

Information is data that has been processed to provide context.

Data is unprocessed observations from the environment.

Judgement is the act of forming an opinion about something or a situation by discerning or comparing.

Analysis is the act of analyzing and fusing various pieces of information to generate knowledge.

Processing includes filtering, formatting, organizing, collating, correlating, plotting, translating, categorizing, and arranging.

Ref: ADP 3-13, (Nov '23), fig. 1-1. Cognitive hierarchy.

The meaning of information that leads to understanding and decision making relies on both the information itself (data and its context) and factors that influence how a receiver interprets that information. The premise of receiver-centric meaning is that individuals interpret symbols, messages, actions, and events differently. To increase the likelihood of a receiver interpreting the information in the way it was intended, the sender considers the factors that influence how a receiver assigns meaning. Two models help describe factors that affect how humans assign meaning to data:

Inherent Informational Aspects

All operations and activities have inherent informational aspects—features and details of a situation or an activity that can be observed. Humans use these inherent informational aspects to derive meaning from that situation or activity. When not directly observed, these aspects can be communicated to, inform, or influence an audience.

Inherent informational aspects include, but are not limited to, physical attributes of the capabilities and forces involved; the duration, location, and timing of the situation or activity; and any other characteristics that convey information to an observer. Inherent informational aspects, along with the context within which the activity occurs (for example, the background, setting, or surroundings), are processed through an individual's worldview to make sense of what is happening. Commanders purposefully design operations to optimize their inherent informational aspects, to include revealing or concealing signatures to influence relevant actor's perceptions and behavior.

- **Duration**: The period during which an activity or situation lasts. For example, an exercise occurring for one day or three weeks.
- **Location**: A position or site in which the activity or situation takes place usually marked by a distinguishing feature. For example, the situation or activity takes place on key terrain or a culturally significant site.
- **Timing**: The precise moment or the range of times in which the activity or situation takes place. For example, a cordon and search conducted during the night.
- **Platform**: The equipment or capability used during an activity or situation. For example, a force patrolling on foot or in armored vehicles.
- **Size**: The physical magnitude, extent, or bulk; the relative or proportionate dimensions of the force being presented. For example, an infantry company or an armored brigade in an assembly area.
- **Posture**: The state or condition at a given time in a particular circumstance; the position or bearing of the force.

Drivers of Behavior

In addition to inherent informational aspects, a combination of many other factors influences how humans interpret data to make sense of an idea or a situation. These factors drive behavior because they ultimately affect how humans decide and act on information. Understanding these factors is essential to leaders effectively using information to inform or influence audiences. Examples of drivers of human behavior include:

- **Attitude**—a positive or negative evaluation of a thing based on thoughts, behavior, and social content.
- **Bias**—a tendency to simplify information through a filter of personal experience and preferences that can cause errors in thinking.
- **Cognition**—the process by which knowledge and understanding are developed in the mind, to include retrieving stored information and processing that information.
- **Culture**—the customs, arts, social institutions, religious traditions, and achievement of a particular nation, people, or other social group.
- **Desire**—a strong feeling of wanting to have something or wishing for something to happen derived from factors such as affiliation, self-esteem, safety, security, freedom, & power.
- **Emotion**—an internal, unconscious mental reaction subjectively experienced and often manifested in physiological reactions and behavior. Emotional appeals can be highly effective because they bypass logic and critical thinking. However, forecasting the response (in order to measure it) is challenging.
- **Expertise**—in-depth knowledge and skill developed from experience, training, and education.
- **Instinct**—an innate, typically fixed pattern of behavior derived from desires such as a will to live, procreation, and pleasure.
- **Language**—shared communication that enables a population or group to interpret or make sense of data and information. Awareness of the attributes of a culture's language can provide insight to a culture's norms, attitudes, and beliefs.
- **Memory**—the mental storage of things learned and retained from activities and experiences. Memories are subject to deterioration and inaccurate recall. These inaccuracies can affect behavior just as much as accurate memories can.
- **Narrative**—a way of presenting or understanding a situation or series of events that reflects and promotes a particular point of view or set of values.
- **Perception**—the organization, identification, and interpretation of sensory information influenced by factors such as experiences, education, faith, and values.

Informational Considerations (of the OE)

Ref: ADP 3-13, Information (Nov '23), pp. 1-8 to 1-9.

The interrelationship among the land, maritime, air, space, and cyberspace domains requires cross-domain understanding. As such, Army leaders seek to understand an OE through the human, information, and physical dimensions inherent to each domain. While used to understand all aspects of an OE, analysis of the human, information, and physical dimensions also helps leaders identify and understand informational considerations.

See pp. 2-12 to 2-16 for related discussion of joint doctrine's "analysis of informational, physical, and human aspects of the environment" from JP 3-04.

Informational considerations are those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information (FM 3-0).

Informational Considerations

Human Dimension

Relevant Actors *(p. 1-27.)*
- **Military leaders**
- **Civilian leaders**
- **Key influencers**
- **Groups**
- **Organizations**
- **Populations**

Drivers of Behavior *(p. 0-3.)*
- **Attitude**
- **Bias**
- **Cognition**
- **Culture**
- **Desire**
- **Emotion**
- **Expertise**
- **Instinct**
- **Language**
- **Memory**
- **Narrative**
- **Perception**

Information Dimension

Ideas *(See p. 3-15.)*
- **Narratives**
- **Messages**
- **Themes**

Data

Software

Information
- **Friendly**
- **Neutral**
- **Threat**

Malign and Benign Information *(See p. 0-9.)*
- **Misinformation**
- **Propaganda**
- **Disinformation**
- **Information for effect**

Physical Dimension

Inherent Informational Aspects of Opns *(See p. 0-2.)*
- **Duration**
- **Location**
- **Timing**
- **Platform**
- **Size**
- **Posture**

Terrain

Weather

Electromagentic Radiation

Communications
- **Computer networks**
- **Internet**
- **Cellular networks**
- **Print**
- **Television**
- **Radio**
- **Satellite constellations**

Bandwidth

Storage

Ref: ADP 3-13 (Nov '23), fig. 1-4. Example informational considerations.

Leaders analyze informational considerations from friendly, threat, and neutral perspectives to aid them in developing ways to use, protect, and attack data, information, and capabilities. This analysis enhances several aspects of planning, to include the selection of objectives and targets; approaches to influence foreign relevant actors; and identification of force protection measures. Figure 1-4 depicts potential informational considerations by dimension.

NOTE: The Army's model of an OE established in FM 3-0 no longer includes an information environment. The term informational considerations is similar to the joint term and definition of information environment. The information environment is the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information (JP 3-04).

See p. 2-1 for discussion of the information environment from a joint perspective.

Chap 1 Information Advantage

Ref: ADP 3-13, Information (Nov '23), chap. 2.

I. Information Advantage (Overview)

An **information advantage** is a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior. There are several forms of information advantage.

Information Advantage (Activities)

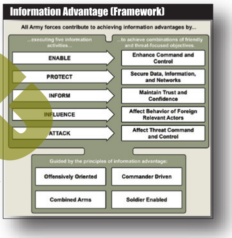
I **ENABLE** *(See pp. 1-21 to 1-28.)*

II **PROTECT** *(See pp. 1-29. to 1-34.)*

III **INFORM** *(See pp. 1-35 to 1-44.)*

IV **INFLUENCE** *(See pp. 1-45 to 1-48.)*

V **ATTACK** *(See pp. 1-49 to 1-56.)*


Information Advantage (Framework)
All Army forces contribute to achieving information advantages by...
...executing five information activities...
...to achieve combinations of friendly and threat-focused objectives.
ENABLE
Enhance Command and Control
PROTECT
Secure Data, Information, and Networks
INFORM
Maintain Trust and Confidence
INFLUENCE
Affect Behavior of Foreign Relevant Actors
ATTACK
Affect Threat Command and Control
Guided by the principles of information advantage:
Offensively Oriented
Commander Driven
Combined Arms
Soldier Enabled

(See p. 1-3.)

When Army forces achieve an information advantage, they—

- Communicate more effectively than the threat.
- Collect, process, analyze, and use information to understand an OE better than the threat.
- Understand, decide, and act faster and more efficiently than the threat.
- Are resilient to threat information warfare, to include disinformation and information for effect.
- Maintain domestic support and the support of multinational partners.
- Degrade threat command and control (C2) by affecting the threat's ability to understand, make effective decisions, and communicate.
- Influence threats and other foreign relevant actors' behavior favorable to friendly objectives.

An information advantage can result from and exploit human and physical advantages or enable those advantages. Like human and physical advantages, information advantages are often temporary and change over time relative to the threat and changes in an OE. While friendly forces are seeking information advantages, threat forces are doing the same. As such, an information advantage is something to gain, protect, and exploit across as many domains as possible.

ADP 3-13, Information (Nov '23): Introduction & Overview

Information is central to everything we do—it is the basis of intelligence, a fundamental element of command and control, and the foundation for communicating thoughts, opinions, and ideas. As a **dynamic of combat power**, Army forces fight for, defend, and fight with information **to create and exploit information advantages**—the use, protection, and exploitation of information to achieve objectives more effectively than enemies and adversaries do.

Advancements in information technologies and increased global connectivity continue to shape how we interact with each other and how forces fight. These advancements accelerate and expand the ability of joint and Army forces to collect, process, analyze, store, and communicate information at a scale previously unimaginable.

* Editor's Note on Changes in Information Terminology

Based on changes to joint information doctrine, **Army forces will no longer use the terms** *information operations, information-related capabilities, or information superiority*.

A significant joint doctrinal change is the transition from *joint information operations (IO)* to *operations in the information environment (OIE)*. Joint doctrine, however, retains the term *information environment*. The Army's new model of an operational environment established in FM 3-0 no longer includes an information environment. The term *informational considerations* aligns with the joint term *information environment*.

The Army is currently revising all its doctrine, to include FM 3-13, to account for these changes and the Army's new information advantage framework. ***As such, the INFO2 SMARTbook retains the original terminology as referenced from the original source, while recognizing this terminology is changing (marked with an asterisk).***

- ADP 3-13 (Nov '23) (See pp. 2-2 to 2-3 for joint doctrine changes.)

ADP 3-13, Information, is the Army's first publication dedicated to information. It provides a framework for creating and exploiting information advantages during the conduct of operations and at home station. It represents an evolution in how Army forces think about the military uses of data and information, emphasizing that everything Army forces do, to include the information and images it creates, generates effects that contribute to or hinder achieving objectives. **As such, creating and exploiting information advantages is the business of all commanders, leaders, and Soldiers.**

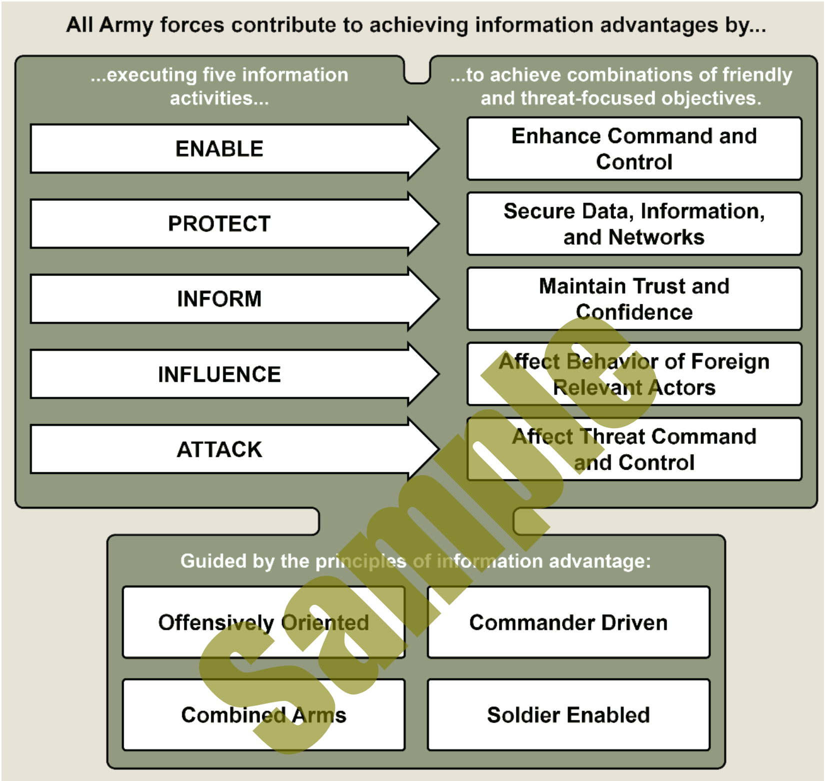
ADP 3-13 operationalizes the two big ideas inherent in multidomain operations—combined arms and positions of relative human, information, and physical advantage. **We no longer regard information as a separate consideration or the sole purview of technical specialists. Instead, we view information as a resource that is integrated into operations with all available capabilities in a combined arms approach** to enable command and control; protect data, information, and networks; inform audiences; influence threats and foreign relevant actors; and attack the threat's ability to exercise command and control.

Army leaders are accustomed to **creating and exploiting relative advantages** through a combined arms approach that traditionally focuses on the human and physical dimensions of an operational environment. ADP 3-13 acknowledges that advantages in the information dimension complement and reinforce advantages in the human and physical dimensions. The advantages do not necessarily have to be great: small advantages exploited quickly help commanders gain and maintain the operational initiative. Combining these advantages slows threat decision making, increases its level of uncertainty, and allows Army forces to dictate the tempo of operations.

Information Advantage Framework

Fig. 2-2 depicts a framework for creating and exploiting information advantages—the use, protection, and exploitation of information to achieve objectives more effectively than the threat.

Information Advantage (Framework)


All Army forces contribute to achieving information advantages by...
...executing five information activities...
...to achieve combinations of friendly and threat-focused objectives.
ENABLE
PROTECT
INFORM
INFLUENCE
ATTACK
Enhance Command and Control
Secure Data, Information, and Networks
Maintain Trust and Confidence
Affect Behavior of Foreign Relevant Actors
Affect Threat Command and Control
Guided by the principles of information advantage:
Offensively Oriented
Commander Driven
Combined Arms
Soldier Enabled

ADP 3-13 is a new publication that represents an evolution in how Army forces think about military uses of data and information in competition, crisis, and armed conflict. It represents a change in mindset based on the recognition that all activities have inherent informational aspects that generate effects which contribute to or hinder achieving objectives. Accounting for advances in information technologies and threat information warfare capabilities, ADP 3-13 describes a combined arms approach to creating and exploiting information advantages to achieve objectives. ADP 3-13 incorporates the Army's operational concept of multidomain operations and related doctrine described in the FM 3-0. ADP 3-13 describes—

- A revised model for understanding an operational environment through the human, information, and physical dimensions.
- Information as a dynamic of combat power.
- Information advantages as a central component of multidomain operations.
- Considerations for how Army forces seek information advantages within the strategic contexts of competition below armed conflict, crisis, and armed conflict.

II. Information in Multidomain Operations

Ref: ADP 3-13, Information (Nov '23), pp. 2-2 to 2-3.

The Army organizes, trains, and equips its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. Trained and ready Army forces support joint force commanders in three strategic contexts: **competition below armed conflict, crisis, and armed conflict.** *(See pp. 1-16 to 1-20.)*

An **operation** is a sequence of tactical actions with a common purpose or unifying theme. Operations vary in scale of forces involved, duration, and level of violence. While most operations conducted by Army forces occur either below the threshold of armed conflict or during limited contingencies, the focus of Army readiness is on large-scale combat operations against a peer threat.

Multidomain operations are the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders. Multidomain operations are the Army's contribution to joint campaigns during competition, crisis, and armed conflict. Below the threshold of armed conflict, multidomain operations are how Army forces accrue advantages and demonstrate readiness for conflict, deterring adversaries while assuring allies and partners. During armed conflict, Army forces use multidomain operations to close with and destroy the enemy, defeat enemy formations, seize critical terrain, and control populations and resources to deliver sustainable political outcomes.

The central idea of multidomain operations is the combined arms employment of all available joint and Army capabilities to create and exploit **relative advantages** to achieve objectives.

Relative Advantages

Relative advantages provide opportunities. A relative advantage is a location or condition, in any domain, relative to an adversary or enemy that provides an opportunity to progress towards or achieve an objective. During operations, small advantages can significantly impact the outcome of a mission, particularly when they accrue over time. Commanders seek and create relative advantages to exploit through action, and they continually assess friendly and enemy forces in relation to each other for opportunities to exploit.

Relative Advantages

- **Human**
- **Informational**
- **Physical**

Combined, these physical and information advantages can lead to a collapse of the enemy's morale and will—a human advantage. Army forces combine, reinforce, and exploit human, information, and physical advantages to achieve objectives across the competition continuum.

HUMAN Advantage

Human advantages are individual and group characteristics that provide opportunities for friendly forces. War is inherently a human endeavor—a violent struggle between multiple hostile, independent, and irreconcilable wills, each trying to impose its will on the other. Human will, instilled through commitment to a cause and leadership, is the driving force of all action in war. Army forces create and exploit human advantages throughout the conduct of operations. Combined with physical and information advantages, human advantages enable friendly morale and will, degrade enemy morale and will, and influence popular support.:

- Health, physical fitness, and toughness.
- Intelligence and intellect.
- Training.
- Leadership.
- Troop morale and will.
- Relevant actor trust.
- Positive relationships with foreign governments, populations, and forces.
- Cultural affinity and familiarity with indigenous populations and institutions.

INFORMATION Advantage *(See pp. 1-1 and 1-19.)*

An information advantage is a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior. There are several forms of information advantage. For example, a force that understands, decides, and acts more effectively than its opponent has an information advantage. A force that effectively communicates and protects its information, while preventing the threat from doing the same, is another form of an information advantage.

An information advantage can result from and exploit human and physical advantages or enable those advantages. Like human and physical advantages, information advantages are often temporary and change over time relative to the threat and changes in an OE. While friendly forces are seeking information advantages, threat forces are doing the same. As such, an information advantage is something to gain, protect, and exploit across as many domains as possible.

- Communicate more effectively than the threat.
- Collect, process, analyze, and use information to understand an OE better than the threat.
- Understand, decide, and act faster and more efficiently than the threat.
- Are resilient to threat information warfare, to include disinformation & information for effect.
- Maintain domestic support and the support of multinational partners.
- Degrade threat command and control (C2) by affecting the threat's ability to understand, make effective decisions, and communicate.
- Influence threats & other foreign relevant actors' behavior favorable to friendly objectives.

PHYSICAL Advantage

Physical advantages are most familiar to tactical forces, and they are typically the immediate goal of most tactical operations. Finding the enemy, defeating enemy forces, and seizing occupied land typically require the creation and exploitation of multiple physical advantages. These advantages include occupation of key terrain, the physical isolation of enemy forces, and the imposition of overwhelming fires. The exploitation of physical advantages reduces the enemy's capability to fight, which creates information and human advantages. Physical advantages implicitly communicate a message that can influence enemy forces' will to fight, sway popular support, and disrupt enemy risk calculus at all echelons.

- Geographic and positional advantages.
- Capabilities or qualitative advantages.
- Overall combat power, including numbers of systems and firepower.

Refer to AODS7: The Army Operations & Doctrine SMARTbook (Multidomain Operations). Completely updated with the 2022 edition of FM 3-0, AODS7 focuses on Multidomain Operations and features rescoped chapters on generating and applying combat power: command & control (ADP 6-0), movement and maneuver (ADPs 3-90, 3-07, 3-28, 3-05), intelligence (ADP 2-0), fires (ADP 3-19), sustainment (ADP 4-0), & protection (ADP 3-37).

III. Informational Power

Ref: ADP 3-13, Information (Nov '23), pp. 1-4 to 1-6.

Power—the capacity or ability to direct or influence the behavior of others—has many forms. **Informational power** is an ability to use information to support achievement of objectivities and create information advantages. Informational power and physical power (strength or force) are interdependent and mutually supporting forms of power applicable below and above the threshold of armed conflict. An effective application of informational power to achieve objectives requires a whole of government, joint, and combined arms approach.

Information and the INSTRUMENTS OF NATIONAL POWER

Information is a vital resource for national security. From a U.S. government perspective, the informational instrument of national power is employed in combination with diplomatic, military, and economic power to advance national interests. Previously considered in the context of traditional nation states, the construct of information as an instrument of national power now extends to nonstate actors. Nonstate actors include terrorists, mercenary companies, and transnational criminal organizations—actors who use information to further their causes and undermine those of the U.S. government and its multinational partners. Nonstate actors can also include nongovernmental organizations and multinational corporations who can be supportive of U.S. interests.

The U.S. government employs informational power in three primary ways. First, it synchronizes its communications activities to influence the perception and attitudes of other governments, organizations, groups, and individuals deemed vital to strategic objectives. Second, the U.S. government coordinates efforts to secure cyberspace and critical infrastructure against information disruption. Third, the U.S. government provides information to bolster national will and resolve.

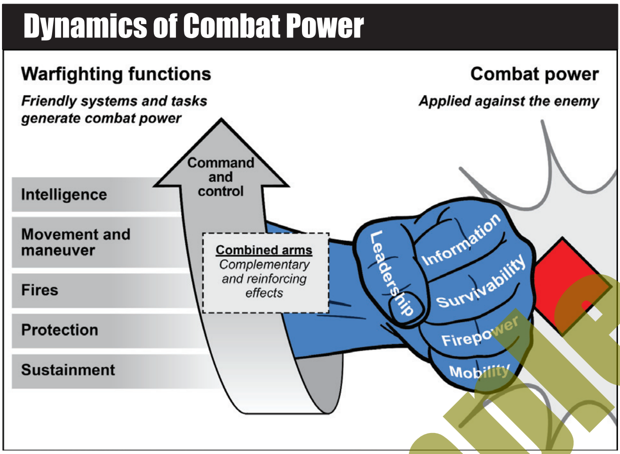
JOINT Informational Power *(See pp. 2-4 to 2-5.)*

For joint force commanders, the essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of military objectives. The joint force uses information to perform many simultaneous and integrated activities ranging from improving friendly understanding and decision making to affecting threat behavior. The joint force leverages the power of information to effectively expand the commander's range of operations. Joint force commanders apply informational power—

- To operate in situations where the use of destructive or disruptive physical force is not authorized or is not an appropriate course of action.
- To degrade, disrupt, and destroy threat C2.
- To prevent, counter, and mitigate the effects of external actors' actions on friendly capabilities and activities.
- To create and enhance the psychological effects of destructive or disruptive physical force.
- To create psychological effects without destructive or disruptive force.
- To confuse, manipulate, or deceive an adversary or enemy to create an advantage or degrade a threat's existing advantage.
- To prevent, avoid, or mitigate any undesired psychological effects of operations.
- To communicate and reinforce the intent of operations, regardless of whether those activities are constructive or destructive.
- To reinforce the will to fight in friendly forces and populations.
- To degrade the will to fight in threat forces and populations.

Information as a DYNAMIC OF COMBAT POWER *(AODS7, chap. 2.)*

Army forces create and exploit informational power similarly to the joint force through five information activities (enable, protect, inform, influence, and attack). Army forces also consider information as a dynamic of combat power employed with mobility, firepower, survivability, and leadership to achieve objectives during armed conflict. Combat power is the total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time (JP 3-0). As a dynamic of combat power, Army forces fight for, defend, and fight with information.



Combat power *is the total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time (JP 3-0). It is the ability to fight. The complementary and reinforcing effects that result from synchronized operations yield a powerful blow that overwhelms enemy forces and creates friendly momentum.*

Army leaders at every level require and use information to seize, retain, and exploit the initiative and achieve decisive results. Army forces collect, process, and analyze data and information from all domains to develop understanding, make decisions, and apply combat power against enemy forces. Army forces fight for information about the enemy and terrain through reconnaissance and surveillance, and through offensive operations such as movement to contact or reconnaissance in force. Intelligence and cyberspace operations penetrate enemy networks and observe activities to gain and exploit information on the threat. Simultaneously, Army forces defend their own networks to secure friendly data and ensure secure communications. Friendly security operations, operations security, counterintelligence, and defensive cyberspace operations deny enemy access to friendly information and intentions.

Army forces fight with information to influence threat behavior. Creatively employing and concealing information can enable Army forces to achieve surprise, cause enemy forces to misallocate or expend combat power, or mislead enemy forces as to the strength, readiness, locations, and intended missions of friendly forces. Army forces also employ information as a means of amplifying the psychological effects of disruptive and destructive physical force to erode morale, impede decision making, and increase uncertainty among enemy forces. Army forces employ all relevant capabilities to attack threat data, information, and networks to hinder the threat's ability to exercise C2.

Refer to AODS7: The Army Operations & Doctrine SMARTbook (Multidomain Operations). Completely updated with the 2022 edition of FM 3-0, AODS7 focuses on Multidomain Operations and features rescoped chapters on generating and applying combat power: command & control (ADP 6-0), movement and maneuver (ADPs 3-90, 3-07, 3-28, 3-05), intelligence (ADP 2-0), fires (ADP 3-19), sustainment (ADP 4-0), & protection (ADP 3-37).

VIII. Information Advantages (Across Strategic Contexts)

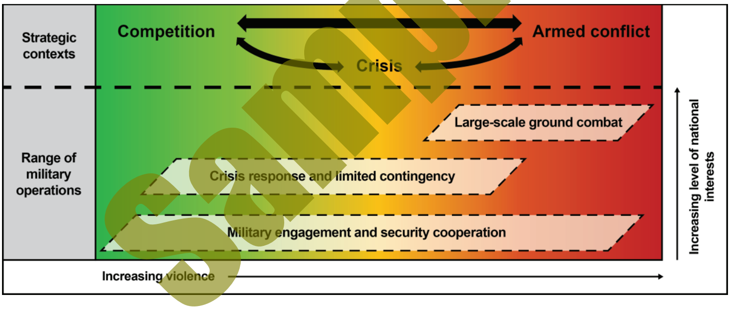
Joint doctrine describes the strategic environment in terms of a competition continuum. Rather than a world either at peace or at war, the competition continuum describes three broad categories of strategic relationships: cooperation, competition below armed conflict, and armed conflict. Each relationship is defined as between the United States and another strategic actor relative to a specific set of policy aims. Within this competition continuum, Army forces support combatant commanders in achieving their objectives in three strategic contexts:

Army Strategic Contexts

A Competition (Below Armed Conflict)

B Crisis

C Armed Conflict


Strategic contexts
Competition
Armed conflict
Crisis
Range of military operations
Large-scale ground combat
Crisis response and limited contingency
Military engagement and security cooperation
Increasing violence
Increasing level of national interests

Ref: FM 3-0 (Oct. '22), fig. 1-3. Army strategic contexts and operational categories.

Whether in times of relative peace or periods of armed conflict, Army forces seek to create and exploit information advantages to achieve objectives.

Refer to AODS7: The Army Operations & Doctrine SMARTbook (Multidomain Operations). Completely updated with the 2022 edition of FM 3-0, AODS7 focuses on Multidomain Operations and features rescoped chapters on generating and applying combat power: command & control (ADP 6-0), movement and maneuver (ADPs 3-90, 3-07, 3-28, 3-05), intelligence (ADP 2-0), fires (ADP 3-19), sustainment (ADP 4-0), & protection (ADP 3-37).

A. Competition (Below Armed Conflict)

(AODS7, pp. 1-63 to 1-72.)

Competition below armed conflict occurs when an adversary's national interests are incompatible with U.S. interests, and that adversary is willing to actively pursue those interests short of armed conflict. Operations during competition involve security cooperation and deterrence activities conducted under numerous programs within a combatant command. The combatant commander uses these activities to improve security within partner nations, enhance international legitimacy, gain multinational cooperation, and influence adversary decision making.

During competition below armed conflict, Army forces conduct operations and execute activities that support joint force campaigning goals, satisfy interagency requirements, and set the necessary conditions to employ Army combat power during crisis and armed conflict. Threat information warfare activities are continuous during competition. The theater army works with the joint force to thwart threat information warfare, communicate U.S. resolve, and achieve campaign plan objectives.

During competition, Army forces provide essential support to shaping foreign perceptions and behavior by—

- Using information to promote stability, cooperation, interoperability, and partnership among multinational partners as well as fostering legitimacy of U.S. and coalition efforts.
- Informing international audiences to create shared understanding, promote trust, mitigate malign information efforts, and enhance the legitimacy of U.S. and coalition operations and activities.
- Helping to develop and communicate a compelling narrative that influences foreign relevant actors to support friendly objectives or preempts the threat's messaging and malign information efforts.
- Executing MISO, participating in joint and combined exercises that demonstrate will and interoperability, maintaining readiness, and conducting security cooperation activities.

As part of competition below armed conflict, Army leaders engage and communicate with domestic audiences to maintain support at home and establish advantageous relationships with allies and partners abroad. Army forces help shape an OE by conducting security cooperation activities with partner nation armed forces and civilian agencies. These types of engagements, coordinated with applicable American embassies, help shape a credible narrative that builds trust and confidence by sharing information and coordinating mutually beneficial activities.

Shaping adversary behavior requires persistent engagement and the presence of sufficient Army forces to ensure alignment between stated objectives and subsequent actions. Physically demonstrating the scope and scale of capabilities necessary to compel desirable behavior is a critical component of influencing both adversary attitudes and behavior and assuring allies and partners. For example, a combined arms exercise with an allied nation's armed forces amplifies messages of resolve and reassurance that fosters positive perceptions and attitudes toward U.S. presence, posture, and objectives. This, in turn, builds confidence among allies and partners. Conversely, this same exercise can support conventional deterrence against an adversary.

During competition below armed conflict, Army forces protect information and remain vigilant against threat attempts to confuse situations and disrupt positive relationships among Army forces and partners. Army forces must expect threats to conduct disinformation campaigns designed to sow distrust or doubt among U.S. domestic audiences and among foreign partners. As such, Army leaders engage with and inform Army, domestic, and international audiences to put operations into context, build and maintain resiliency, and maintain the trust and confidence in the Armed Forces of the United States.

Information Advantage (Examples)

Ref: FM 3-0, Operations (Oct. '22), chaps. 4 to 6.

Information Advantages (Competition) *(AODS7, p. 1-72.)*

Information activities play a key role during competition. They include Army support to the combatant command and unified action partner strategic messaging. Coordinating with interagency and other unified action partners helps to develop and deliver coherent messages that counter adversary disinformation. Army forces reinforce strategic messaging by maintaining and demonstrating U.S. Army readiness for operations. Examples of relative information advantages are—

- Identifying targets and conducting target development on threat capabilities.
- Setting the conditions for convergence by developing methods to penetrate adversary computer networks.
- Discrediting adversary disinformation by helping the JFC inform domestic and international audiences through Army and joint information activities.
- Promoting the purpose and outcomes of multinational exercises and training events.
- Continuously monitoring the operational environment to detect changes to adversary methods or narratives.

Information Advantages (Crisis) *(AODS7, p. 1-82.)*

Two key information activities are protecting friendly information and degrading the threat's ability to communicate, sense, make effective decisions, and maintain influence with relevant actors and populations. An example is the use of strategic messaging to undermine the credibility of an adversary by exposing violations of international law and showing that adversary narratives are false. Achieving information advantages is a commander-driven, combined arms activity that employs capabilities from every warfighting function. During crisis, commanders lead their staffs to refine information activities based upon plans and processes developed during competition. Examples include commanders and staffs focusing on the challenges and tasks of establishing a mission-partner environment, building or modifying an intelligence architecture, and creating or refining common operating procedures with allies and other partners.

Information Advantages (Armed Conflict) *(AODS7, p. 1-89.)*

Information advantages invariably overlap with and emanate from physical and human advantages. To gain an information advantage, units first require a physical or human advantage. Army forces create and exploit information advantages by acting through the physical and human dimensions of an operational environment. Leaders combine information advantages with other advantages to understand the situation, decide, and act faster than enemy forces. Examples of information advantages during armed conflict include—

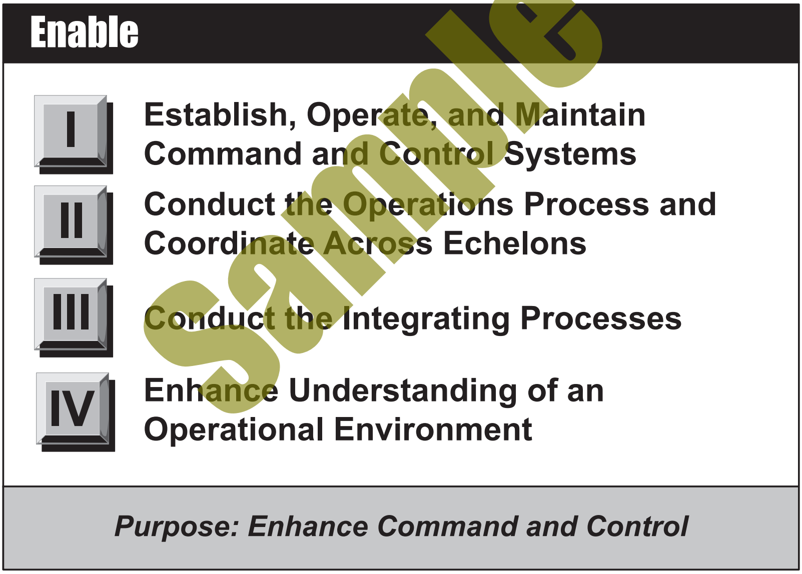
- The ability to access enemy C2 to disrupt, degrade, or exploit enemy information.
- Opportunities created by deception operations to achieve surprise and thwart enemy targeting.
- The ability to mask electromagnetic signatures.
- The ability to integrate and synchronize friendly forces in denied or degraded environments through use of redundant communications.
- The ability to rapidly share information with domestic and international audiences to counter enemy malign narratives.
- The ability to inform a wide range of audiences to maintain legitimacy and promote the friendly narrative.
- The ability to rapidly share and analyze information among commanders and staffs to facilitate decisions and orders.

Chap 1 (Information Advantage) I. Enable

Ref: ADP 3-13, Information (Nov '23), chap. 3.

Information is the basis of C2, intelligence, and communication. Army forces collect, process, and analyze data and information to understand situations, make decisions, and develop plans. They communicate information to integrate, synchronize, and control operations. Information, in the form of feedback, enables Army leaders to assess progress and adjust operations as required.

The force that uses and exploits data and information to understand, make decisions, and act more effectively than its opponents has a significant advantage. The enable information activity contributes to this advantage through four related tasks: establish, operate, and maintain C2 systems; execute the operations process and coordinate across echelons; conduct the integrating processes; and enhance understanding of an operational environment (OE) as shown in Figure 3-1.



Enable

- I — Establish, Operate, and Maintain Command and Control Systems
- II — Conduct the Operations Process and Coordinate Across Echelons
- III — Conduct the Integrating Processes
- IV — Enhance Understanding of an Operational Environment

Purpose: Enhance Command and Control

Ref: ADP 3-13 (Nov '23), fig. 3-1. Tasks and purpose of the enable information activity.

I. Establish, Operate, and Maintain Command and Control Systems *(AODS7, chap. 3.)*

Command and control is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission (JP 1, Volume 2). Commanders cannot exercise C2 alone. Even at the lowest levels, commanders need support to command forces and control operations. At every echelon of command, each commander has a C2 system to provide that support. The command and control system is the arrangement of people, processes, networks, and command posts that enable commanders to conduct operations (ADP 6-0).

IV. Enhance Understanding of an Operational Environment

Success during operations demands timely and effective decisions based on applying judgement to available information and knowledge. As such, commanders and staffs seek to build and maintain situational understanding throughout the operations process. Understanding informational considerations of an OE bolsters this understanding. Several tasks assist commanders and staffs in understanding how information and information capabilities impact operations, to include—

- Analyze the operational and mission variables.
- Identify and describe relevant actors. *(See facing page.)*
- Identify likely behavior of relevant actors. *(See facing page.)*

A. Analyze the Operational and Mission Variables

The operational and mission variables are tools to assist commanders and staffs in developing situational understanding.

Upon receipt of a mission, commanders use the mission variables, in combination with the operational variables, to refine their understanding of the situation and to visualize, describe, and direct operations.

Operational Variables - PMESII-PT *(BSS7, p. 1-18.)*

Operational variables are categories of relevant information that commanders and staffs use to understand their OE. Commanders and staffs analyze and describe an OE in terms of eight interrelated operational variables known as PMESII-PT: political, military, economic, social, information, infrastructure, physical environment, and time.

Mission Variables - METT-TC (I) *(BSS7, p. 1-19.)*

METT-TC (I) represents the mission variables that leaders use to analyze and understand a situation in relationship to the unit's mission. The first six variables are not new. However, the increased reliance on information (military and private sector) to enable operations requires leaders to continuously assess the informational considerations on assigned missions. Because of this, the variable of informational considerations is added to the familiar METT-TC mnemonic. Within the mission variables, informational considerations are expressed as a parenthetical variable in that it is not an independent variable by itself, but it is an important consideration within each mission variable.

Informational considerations are those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information.

B. Identify and Describe Relevant Actors

Ref: ADP 3-13, Information (Nov '23), pp. 3-12 to 3-13.

The analysis of human, information, and physical dimensions of an OE provides the context needed to understand how individuals, groups, populations, and automated systems operate.

See p. 2-64 for related discussion of audiences, targets, and target audiences.

Relevant Human Actors

Relevant human actors include individuals, groups, or populations whose behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. Relevant actors may be friendly, neutral, or threat; military or civilian; and state or nonstate. Army forces use information combined with action to influence relevant actors in support of objectives.

When considering relevant human actors, staffs gain understanding by conducting two activities. First, commanders and their staffs describe the individuals, groups, and populations who can aid or hinder success of their missions. Some of these actors may exist outside the unit's area of operations. Second, the staff describes how the human, information, and physical dimensions affect each relevant actor.

Relevant Automated Systems

Automated systems are a combination of hardware and software that allow computer systems, network devices, or machines to function with limited human intervention. Automated systems with emerging artificial intelligence technologies can rapidly sort, collate, and identify trends, patterns, and vital information far faster and more efficiently than any human analysts can.

When considering relevant automated systems, staffs gain understanding by conducting the following two activities. First, commanders and their staffs remain aware that as automated systems become more sophisticated, they will have greater impacts on operations. Automated systems vary based on their degree of autonomy, intelligence, and sophistication. Additionally, their ubiquity makes it difficult to identify their presence and relevance among other actors. Conducting functional analysis as outlined in ATP 2-01.3 assists in identifying relevant automated systems within the area of operations. Second, staffs describe what effects informational and physical aspects of the environment have on each automated system.

C. Identify BEHAVIORS of Relevant Actors

Identifying current relevant actor behaviors helps planners formulate an operational approach to influence those behaviors. The staff helps the commander to develop a detailed understanding of the options available to affect relevant actor behaviors and assess which option might most strongly impact friendly operations.

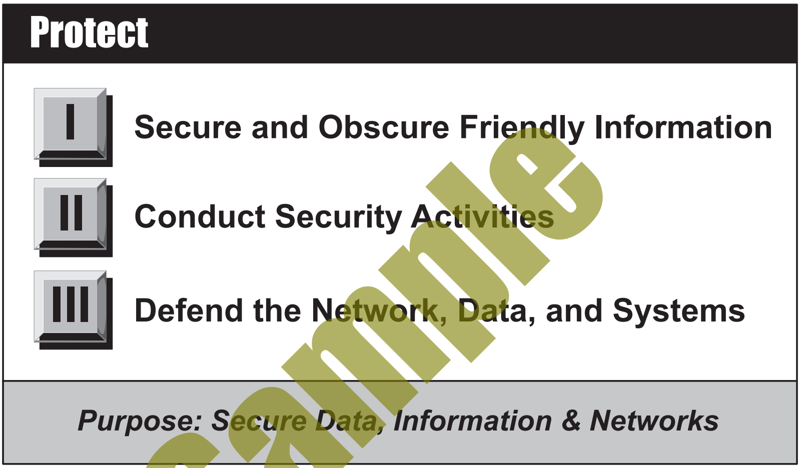
- Identify current behaviors relative to impending friendly operations.
- Identify what relevant actor behaviors will likely affect operations.
- Describe how the selected behaviors of relevant actors may evolve over time.
- Describe how information and action can affect behavioral trends to yield outcomes favorable or unfavorable to friendly forces.
- Identify what broad actions friendly forces take to create effects in an OE that arrest or encourage behavioral trends.
- Identify potential second-and third-order effects of the operational approach.

Once the staff identifies relevant actors and their behaviors, the commander selects the appropriate means to affect behavior.

(Information Advantage) II. Protect

Ref: ADP 3-13, Information (Nov '23), chap. 4.

All Army forces continuously provide protection. Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (JP 3-0). Achieving protection is a continuous endeavor, requiring Army leaders to apply a comprehensive, layered, and redundant approach in different contexts.



Protect

I Secure and Obscure Friendly Information

II Conduct Security Activities

III Defend the Network, Data, and Systems

Purpose: Secure Data, Information & Networks

Ref: ADP 3-13 (Nov '23), fig. 4-1. Tasks and purpose of the protect information activity.

I. Secure and Obscure Friendly Information

Securing information about Army forces is a responsibility of all Soldiers, Army Civilians, and contractors. For commanders and leaders, it means two things. First, leaders educate Soldiers, Army Civilians, contractors, and family members on the type and nature of data and information that threat forces seek. Second, leaders inculcate into their unit culture the imperative of securing friendly data and information.

> **Imperative of operations**: Account for being under constant observation and all forms of enemy contact. *(AODS7, p. 1-44.)*

Securing and obscuring friendly information begins with an understanding of what data exist relating to friendly forces. Army leaders must understand their own data and information signature from a threat's perspective. They must assume that threats constantly observe their formations from different domains and the electromagnetic spectrum.. Tasks that secure and obscure friendly information include—

- Implement operations security (OPSEC). *(See pp. 3-39 to 3-40.)*
- Conduct deception in support of OPSEC (DISO). *(See p. 3-28.)*
- Employ camouflage, concealment, and obscuration.

II. Conduct Security Activities

Ref: ADP 3-13, Information (Nov '23), pp. 4-5 to 4-6.)

All Soldiers share a responsibility for securing important information about Army forces. Some Army forces are manned, trained, and equipped to engage in specialized security activities, specifically conducted to deny threat forces relevant information. Security activities related to securing information include—

Security Activities

A. Conduct Security Operations
B. Implement Physical Security
C. Implement Personnel Security Program
D. Conduct Counterintelligence

A. Conduct Security Operations *(AODS7, pp. 4-21 to 4-24.)*

Commanders prevent threats from collecting information about friendly force activities in part by performing security operations. Security operations are those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow commanders to effectively use their protected forces (ADP 3-90). Security operations focus on the protected force or location. By denying threat actors a vantage point from which to observe friendly activities and dispositions, forces conducting security operations can protect friendly information against threat reconnaissance efforts. Army forces conduct four types of security operations:

- Screen.
- Guard.
- Cover.
- Area security.

Counterreconnaissance is a tactical mission task that encompasses all measures taken by a commander to counter enemy reconnaissance and surveillance efforts. It prevents hostile observation of a force or area and accounts for all the domains through which the threat can conduct reconnaissance in a particular situation. It involves both active and passive elements and includes combat action to destroy or repel enemy reconnaissance units and surveillance assets. Counterreconnaissance is not a distinct mission but an essential component to security operations.

Threat unmanned aircraft systems carry a variety of surveillance and reconnaissance capabilities, ranging from high-resolution video to infrared or electromagnetic reconnaissance. Unmanned aircraft systems carry a range of capabilities, to include surveillance, reconnaissance, targeting, electromagnetic attack, and air-to-surface weapons.

B. Implement Physical Security

Physical security consists of physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and safeguard them against espionage, sabotage, damage, theft, and terrorism. Army forces employ physical security measures in depth to protect personnel, information, and critical resources in all locations and situations against various threats. This total system approach is based on the continuing analysis and employment of protective measures, including—

- Physical barriers.

- Clear zones.
- Lighting.
- Access and key control.
- Intrusion detection devices.
- Biometrically enabled base access systems.
- Defensive positions.
- Nonlethal capabilities.

Refer to ATP 3-39.32 for additional information on physical security.

C. Implement Personnel Security Program

Personnel security plays an important role in protecting friendly information. Units should ensure that personnel in sensitive positions have the appropriate clearance, a need to know, and required certifications before granting access to critical network infrastructure. The clearance and sensitive position standard determines whether a person is eligible for access to classified information or assignment to sensitive duties. This standard evaluates if the person's loyalty, reliability, and trustworthiness for having access to classified information or assignment to sensitive duties is clearly consistent with the interests of national security.

Refer to AR 380-67 for more information about the Army personnel security program.

D. Conduct Counterintelligence (CI)

Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (JP 2-0). Counterintelligence (CI) is one of the Army's intelligence disciplines conducted by specially trained CI agents, technicians, and special agents. These specially trained personnel focus on detecting and identifying the FIE's intelligence collection activities targeting U.S. and multinational forces.

CI operations are broadly executed CI activities using one or more of the CI functions (investigations, collection, analysis and production, and technical services and support) that support a program or specific mission. The CI mission includes defensive and offensive activities conducted worldwide to protect Army forces, installations, and operations from the foreign intelligence collection threat. The CI mission encompasses four different mission areas:

- Counterespionage.
- CI support to force protection.
- CI support to research, development, and acquisition.
- CI-cyber.

CI relies on the Threat Awareness and Reporting Program (known as TARP) to identify systemic or personnel issues and to identify other inconsistencies that may indicate a vulnerability or incident of CI interest. The Threat Awareness and Reporting Program is an education, awareness, and reporting program to help identify incidents of potential CI interest. The program is a primary factor in obtaining information to initiate CI investigations in response to suspected national security crimes under Army CI jurisdiction. The Threat Awareness and Reporting Program education activities should be tailored to the supported unit based on the unit mission, unique foreign intelligence entities characteristics, and methods of operation.

Refer to ATP 2-22.2-1 for more information on Army CI.

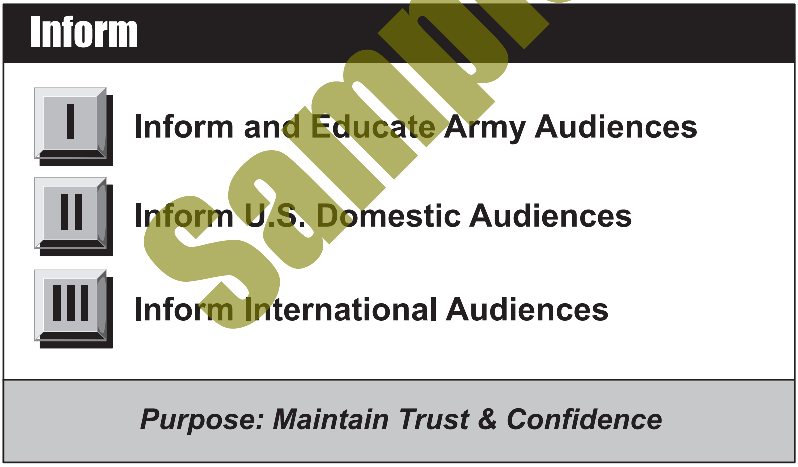
(Information Advantage) III. Inform

Ref: ADP 3-13, Information (Nov '23), chap. 5.

See pp. 3-5 to 3-16 for related discussion of public affairs operations (JP/FM 3-61) and p. 2-19 for discussion of "inform" from a joint doctrine perspective (JP 3-04).

The U.S. Army has an obligation to inform. Army leaders keep internal audiences (Soldiers, Army Civilians, contractors, and family members) informed about organizational goals, priorities, values, and expectations. Army leaders keep external audiences (U.S. domestic and international) informed to maintain their trust and confidence. Within a larger national and joint narrative, Army leaders inform various international audiences to facilitate informed perceptions about military objectives and activities. Combined with demonstrated competence and professionalism, informing international audiences strengthens partnerships and alliances during competition, crisis, and armed conflict.

Army forces communicate accurate and timely information to internal and external audiences to gain an information advantage. The inform information activity contributes to this advantage through its related tasks: inform and educate Army audiences; inform U.S. domestic audiences; and inform international audiences as shown in Figure 5-1.



Inform

I Inform and Educate Army Audiences

II Inform U.S. Domestic Audiences

III Inform International Audiences

Purpose: Maintain Trust & Confidence

Ref: ADP 3-13 (Nov '23), fig. 5-1. Tasks and purpose of the inform information activity.

Note. The inform information activity relies on several public affairs terms. Public affairs are communication activities with external and internal audiences (JP 3-61). In public affairs, an audience is a broadly-defined group that contains stakeholders and/or publics relevant to military operations (JP 3-61). An audience can be internal or external. In public affairs, an internal audience is United States military members and Department of Defense civilian employees and their immediate families (JP 3-61). In public affairs, an external audience is all people who are not United States military members, Department of Defense civilian employees, and their immediate families (JP 3-61). External audiences are categorized as U.S. domestic and international audiences. In public affairs, a public is a segment of the population with common attributes to which a military force can tailor its communication (JP 3-61).

I. Inform and Educate Army Audiences

Commanders establish and maintain a positive command climate—the characteristic atmosphere in which people work and live. Command climate is directly attributable to the leader's values, skills, and actions. A positive climate facilitates team building, encourages initiative, and fosters collaboration, mutual trust, and shared understanding. Commanders shape the climate of their organization no matter the size. Maintaining a positive command climate includes—

A. Inform Internal Audiences

Keeping internal audiences informed plays a crucial role in sustaining the morale and will of Army forces. Commanders and leaders keep internal audiences informed on organizational goals, priorities, values, and expectations, while encouraging feedback. They inform through various means ranging from conducting mission briefings to hosting town hall meetings.

An effective command information program combined with community engagement aids commanders in informing internal audiences. Command information is communication by a military organization directed to the internal audience that creates an awareness of the organization's goals, informs them of significant developments affecting them and the organization, increases their effectiveness as ambassadors of the organization, and keeps them informed about what is going on in the organization (JP 3-61).

Refer to DODI 5400.17 for policy concerning official use of social media.

Operations, particularly those involving armed conflict, are fraught with danger and hardship. Violence, fatigue, and fear characterize large-scale combat operations. To help build unit cohesion and maintain morale and will, commanders and leaders communicate to all Soldiers how their units' efforts and purpose fit into the overall purpose of the operations. Communicating "why we fight" helps Soldiers understand they are part of a larger team and effort. Shared understanding of purpose helps Soldiers reconcile their sacrifices toward a greater effort.

B. Educate Soldiers

Threats do not hesitate to employ a variety of influence techniques to weaken the resolve of Americans, especially members of the Department of Defense (DOD). Social media, internet-based communication, on¬line gaming, and other dynamic forms of communication allow threats to extend their reach in the human and information dimensions beyond what was previously possible. The potential for Soldiers to have contact with threat influence activities is high, even when in garrison. The chances of threat influence activities increase as Army forces initiate operations during crisis and conflict.

Soldiers must remain vigilant to recognize threat attempts to undermine their morale and will. The entire Army force is potentially subject to monitoring and threat influence activities through various mediums, to include the internet. Leaders train and educate Soldiers to maintain online awareness, to include identifying threats and applying operational security when posting information and images online. To provide Soldiers the ability to recognize and mitigate threat influence activities, as well as to withstand enemy influence attempts, leaders educate the force concerning—

- **Threat influence methods**. Threat influence methods can affect Soldiers directly or indirectly with the goal of influencing their thinking. The threat may employ direct influence activities, for example overt propaganda, or more subtle attacks like engaging in activities that amplify social or political differences.
- **The Army profession.** Understanding the role of the Army as articulated in ADP 1 can help defend against the effects of misinformation, disinformation, and information for effect. When Soldiers understand why the Army exists and their role in protecting their nation's interests, it becomes increasingly difficult for the threat to undermine their commitment to their duty.

II. Inform United States Domestic Audiences

Federal laws and military instructions such as DODD 5122.05 and AR 360-1 require Army forces to inform domestic audiences of their operations, programs, and activities. The Department of the Army and Army commanders are responsible for informing the American people about the Army's mission and goals.

> Accurately informing the American people assists the Army in establishing conditions that lead to the public's understanding, trust, confidence, and support.

Army senior leaders ensure the operations and activities conducted by Army forces are aligned with the national security interests and values of the American people as articulated by various strategic documents. These documents include the National Security Strategy and the National Military Strategy. By informing the U.S. domestic audience, Army forces reassure the American public that they execute operations in accordance with national values. Commanders of Army formations inform domestic audiences primarily through public communication, which includes community engagement within the broader Army communication strategy.

Inform U.S. Domestic Audiences

A. Conduct Public Communication
B. Conduct Community Engagement
C. Correct Misinformation and Counter Disinformation Related to Army Forces or Operations

Refer to FM 3-61 for more information on public communication and community engagement. (See pp. 3-5 to 3-16.)

A. Conduct Public Communication

Informing U.S. domestic audiences helps these audiences understand that Army operations align with American interests. This communication increases public trust and support through active engagements. Through public communication programs, commanders demonstrate they are community partners and responsible stewards of national resources.

Public communication includes the release of official information through news releases that encompass public service announcements, media engagements, town hall meetings, public engagements, and social networks. Public communication enables commanders to meet their obligations to keep the American people informed. Public communication objectives include the following:

- Increase public awareness of the Army's mission, policies, and programs.
- Foster good relations within the communities with which Army forces interact.
- Maintain the Army's reputation as a respected professional organization responsible for national security.
- Support the Army's recruiting and personnel procurement mission.
- Correct misinformation and counter disinformation.

B. Conduct Community Engagement

Community engagements are activities that support the relationship between military and civilian communities. Advised by public affairs personnel, commanders provide direction and purpose for engagement with civilian communities. These activities involve collaborating with groups of people affiliated by geographic proximity or special interests to enhance the understanding and support for the Army, Soldiers, and op-

(Information Advantage) IV. Influence

Ref: ADP 3-13, Information (Nov '23), chap. 6.

See p. 2-19 for discussion of influence from a joint doctrine perspective (JP 3-04).

To influence is to shape or alter the opinions, attitudes, and ultimately the behavior of threats and other foreign relevant actors. As a form of contact, Army forces influence threats to decrease their combat effectiveness, erode organizational cohesion, diminish will, and deceive threats about friendly intent. Army forces influence selected foreign audiences to increase support, decrease potential interference with Army operations, and undermine threat attempts to influence those same audiences.

The friendly force garners an information advantage by using information to influence the behavior of foreign relevant actors more effectively than an adversary or enemy does. The influence information activity contributes to this advantage through two related tasks: influence threat perception and behaviors and influence other foreign audiences as shown in Figure 6-1.

Influence

I Influence Threat Perception & Behaviors

II Influence Other Foreign Audiences

Note: U.S. audiences are not targets for military activities intended to influence.

Purpose: Affect Behavior of Foreign Relevant Actors

Ref: ADP 3-13 (Nov '23), fig. 6-1. Tasks and purpose of the influence information activity.

I. Influence Threat Perception and Behaviors

Influence information activities by Army forces, integrated into the combatant commander's campaign plan, support setting a theater, challenge threat activities, and facilitate campaign objectives. During competition and crises, influence efforts deter threat actions and erode threat cohesion and effectiveness.

During armed conflict, influence activities disrupt or corrupt enemy forces' understanding and decision making, decrease their combat effectiveness, erode command and control (C2), and degrade morale and will.

A commander's ability to integrate disparate capabilities and synchronize application in the human, information, and physical dimensions is critical to influencing threat behavior. Commanders understand their higher echelon commander's intent and concept of operations and so employ their joint and Army capabilities in ways that support making the threat act or react in a desired manner. Tasks specifically designed to influence threat perceptions and behavior include—

Influence Threat Perception and Behaviors

A. Conduct Deception Activities
B. Conduct Military Information Support Operations (MISO)

A. Conduct Deception Activities *(See pp. 3-27 to 3-32.)*

Surprise is a combat multiplier that amplifies the effects of the other principles of war and provides a relative advantage where none previously existed. Its effective use allows friendly units to strike at a time and place or in a manner for which the enemy is unprepared, which induces shock and causes hesitation. Surprise seldom lasts for long periods because enemies adapt, so rapidly exploiting the opportunities surprise affords is critical. Every echelon works to achieve surprise during an operation.

One way to achieve surprise is to use deception. Deception is the act of causing someone to accept as true or valid what is false. Army forces conduct deception activities to cause enemy decision makers to act or not act in ways prejudicial to themselves and favorable to achieving friendly objectives.

Army forces support or conduct three types of deception:

- **Military Deception (MILDEC).** Military deception is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-13.4).
- **Tactical Deception (TAC-D).** Army forces conduct TAC-D to cause the enemy to react or falsely interpret friendly operations. Tactical deception is a friendly activity that causes enemy commanders to take action or cause inaction detrimental to their objectives (FM 3-90). Properly planned and executed TAC-D helps Army forces to hide what is real and display what is false.
- **Deception in Support of Operations Security (DISO)** *(See p. 3-28.)*

B. Conduct Military Information Support Operations *(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). MISO can degrade enemy combat power, reduce civilian interference, minimize collateral damage, and increase a population's support for operations.

MISO focus on information and indicators to convey meaning and to influence specific target audiences—individuals or groups selected for influence. The Secretary of Defense approves all MISO programs submitted as part of combatant commander campaign and contingency plans. Combatant commanders plan and execute MISO in support of theater objectives. Within this framework, psychological operations (PSYOP) units execute MISO programs in support of combatant commanders, subordinate joint task forces, the theater special operations command, and Army forces. MISO programs directed at enemy forces focus on themes, such as—

- Degrading enemy combat power by encouraging surrender, desertion, and malingering.
- Reducing the will of the enemy to resist.
- Degrading the decision-making abilities and operational effectiveness of the enemy.
- Exploiting and amplifying friendly successes on the battlefield.
- Exploiting and amplifying enemy failures and actions on the battlefield.

Army PSYOP forces are trained and equipped to conduct MISO.

(Information Advantage) V. Attack

Ref: ADP 3-13, Information (Nov '23), chap. 7.

See p. 2-19 for discussion of "attack" from a joint doctrine perspective (JP 3-04).

The threat is increasingly reliant on space, cyberspace, and the electromagnetic spectrum (EMS) for intelligence, surveillance, and reconnaissance (ISR); target acquisition; fire control; communications; and C2. Threat forces increasingly communicate (human to human, human to machine, and machine to machine) through the cyberspace domain. The cyberspace domain consists of the network and information technology infrastructures, resident data, the internet, telecommunications networks, computer systems, processors, and portions of the EMS that facilitate or inhibit them. Threats also employ information warfare capabilities through space, cyberspace, and the EMS to attack friendly data, information, and communications and to spread propaganda.

Affecting the threat's ability to use data and information to communicate, command, and control its forces or conduct information warfare provides the friendly force an advantage. The attack information activity contributes to this advantage through two related tasks: degrade the threat's ability to exercise C2 and affect threat information warfare capabilities as shown in Figure 7-1.

Attack

I **Degrade Threat Command and Control**

II **Affect Threat Information Warfare Capabilities**

Purpose: Affect Threat Command and Control

Ref: ADP 3-13 (Nov '23), fig. 7-1. Task and purpose of the attack information activity.

While both attack tasks affect the threat's use of data and information, each task has a different focus. Degrading threat C2 focuses on negatively affecting threat situational understanding, networks, and information systems. Affecting threat information warfare capabilities focuses on protecting friendly forces from threat cyber and electromagnetic attacks and contributes to a broader joint and national effort in attacking threat disinformation, propaganda, and legitimacy.

Information Attack Methods

Threat C2 nodes (command post [CP], signal centers, networks, and information systems); ISR sensors and systems; and fire control and target acquisition radars and systems are often high-payoff targets for Army forces. As part of the concept of operations and scheme of fires, Army forces attack these targets through a combination of methods: physical destruction, electromagnetic attack (EA), cyberspace attack, and offensive space operations.

See following pages (pp. 1-50 to 1-51) for an overview and further discussion.

Information Attack Methods

Ref: ADP 3-13, Information (Nov '23), pp. 7-2 to 7-5.

Army leaders combine available organic, joint, and multinational capabilities in complementary and reinforcing ways to create and exploit an information advantage.

Note. Additional classified capabilities, activities, and programs exist that can affect threat C2, networks, and systems. Technical effects are one or more capabilities, activities, or programs planned, coordinated, or executed that utilize classified means to accomplish an objective or enable military operations. Commanders requiring the execution of technical effects for an operation should understand that authorities and approvals generally reside at the combatant command or higher level and will often require long lead times for approval and execution.

Physical Destruction

In the context of information attack, physical destruction is the application of fires and maneuver to affect threat C2 and communications. Targets for physical destruction range from enemy CPs and communications centers to sensor and fire control systems. During armed conflict, commanders direct or coordinate for surface-to-surface fires, air-to-surface fires, and surface-to-air fires against threat C2, ISR, and information warfare targets. Commanders also direct maneuver forces to conduct raids and other offensive operations to seize or destroy enemy C2 nodes.

Physical destruction capabilities are inherent in combined arms formations and often provide more immediate results than employing other methods of attack. Depending on the echelon, organic indirect fires, to include mortars, cannons, rockets, and missiles, are well suited to destroy threat C2 nodes. Attack aviation and ground maneuver units can also execute physical destruction tasks focused on a threat C2 system. Army forces likewise nominate threat C2 and ISR targets to the joint force commander for physical destruction. Depending on priority, the joint force may attack these targets with fires or special operations forces.

Commanders and staffs consider rules of engagement, availability of assets and munitions, the potential for collateral damage, and the impact on escalation when directing physical destruction. At brigade and below echelons, physical destruction of the enemy's communications equipment can effectively create an advantage. At echelons above brigade, physical destruction is often combined with EA and cyberspace attacks to affect threat situational understating and the threat's ability to exercise C2.

Electromagnetic Attack (EA) *(See p. 3-56.)*

Threat forces rely on communications equipment using broad portions of the EMS to conduct operations. This equipment allows threats to talk, transmit data, provide navigation and timing information, and to exercise C2. Threat forces also collect signals in the EMS to build understanding and to target friendly forces and equipment. EA prevents or reduces an enemy's effective use of the EMS by employing jamming and directed-energy weapon systems against enemy spectrum-dependent systems and devices.

Electromagnetic attack is a division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). EA systems and capabilities include—

- Jammers.
- Directed energy weaponry.
- Radio frequency emitters.
- Technical means of deception.
- Antiradiation missiles.

Cyberspace Attacks *(See p. 3-54.)*

Cyberspace attacks are actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires (JP 3-12). Cyber forces execute cyberspace attacks through defensive cyberspace operations-response actions (known as DCO-RA) and offensive cyberspace operations (known as OCO). Cyberspace attacks require coordination with other U.S. Government departments and agencies and careful synchronization with other lethal and nonlethal effects through the targeting processes.

Cyberspace attacks are executed under the authority of the Secretary of Defense. The effects from these attacks provide windows of opportunity Army forces can exploit. For example, the joint force commander times cyberspace attacks to affect threat air defense and fire control systems so that they do not interfere with joint and Army forces attacking in a specific area. Additionally, the joint force commander may provide direct offensive cyberspace operations support to corps and below Army commanders in response to requests via the joint targeting process.

Cyberspace attack actions create denial effects in cyberspace or manipulation in cyberspace to create denial effects in the physical dimension. In some cases, cyberspace attack actions can lead to physical destruction. Cyberspace attacks affect physical processes when they modify or destroy cyberspace capabilities that control the physical process. Some examples of effects created by a cyberspace attack include—

- Deny.
- Disrupt.
- Destroy.
- Manipulate.

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

Space capabilities enable joint and Army operations. Space capabilities include space situational awareness; positioning, navigation, and timing; satellite communications; satellite operations; missile warning; environmental monitoring; space-based surveillance and reconnaissance; defensive space operations; and offensive space operations. Army space planners at all echelons advise commanders on the current space assessment and ways to coordinate for and integrate space capabilities and effects into operations.

Space operations enable freedom of action in the space domain for the United States and its allies. Offensive and defensive space operations, including navigation warfare, enable freedom of action in space and counter efforts to interfere with or attack space forces of the United States, allies, or commercial partners.

- **Offensive Space Operations.** Offensive space operations are actions taken to negate attacks against U.S. and friendly space assets and threat freedom of action. Measures include actions against ground, data link, and space segments or users to affect an enemy's space systems, or to thwart hostile interference on U.S. and multinational space systems:
  - Deceive
  - Disrupt
  - Deny
  - Degrade
  - Destroy.
- **Navigation Warfare.** Navigation warfare aims to ensure unimpeded access to the Global Navigation Satellite System for joint forces and multinational partners while denying it to the enemy. It encompasses various offensive, defensive, and support activities (such as surveillance, reconnaissance, and EMS management) to ensure unimpeded availability and integrity of positioning, navigation, and timing information.

I. Degrade Threat Command and Control

To degrade means to reduce or to lower. Army forces create and exploit every opportunity to degrade the threat's ability to exercise C2. As with the friendly forces, information is a central resource for the threat to exercise C2. Threats collect information, process and analyze it to understand, and use it to inform decisions. Before a threat actor can make a decision, an Army force aims to prevent, delay, or alter that threat's decisions by degrading its access to information, manipulating the information available, or overwhelming its systems and processes with large amounts of information. After a threat decision is made, an Army force aims to prevent, alter, or limit the threat force's ability to execute military actions by attacking threat C2 nodes, networks, and information systems. Limiting the information available to an enemy or adversary while also inhibiting the ability to exchange what information it does have thus provides significant military advantage.

The protect information activity contributes to degrading threat C2 by denying the threat's access to friendly data and information (see pp. 1-29 to 1-34). The influence information activity contributes to degrading threat C2 by affecting threat perceptions (see pp. 1-45 to 1-46).

The attack information activity degrades threat C2 by—

A. Affect Threat Understanding of an Operational Environment

Threat decision makers use information from a variety of sources to make decisions. Threat decision makers may rely on traditional intelligence sources—such as geospatial intelligence, human intelligence, and signals intelligence—as well as information gained through cyberspace reconnaissance, social media exploitation, and collection of publicly available information. Staffs often process and analyze this information by both technical and human means before it reaches the decision maker. Each source of information and each step in this information process represent an opportunity for Army forces to impact the threat's decision making.

Commanders should consider all ways and means to affect the threat's ability to build and maintain situational understanding. Within the attack information activity, commanders direct or coordinate for physical destruction, EA, cyberspace attack, and technical effects to—

- **Disrupt or deceive** sensors that provide threat actors with intelligence.
- **Disrupt or manipulate** data transmissions among threat sensors, analysis capabilities, and decision makers.
- **Deceive** threat decision makers about friendly intentions and capabilities.
- **Disrupt or manipulate** communication between threat decision makers and units.

Note. In some instances, Army commanders may want to deter threat actions by improving the threat's understanding of friendly capabilities and intent.

B. Affect Threat Networks and Systems

Army commanders use many military capabilities to affect threat networks and systems. The type of capabilities a commander employs depends on the objective, the type of target system, acceptable levels of risk, and the strategic context. Commanders carefully consider what parts and the duration of threat networks and systems they desire to affect. In some instances, commanders want the threat to see and communicate the activities of friendly forces. In other instances, they may want to degrade certain networks and systems for a specified time. Commands may focus attacks on disintegration by targeting. In these instances, units target key nodes

(Information Advantage) Integration

Ref: ADP 3-13, Information (Nov '23), chap. 8.

I. Joint and Multinational Information Advantage

Gaining and exploiting information advantages is a whole of government, joint, and multinational effort requiring unified action. Unified action is the synchronization, coordination, or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1, Volume 1). Unity of effort is the coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization that is the product of successful unified action (JP 1, Volume 2). To facilitate unified action, Army commanders and supporting staff must understand the roles, capabilities, and processes of U.S. government, joint, and multinational organizations involved in creating and exploiting information advantages. (See paragraphs 1-13 through 1-20 for a discussion of informational power employed by the U.S. government.)

A. Information Joint Function *(See pp. 2-7 to 2-20.)*

The information joint function is the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior, and to support human and automated decision making. Combined with the other joint functions (command and control [C2], intelligence, fires, movement and maneuver, protection, and sustainment), the information joint function helps joint force commanders and staffs effectively use information during operations across the competition continuum. The primary joint tasks are—

- Understand how information impacts the operational environment (OE).
- Support human and automated decision making.
- Leverage information.

Joint Information Advantage *(See p. 2-1.)*

When the joint force successfully executes the tasks and subtasks associated with the information joint function, the joint force gains information advantages. Joint doctrine describes information advantage as the operational advantage gained through the joint force's use of information for decision making and its ability to leverage information to create effects in the information environment. The joint force applies information power to create and exploit information advantages in two primary ways:

- Planning and executing all operations, activities, and investments with deliberate intent to leverage its inherent informational aspects.
- Employing specially trained units to conduct joint operations in the information environment (OIE).

Leveraging the Inherent Informational Aspects of Operations *(See pp. 2-10 to 2-11.)*

Joint force action impacts the OE either intentionally or incidentally. All joint force operations, activities, and investments can affect the behavior of relevant actors. The conclusions that observers draw from interpreting joint force activities may drive

Integration of the Information Activities

Ref: ADP 3-13, Information (Nov '23), pp. 8-11 to 8-18 (table 8-1).

Each information activity and correlating subordinate tasks have staff leads. Information task leads assist the five information activity leads in integrating information tasks as depicted in Table 8-1. Most staff work occurs within the functional and integrating cells. The functional cells include intelligence, movement and maneuver, fires, protection, and sustainment. The integrating cells include current operations, future operations, and plans.

Activity Lead	***Enable***	***Task Leads***
Chief of staff	Establish, operate, and maintain C2 systems.	G-6 and KMO
	Execute the operations process and coordinate across echelons.	G-3
	Conduct the integrating processes.	Integrating process leads: G-2, G-3, chiefs of fires, chief of protection, and KMO
	Enhance understanding of an operational environment.	G-2
Activity Lead	***Protect***	***Task Leads***
Chief of Protection	Secure and obscure friendly information.	OPSEC officer
	Conduct security activities.	G-3
	Defend the network, data, and systems.	G-6
Activity Lead	***Inform***	***Task Leads***
PAO	Inform and educate Army audiences.	Army leaders and PAO
	Inform United States domestic audiences.	PAO
	Inform international audiences.	PAO
Activity Lead	***Influence***	***Task Lead***
G-3	Influence adversary and enemy perceptions and behaviors.	G-39
	Influence other foreign audiences.	
Activity Lead	***Attack***	***Task Lead***
G-3	Degrade threat command and control	Chief of Fires (DFSCOORD)
	Affect threat information warfare.	

C2	command and control	G-39	assistant chief of staff, information plans and operations
DFSCOORD	deputy fire support coordinator	OPSEC	operations security
G-2	assistant chief of staff, intelligence	KMO	knowledge management officer
G-3	assistant chief of staff, operations	PAO	public affairs officer
G-6	assistant chief of staff, signal		

While most staff work occurs in the functional and integrating cells, successfully integrating the information activities into operations occurs when functional expertise from across the staff comes together in support of the commander's decision requirements. This occurs in integrating cells and when the commander directs temporary groupings of staff members in boards, working groups, and planning teams.

Army forces require authorities to conduct operations. Some information tasks—to include MISO, cyberspace operations, and some types of deception activities—illustrate activities requiring specific authorities. When execution authority is granted for these operations, the command may have to meet specific reporting requirements. The staff judge advocate verifies authorities required to execute required information tasks have been granted by the appropriate authority prior to execution.

The information task leads use established boards, working groups, and planning teams in conjunction with the integrating processes to incorporate the five information activities into the operations process. The operations assessment, plans synchronization, and targeting boards are examples of boards typically found within a unit's battle rhythm that help to integrate information tasks. The assessment, cyberspace electromagnetic activities, civil-military operations, information collection, knowledge management, protection, and targeting working groups exemplify working groups typically found within a unit's battle rhythm.

B. Preparing *(See 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. It requires commander, staff, and Soldier actions to ensure the force is ready to execute operations. Preparing to execute information tasks often requires Army forces to anticipate and account for requirements earlier than many other Army tasks. This is because some information tasks require additional coordination or lead times to create desired effects. Some types of preparation begin at home station during competition, for example, configuring and training various information systems. In other cases, units assigned to a combatant commander may already be conducting information activities to support the commander's campaign objectives during competition which will enable friendly operations in a crisis or during conflict.

Successful preparation enables leaders to—

- Improve situational understanding.
- Develop a common understanding of the plan.
- Train and become proficient on critical tasks.
- Task-organize and integrate the force.
- Maintain unit resiliency.
- Ensure forces and resources are positioned.
- Protect critical aspects of operations.

Preparation to execute information activities takes place within headquarters and by units across the Army. The staff executes various activities in preparation to integrate and assess information activities during execution. Some of these activities include—

- Continuing to revise and refine planned information tasks and support development of branches and sequels.
- Conducting external coordination and establishing liaison to integrate echelons and synchronize information tasks.
- Assessing ongoing information collection and updating information requirements.
- Tracking and monitoring the movement and integration of units executing specific information tasks.
- Coordinating for the necessary authorities to execute anticipated information tasks.
- Helping subordinate commanders to understand specified and implied information activities and tasks.
- Participating in rehearsals to ensure information tasks are synchronized with the concept of operations.
- Assessing and mitigating vulnerabilities created through inadvertent information signatures.

Some unit preparations include ensuring that friendly forces—

- Can identify misinformation and disinformation.
- Can identify threat information disruption or information attacks.
- Understand relevant actors within their assigned areas.
- Understand how to report relevant information.
- Understand what actions to take to reinforce the prevailing narrative.
- Understand how to reduce risks associated with friendly emission in the electromagnetic spectrum (EMS).
- Understand potential impacts of friendly use of EW capabilities on friendly communications.

Chap 2

I. Joint Force Uses of Information

Ref: JP 3-04, Information in Joint Operations (Sept '22), chap. 2.

I. Military Operations and Information

Information is a resource of the informational instrument of national power at the strategic level. Information is also a critical military resource. The joint force uses information to perform many simultaneous and integrated activities. The joint force uses information to improve understanding, decision making, and communication. Commanders use information to visualize and understand the OE and direct and coordinate actions. The joint force leverages information to affect the perceptions, attitudes, decision making, and behavior of relevant actors. The joint force employment of information is of central importance because it may provide an operational advantage.

II. The Operational Environment (OE) and the Information Environment (IE)

An OE is the aggregated conditions, circumstances, and influences that affect the employment of forces and bear on the decisions of a commander. Each commander's OE is different from every other commander's OE.

Within the OE there exist factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information. We refer to the aggregate of social, cultural, linguistic, psychological, technical, and physical factors as the IE.

The IE is not distinct from any OE. It is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decisions of the commander.

The joint force plans and conducts activities and operations that have inherent informational aspects that will impact the factors that make up the IE. The joint force must account for those informational aspects so that joint force activities and operations affect the OE in a way that supports the JFC's objectives. Additionally, to ensure unity of effort among different commands, each JFC must consider and communicate how the informational aspects of their planned activities and operations may impact the factors that make up the IE to affect other OEs.

III. Information Advantage

Information advantage is the operational advantage gained through the joint force's use of information for decision making and its ability to leverage information to create effects on the IE. Commanders achieve this advantage in several ways: identifying threats, vulnerabilities, and opportunities along with understanding how to affect relevant actor behavior; obtaining timely, accurate, and relevant information with an ascribed level of confidence or certainty for decision making and the impact of decision making; influencing, disrupting, or degrading the opponent's decision making; protecting the joint force's morale and will; and degrading the morale and will of adversaries. The joint force exploits these advantages through the conduct of operations. For example, disabling an opponent's space-based assets might provide the joint force with the operational advantage of being able to communicate securely over long distances without interruption and of being able to move without being detected. The joint force could then exploit that advantage through an operation to destroy an enemy ground force. Likewise, gaining and maintaining sufficient goodwill among a

JP 3-04, Information in Joint Operations, Sept '22 (Summary of Changes)

Joint publication (JP) 3-04 guides how the joint force considers and uses information to support achieving its objectives. This JP identifies the operational significance of information in achieving commanders' objectives across the competition continuum. This publication is the result of a change in mindset based on the joint force's recognition that all activities have inherent informational aspects that impact the operational environment (OE) and can generate effects that may contribute to or hinder achieving commanders' objectives. The Department of Defense (DOD), in coordination with the other United States Government (USG) departments and agencies, supports the informational instrument of national power by using information to impact the way in which humans and systems behave or function. The joint force leverages information across the competition continuum to assure, deter, compel, and force relevant actor behaviors that support US interests.

Joint Force Transition from "Information Operations" (IO) to "Operations in the Information Environment" (OIE)

The establishment of the information joint function and the development of joint publication (JP) 3-04 on information in joint operations is driving changes across joint and Service DOTMLPF-P [doctrine, organization,training, materiel, leadership and education, personnel, facilities, and policy]. **One significant doctrinal change is the transition from joint information operations (IO) to operations in the information environment (OIE).** This transition is a substantial force development challenge requiring the joint force to evaluate how to organize forces and staffs to deliberately plan and execute OIE.

The Armed Forces of the United States are poised to fight and win the Nation's wars. Transregional, all-domain, and multifunctional threats require the joint force to conduct operations across the competition continuum to prevent armed conflict and set the conditions to prevail during armed conflict. To deter or defeat these threats and achieve strategic objectives, the joint force commander (JFC) should understand how information impacts the OE, use information to support human and automated decision making, and leverage information through offensive and defensive actions to affect behavior. Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors can affect the success of a particular campaign, operation, or tactical action.

The joint force can win tactical fights during armed conflict but has not always been able to translate victories into enemy behaviors that lead to intended, enduring, strategic outcomes. Defeat of an enemy, by whatever mechanism, is usually a psychological outcome. The enemy is not really defeated until they believe they are defeated. Even in operations without an enemy or adversary, such as foreign humanitarian assistance, successful outcomes hinge on the perceptions, attitudes, beliefs, and other drivers of behaviors of the affected population.

The joint force cannot rely on attrition or its ability to compel behavior through the use of destructive and disruptive lethal force. To support achieving the commander's objectives, the joint force deliberately leverages information through activities that inform audiences; influence foreign relevant actors; and attack and exploit information, information networks, and information systems.

JP 3-04, Information in Joint Operations CANCELS JP 3-13, Information Operations

This supersedes and cancels JP 3-13, Information Operations, 27 November 2012 Incorporating Change 1, 20 November 2014. Relevant material from JP 3-13 has been incorporated into the main body and appendices of this publication. Accordingly, JP 3-13, Information Operations, will be removed from the joint doctrine hierarchy.

Joint IO, as defined and practiced, had shortcomings that inhibited it from contributing to the commander's application of informational power. As defined, IO focused on the integration of information-related capabilities (IRCs) to affect the decision making of adversaries and potential adversaries, and effectively ignored other relevant actors that shape the strategic and operational environments. IO planning concentrated on the employment of those IRCs in support of broader joint force operations, ignoring planning for the inherent informational aspects of all activities.

JP 3-04 describes how the joint force applies informational power across the competition continuum. That application of informational power includes both the deliberate leveraging of the inherent informational aspects of activities as an imperative for all joint force operations, and the conduct of OIE. OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by: informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems. As such, OIE are distinct from, but complementary to, the joint forces' deliberate leveraging of the inherent informational aspects of military activities during all operations.

OIE calls for formations with the capabilities (i.e., the authorities and tools, as well as subject matter experts possessing in-depth skills, knowledge, and abilities to employ those tools) required to carry out actions that leverage information to affect behavior. Building and resourcing organizations with subject matter experts and tools is part of the joint and Service force development challenge.

JP 3-04, Information in Joint Operations, 14 September 2022, Active Terms and Definitions

Information Environment (IE). The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. Also called IE. (Approved for incorporation into the DOD Dictionary.)

Knowledge Management (KM). A discipline that integrates people and processes to create shared understanding, increased organizational performance, and improved decision making. Also called KM. (Approved for inclusion in the DOD Dictionary.)

Operations in the Information Environment (OIE). Military actions involving the integrated employment of multiple information forces to affect drivers of behavior. Also called OIE. (Approved for inclusion in the DOD Dictionary.)

Relevant Actor (RA). Individual, group, population, or automated system whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action. (Approved for inclusion in the DOD Dictionary.)

Target Audience (TA). An individual or group selected for influence. Also called TA. (Approved for incorporation into the DOD Dictionary.)

Terms Removed from the DOD Dictionary

Supersession of JP Supersession of JP 3-13, Information Operations, 27 November 2012; Incorporating Change 1, 20 November 2014:

- Information operations
- Information operations intelligence integration
- Information-related capability
- Information superiority

II. Information (as a Joint Function)

Ref: JP 3-0, Joint Campaigns and Operations (Jun '22), chap. III.

A **joint function** is a grouping of capabilities and activities that enable JFCs to synchronize, integrate, and direct joint operations. A number of subordinate tasks, missions, and related capabilities help define each function, and some tasks and systems could apply to more than one function.

There are seven joint functions common to joint operations: **C2, information, intelligence, fires, movement and maneuver, protection, and sustainment**. Commanders leverage the capabilities of multiple joint functions during operations. The joint functions apply to all joint operations across the competition continuum and enable both traditional warfare and IW, but to different degrees, conditions, and standards, while employing different tactics, techniques, and procedures.

I. Information (as a Joint Function)

The elevation of information as a joint function impacts all operations and signals a fundamental appreciation for the military role of information at the strategic, operational, and tactical levels within today's complex OE.

The **information function** encompasses the management and application of information to support achievement of objectives; it is the deliberate integration with other joint functions to change or maintain perceptions, attitudes, and other elements that drive desired relevant actor behaviors; and to support human and automated decision making. The information function helps commanders and staffs understand and leverage the prevalent nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to preserve friendly information and leverage information and the inherent informational aspects of military activities to achieve the commander's objectives. The information joint function provides an intellectual framework to aid commanders in exerting one's influence through the timely generation, preservation, denial, or projection of information.

All military activities have an informational aspect since most military activities are observable in the Information Environment (IE). 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 in the OE; failing to leverage those aspects in a timely manner may cede this advantage to an adversary or enemy. Leveraging the informational aspects of military activities can support achieving operational and strategic objectives. The information function also encompasses the use of friendly information to influence foreign audiences and affect the legitimacy, credibility, and influence of the USG, joint force, allies, and partners. Additionally, JFCs use friendly information to counter, discredit, and render irrelevant the disinformation, misinformation, and propaganda of other actors.

The information joint function helps commanders and their staffs understand and leverage the pervasive nature of information, its military uses, and its application across the competition continuum, to include its role in supporting human and automated decision making. Information planners should consider coordination activities not only within the information joint function but also among all other joint functions. The information joint function organizes the tasks required to manage and apply information during all activities and operations.

II. Information Use Across the Competition Continuum

Ref: JP 3-0, Joint Campaigns and Operations (Jun '22), pp. III-24 to III-26.

COOPERATIVE Use of Information

During day-to-day activities, the joint force integrates information in SC and FHA activities by:

- Assuring and maintaining allies, widening/publicizing combined exercises and other PN cooperation activities, encouraging neutral actors that the joint force is the partner of choice or that they should remain neutral, and reminding partners of benefits to maintain their support.
- Informing enemies and adversaries of benefits to friendly multinational force membership and collective defense, informing enemies and adversaries that the joint force is committed to its allies and security agreements, and concealing investment priorities and costs.

COMPETITIVE Use of Information

During competition, the joint force conducts activities against state or non-state actors with incompatible interests that are below the level of armed conflict. Competition can include military operations such as CO, special operations, demonstrations of force, CTF, and ISR and often depends on the ability to leverage the power of information through OIE. Expect additional time to coordinate and obtain approval from DOD or other USG departments and agencies to use information due to increased risk. Specific information tasks may include:

- Informing allies and partners of malign influence and antagonistic behavior.
- Declassifying and sharing images that reveal or confirm enemy or adversarial behavior, recommending allies and partners communicate to relevant audiences within their areas of influence, and educating the joint force and allies about online disinformation activities to build understanding and resilience against propaganda.
- Influencing adversary's audiences to prevent escalation to armed conflict by demonstrating joint force resolve, strength, and commitment, as well as the costs and expectations of response actions.
- Targeting adversarial information, networks, and systems by temporarily denying communication or Internet access, disrupting jamming of Internet access to its internal population, and partnering with private-sector communication companies to remove inappropriate enemy and adversarial recruiting and fundraising advertisements.

Use of Information in ARMED CONFLICT

In addition to the above tasks, the joint force can use information defensively or offensively. JFCs can employ information as independent activities, integrated with joint force physical actions, or in support of other instruments of national power. Many of these information activities require additional authorities as they present larger strategic risks or risks to the joint force, though capabilities like PA, which has the preponderance of public communication resources and rarely requires additional authorities in armed conflict.

Defensive Purposes. Basic defense activities include protecting data and communications, movements, and locations of critical capabilities and activities. PA can assist in countering adversary propaganda, misinformation, and disinformation. MILDEC can help mask strengths, magnify feints, and distract attention to false locations. DCO can defeat specific threats that attempt to bypass or breach cyberspace security measures. EW can protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the EMS. The management of EM signatures can mask friendly movements and confuse enemy intelligence collectors.

IV. Information Joint Function Tasks

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. II-6 to II-15.

The information joint function encompasses the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior and to support human and automated decision making. The information joint function is the intellectual organization of the tasks required to use information during all operations— understand how information impacts the OE, support human and automated decision making, and leverage information (see Figure II-1). JFCs and their staff perform these tasks during all operations to accomplish their respective missions.

Information Joint Function Tasks

A **Understand How Information Impacts the Operational Environment (OE)**

B **Support Human and Automated Decision Making**

C **Leverage Information**

A. Understand How Information Impacts the Operational Environment (OE) *(See pp. 0-8 to 0-10.)*

This task helps the joint force identify threats, vulnerabilities, and opportunities in the IE. It provides a foundation for, and supports the continued refinement of, joint intelligence preparation of the operational environment (JIPOE) products to improve the commander's decision making during planning, execution, and assessment of operations. There are three steps to understanding how information impacts the OE: analyzing of the informational, physical, and human aspects of the environment; identifying and describing relevant actors; and determining the most likely behaviors of relevant actors. These steps are continuous and iterative because the OE is always changing. Planners use the JIPOE products and inputs from other subject matter experts (SMEs) to understand the interrelationships between the informational, physical, and human aspects within the context of operational objectives. This task requires fusion of multi-source data from across, and external to, the joint force to achieve and maintain an understanding of how information impacts the OE. Sources of internally produced data for this task include inputs from intelligence, public affairs (PA), civil affairs (CA), cyberspace forces, psychological operations units, and C2 systems. Sources of information external to the joint force include USG departments and agencies, businesses, and academic communities, as well as foreign governments, international organizations, nongovernmental organizations (NGOs), and various traditional and nontraditional media sources. This task also relies on language, regional, and cultural expertise to help avoid mirror-imaging and other forms of bias.

Analysis of the Informational, Physical, and Human Aspects of the Environment

Understanding how information impacts the environment and identifying how it can be used to affect behavior requires analysis of the increasingly complex and dy-

C. Leverage Information *(See pp. 2-10 to 2-11 and 2-41.)*

When commanders leverage information, they expand their range of options for the employment of military capabilities beyond the use of or threatened use of physical force. JFCs leverage information in two ways. First, by planning and conducting all operations, activities, and investments to deliberately leverage the inherent informational aspects of such actions. Second, by conducting OIE.

INFORM Domestic, International, and Internal Audiences

Inform activities are the release of accurate and timely information to the public and internal audiences, to foster understanding and support for operational and strategic objectives by putting joint operations in context; facilitating informed perceptions about military operations; and countering misinformation, disinformation, and propaganda. Inform activities help to ensure the trust and confidence of the US population, allies, and partners in US and MNF efforts; and to deter and dissuade adversaries and enemies from action. PA is the primary means the joint force uses to inform; however, civil-military operations (CMO), key leader engagement (KLE), and military information support operations (MISO) also support inform efforts.

See pp. 1-35 to 1-44 for related discussion from ADP 3-13.

INFLUENCE Relevant Actors

The purpose of the influence task is to affect the perceptions, attitudes, and other drivers of relevant actor behavior. Regardless of its mission, the joint force considers the likely psychological impact of all operations on relevant actor perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation to create desired effects that include maintaining or preventing behaviors or inducing changes in behaviors. This may include the deliberate selection and use of specific capabilities for their inherent informational aspects (e.g., strategic bombers); adjustment of the location, timing, duration, scope, scale, and even visibility of an operation (e.g., presence, profile, or posture of the joint force); the use of signature management and MILDEC operations; the employment of a designated force to conduct OIE; and the employment of individual information forces (e.g., CA, psychological operations forces, cyberspace forces, PA, combat camera [COMCAM]) to reinforce the JFC's efforts. US audiences are not targets for military activities intended to influence.

See pp. 1-45 to 1-48 for related discussion from ADP 3-13.

ATTACK AND EXPLOIT Information, Information Networks, and Information Systems

The joint force targets information, information networks, and information systems to affect the ability of adversaries and enemies to use information in support of their own objectives. This activity includes manipulating, modifying, or destroying data and information; accessing or collecting adversary or enemy information to support joint force activities or operations; and disrupting the flow of information to gain military advantage. Attacking and exploiting information, information networks, and information systems supports the influence task when it undermines opponents' confidence in the sources of information or the integrity of the information that they rely on for decision making. Activities used to attack and exploit information include offensive cyberspace operations (OCO), electromagnetic warfare (EW), MISO, and CA operations. PA also contributes to this task by publicly exposing malign activities.

See pp. 1-49 to 1-56 for related discussion from ADP 3-13.

I. Service Organizations

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. III-23 to III-27.

The Services man, train, and equip organizations to provide the joint force with the ability to leverage information during joint operations and to conduct OIE. Those Service organizations provide distinct specialized capabilities to the joint force (e.g., MISO, CMO, CO, PA, EW, COMCAM) or provide information commands composed of multiple specialized capabilities that focus on leveraging information and enable the joint force to create effects in the IE. Those Service-provided organizations that are trained and equipped to conduct OIE are referred to as OIE units.

United States Army

- Army Cyber Command (ARCYBER).
- 1st IOC [1st Information Operations Command] (Land).
- United States Army Special Operations Command (USASOC).
- United States Army Civil Affairs and Psychological Operations Command.
- The United States Army National Guard TIOG.

United States Navy

- United States Fleet Cyber Command (US FCC)/United States Tenth Fleet. US FCC reports directly to the Chief of Naval Operations as a Navy Echelon 2 command and is assigned to USCYBERCOM.
- United States Naval Information Forces (NAVIFOR). NAVIFOR mans, trains, and equips information warfare capabilities ashore and afloat.

USMC

- DC I [Deputy Commandant for Information].
- Marine Corps Forces Cyberspace Command (MARFORCYBER). MARFORCYBER is assigned to USCYBERCOM and conducts the full spectrum of CO.
- Marine Expeditionary Force Information Group (MIG). MIGs coordinate, integrate, and employ capabilities to ensure the MAGTF commander's ability to facilitate friendly forces maneuver and deny the enemy freedom of action in the IE.
- Marine Corps Information Operations Center (MCIOC). The MCIOC provides operational support to the Marine Corps forces and MAGTFs and provides OIE subject matter expertise in support of USMC OIE advocates and proponents to enable the effective integration of OIE into Marine Corps operations.
- Civil Affairs Group (CAG).

United States Air Force

- 16th AF [Sixteenth Air Force]/Air Force Cyber Command [AFCYBER]. 16th AF is responsible for developing, preparing, generating, employing, and presenting information warfare forces.
- 616th OC [616th Operations Center]. The 616th OC handles daily intelligence-gathering and offensive and defensive missions in the air, in cyberspace, and across the EMS.
- 16th AF Information Warfare Cell.

United States Space Force (USSF)

- Space Delta 6 CO. Space Delta 6, as part of Space Operations Command (SPOC), executes CO to protect space operations, networks and communications.
- Space Delta 8 Satellite Communications and Navigational Warfare. Space

IV. The Joint Force

The JFC establishes and communicates command-specific guidance to ensure all joint force operations and activities are planned and executed to account for the effective management and application of information. This will include assigning responsibility for the tasks related to the information joint function. This may include standardizing organizational practices, establishing routine working groups, or establishing a center with responsibility for the information joint function tasks. Each of the directorates has responsibility related to information joint function tasks, but the JFC should assign overall responsibility and authority to a staff lead to ensure unity of effort. The JFC may choose to create additional staff or functional organizations to conduct or coordinate joint force activities related to the leveraging of information, coordinate with other organizations to obtain support, or synchronize activities with other organizations. This includes creating groups of specialized forces to conduct OIE. The JFC may choose to retain control of any newly created formation under the operations directorate of a joint staff (J-3) or create a separate task force. From this point forward, “OIE unit” will be used to represent a formation that conducts OIE. The JFC also identifies requirements for information planners to serve as OIE and capability SMEs and planners on the joint force staff or other headquarters staffs. During operational design and joint planning, the JFC provides planning guidance that describes the desired conditions that must exist in the IE to support mission accomplishment, how the joint force will leverage the inherent informational aspects of its activities to support the JFC’s objectives, how information activities will support the scheme of maneuver, and the types and level risk that the JFC will accept in the IE. The JFC will also assign missions to OIE units.

A. JFC’s Staff

The JFC’s staff performs duties and handles special matters over which the JFC wishes to exercise close, personal control. JFCs and their staffs evaluate communication considerations with the interagency partners when planning joint operations. The staff advises the JFC on the inherent informational aspects of their activities, including how words and images will impact the JFC’s operational areas. The staff also advises the JFC when their activities may have effects on the IE that impact other AORs. The chief of staff (COS) manages the staff. The staff group may include, but is not limited to, the PAO, staff judge advocate (SJA), KM officer, and POLAD.

- **Political Advisor (POLAD)**. POLADs are senior DOS officers (often flag-rank equivalent) detailed as personal advisors to senior US military leaders and commanders, and they provide policy analysis and insight regarding the diplomatic and political aspects of the commanders’ duties. Due to their status and contacts, they can enable interorganizational cooperation relationships and foster unity of effort. The POLAD provides USG foreign policy perspectives and diplomatic considerations and establishes links to US embassies in the AOR or joint operations area (JOA) and with DOS. They articulate DOS objectives relevant to the CCMD’s theater strategy or JTF commander’s plans.
- **Public Affairs Officer (PAO)**. The PAO is the commander’s principal spokesperson, senior PA adviser, and a member of the CCDR’s personal staff. In that role, the PAO provides counsel to leaders, leads PA and communication activities, collaborates with other information planners to develop the narrative, supports the commander’s intent, and supports community engagement and KLE. The PAO may also co-chair the JFC’s information CFT.
- **Joint Force Staff Judge Advocate (SJA).** The joint force SJA, also titled the command judge advocate, is the principal legal advisor to the CCDR, with a focus on joint operational law issues pertaining to their commander’s AOR.

Each joint staff directorate collaborates routinely, but to varying degrees, to plan, synchronize, support, and assess activities that leverage information.

Joint Organizations

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. III-14 to III-15.

The following joint organizations perform functions that support the joint force use and leveraging of information:

Joint Information Operations Warfare Center (JIOWC)

The JIOWC is a CJCS-controlled activity under the supervision of the JS Director for Operations. JIOWC enables the application of informational power at the strategic level and performs CJCS proponency responsibilities for joint enterprise information and information activities, MILDEC, and OPSEC, to create, enhance, or protect joint force advantages in the IE.

Joint Planning Support Element-Public Affairs (JPSE-PA)

JPSE-PA, a functional group within JPSE, plans, coordinates, and synchronizes PA activities with informational power activities to maximize support to campaign objectives and ensure execution of PA roles, responsibilities, and fundamentals. JPSE-PA provides ready, rapidly deployable, expeditionary joint PA capability to CCDRs to support joint operations, facilitate the rapid establishment of joint force headquarters, and bridge joint requirements supporting worldwide operations. JPSE-PA personnel assist development, planning, assessment, and synchronization of operational and mission narratives, themes, messages, PA and VI activities with the national narrative.

Joint Warfare Analysis Center

The Joint Warfare Analysis Center provides CCMDs, the JS, and other customers with effects-based analysis and precision targeting options for selected networks and nodes to carry out the national security and military strategies of the United States during peace, crisis, and war.

Joint Electromagnetic Warfare Center (JEWC)

JEWC integrates joint effects in the electromagnetic spectrum (EMS) by providing adaptive operational solutions and advocating for the coherent evolution of capabilities and processes to control the EMS during military operations. The JEWC assesses EW requirements, technology, and capabilities while conducting modeling, analysis, and EMS activity coordination between CCMDs and other USG departments and agencies. The JEWC also deploys EW experts, trains staffs, stands up forward planning cells, and delivers rapid warfighter support when required.

Joint Intelligence Support Element (JISE)/Joint Intelligence Operations Center (JIOC)

The JISE provides the JTF with tailored intelligence products and services with a continuous analytical capability. Capabilities of the element may include order of battle analysis, collection management, target intelligence, OIE analysis, a warning intelligence watch, and a request for information (RFI) desk. Alternatively, in a particularly large or protracted campaign, the JTF commander may decide to employ an operational-level JIOC. An operational-level JIOC incorporates the capabilities inherent in a JISE but is generally more robust. The JISE can provide population-centric, socio¬cultural intelligence and physical network lay downs, including the information transmitted via those networks.

Defense Media Activity (DMA)

DMA is a mass media and training and education organization that creates and distributes DOD content across a variety of media platforms to audiences around the world.

Chap 2

IV. (OIE) Operations in the Information Environment

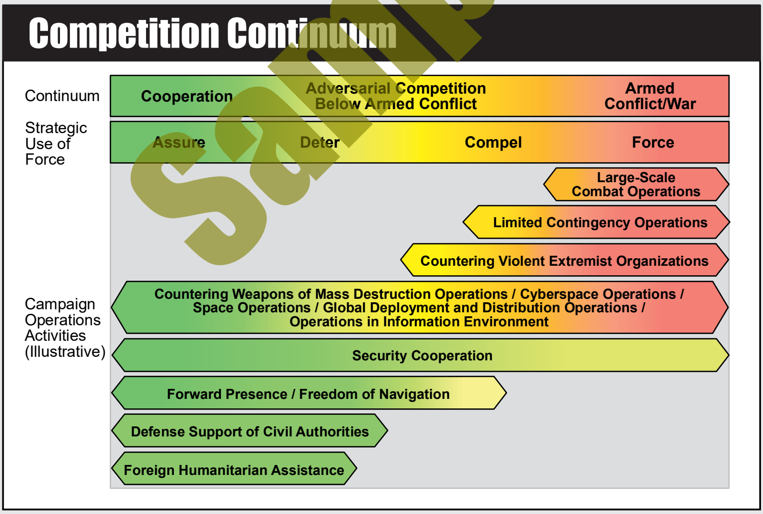
Ref: JP 3-04, Information in Joint Operations (Sept '22), chap. VII.

I. Operations in the Information Environment (OIE)

OIE are military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and by protecting friendly information, information networks, and information systems.

OIE Across the Competition Continuum *(See pp. 2-8 to 2-9.)*

Military operations vary in scope, purpose, and intensity in cooperation, adversarial competition below armed conflict, and armed conflict. Throughout the competition continuum, the JFC integrates **operations in the information envrionment (OIE)** into joint plans and synchronizes it with other operations to create desired behaviors, reinforce or increase combat power, and gain advantage in the IE. Each joint operation has a unique strategic context, so the nature of OIE and its activities will vary according to the distinct aspects of the mission and OE. While OIE may be conducted as an independent operation, it is never done in isolation. OIE are conducted throughout all campaigns or operations and at any level of conflict.


Competition Continuum
Continuum
Cooperation
Adversarial Competition Below Armed Conflict
Armed Conflict/War
Strategic Use of Force
Assure
Deter
Compel
Force
Large-Scale Combat Operations
Limited Contingency Operations
Countering Violent Extremist Organizations
Campaign Operations Activities (Illustrative)
Countering Weapons of Mass Destruction Operations / Cyberspace Operations / Space Operations / Global Deployment and Distribution Operations / Operations in Information Environment
Security Cooperation
Forward Presence / Freedom of Navigation
Defense Support of Civil Authorities
Foreign Humanitarian Assistance

Ref: JP 1 Vol. 1 (Jun '20), fig. II-1. Notional Competition Continuum.

OIE leverage information for the purpose of affecting the will, awareness, and understanding of adversaries and other relevant actors and denying them the ability to act in and through the IE to negatively affect the joint force, while protecting joint force will, awareness, understanding, and the ability to take actions in and through the IE.

OIE may provide commanders with a decisive advantage over adversaries by helping to maintain the credibility and legitimacy of joint force actions, preserving the joint

OIE Unit Core Activities *(See also pp. 2-10 to 2-11 and 2-19.)*

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. VII-9 to VII-11.

OIE unit core activities include conducting OIE and facilitating the JFC's integration of information into joint force operations. Other joint force elements conduct some of the information activities associated with these core activities during their operations.

OIE. OIE are the primary focus of OIE units. OIE encompass critical tasks that OIE units must perform to achieve JFC objectives by leveraging information. OIE units accomplish these tasks using military capabilities in a coordinated and synchronized manner to collectively achieve objectives affecting the IE by informing audiences; influencing foreign relevant actors; attacking and exploiting information, information networks, and information systems; and by protecting friendly information, information networks, and information systems. OIE are conducted in support of the JFC's operation or campaign objectives or in support of other components of the joint force. Joint forces continuously conduct OIE to remain engaged with relevant actors.

INFORM. The inform task involves actions taken to accurately communicate with domestic and foreign audiences to build understanding and support for operational and institutional objectives. It seeks to reassure allies and partners and to deter and dissuade competitors, adversaries, and enemies. The inform task uses accurate and timely information and visual media to counter disinformation; correct misinformation; and put operations, activities, and polices in context. It involves communication with domestic and international audiences and with joint force personnel. Planning and executing tasks to inform include public engagement and the acquisition, production, and dissemination of communication and other information products. The inform task facilitates educated perceptions by establishing facts and placing joint force activities in context, correcting inaccuracies and misinformation, and discrediting propaganda with counter-narratives. The primary means used for the inform task is PA; however CA, cyberspace, and psychological operations forces can facilitate the release of truthful information through their respective CMO, CO, and MISO activities.

INFLUENCE. The purpose of the influence task is to affect the perceptions, attitudes, and other drivers of relevant actor behavior. This task is focused on impacting the human aspects of the OE, so planners should consider elements of these aspects as they relate to decision makers (e.g., each decision maker's culture, life experiences, relationships, outside events, ideology, and the influences of those people inside and outside the decision maker's group) during OIE planning, execution, and assessment. Planners integrate influence activities into the existing targeting process. Activities designed to contribute to the influence task include MISO, CMO, CO, OPSEC, and MILDEC operations. Influence may also involve the use of STO. Commanders consider the influence potential of all available capabilities in design, planning, and targeting. OIE units conduct all influence tasks in accordance with approved authorities.

ATTACK & EXPLOIT. The attack and exploit task comprises activities meant to impact or use opponent information, information systems, and information networks in ways that affect decision making and other drivers of behavior to create relative advantages for the joint force. OIE units execute these actions to manipulate or paralyze the adversary or enemy decision-making processes. Attack activities encompass affecting the real or perceived accuracy, integrity, authenticity, or confidentiality of information or the availability of information. OIE units accomplish attack tasks through technical means, such as CO, EMSO, and STO, though maneuver forces and joint fires can also be employed in support of these tasks. Exploit activities include accessing information, information networks, or information systems to gain intelligence and support operational preparation of the environment (OPE) for current or future operations. OPE may subsequently support inform and influence tasks of OIE. OIE units accomplish the exploit task through technical means, such as CO or EMSO.

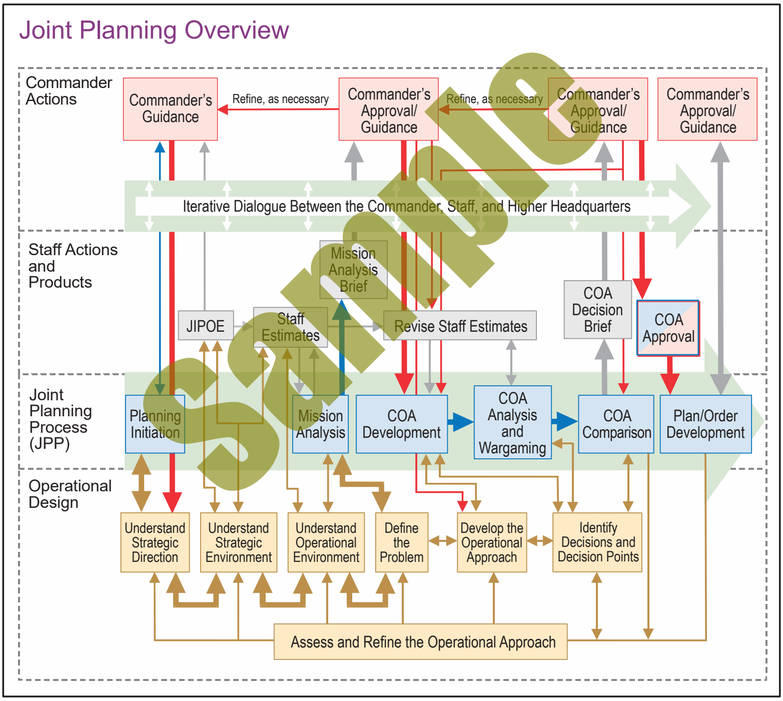
V. OIE: Planning, Coordination, Execution, & Assessment

Ref: JP 3-04, Information in Joint Operations (Sept '22), chap. IV - VII.

*See following pages (pp. 2-46 to 2-49) for an overview of the **integration of information** during the planning, execution, and assessment of joint operations.*

I. Planning *(See pp. 2-55 to 2-66. See also chap. 4.)*

Commanders integrate OIE into their operations at all levels. Plans should address how OIE affect the will, awareness, and understanding of adversaries and other relevant actors; deny competitors the ability to act in and through the IE to undermine the joint force; and protect joint force will, awareness, understanding, and the joint force ability to take actions in and through the IE.


Joint Planning Overview
Commander Actions
Commander's Guidance
Refine, as necessary
Commander's Approval/ Guidance
Refine, as necessary
Commander's Approval/ Guidance
Commander's Approval/ Guidance
Iterative Dialogue Between the Commander, Staff, and Higher Headquarters
Staff Actions and Products
Mission Analysis Brief
JIPOE
Staff Estimates
Revise Staff Estimates
COA Decision Brief
COA Approval
Joint Planning Process (JPP)
Planning Initiation
Mission Analysis
COA Development
COA Analysis and Wargaming
COA Comparison
Plan/Order Development
Operational Design
Understand Strategic Direction
Understand Strategic Environment
Understand Operational Environment
Define the Problem
Develop the Operational Approach
Identify Decisions and Decision Points
Assess and Refine the Operational Approach

Ref: JP 3-04 (Sept '22), fig. V-1. Joint Planning Overview.

Refer to JFODS6: The Joint Forces Operations & Doctrine SMARTbook, 6th Ed. (Guide to Joint Warfighting, Operations & Planning). JFODS6 is updated for 2023 with new/updated material from the latest editions of JP 3-0 Joint Campaigns and Operations (Jun '22), JP 5-0 Joint Planning (Dec '20), JP 3-33 Joint Force Headquarters (Jun '22), and JP 1 Volumes I and II Joint Warfighting and the Joint Force (Jun '20), Additional topics and references include Joint Air, Land, Maritime and Special Operations (JPs 3-30, 3-31, 3-32 & 3-05).

Guide for the Integration of Information in Joint Operations

Ref: JP 3-04, Information in Joint Operations (Sept '22), app. C. Fig. C-1 is a reference guide for the integration of information during planning, execution, and assessment of joint operations.

A. Operational Environment Awareness & Understanding

(Continually Ongoing) Develop and maintain an integrated understanding of the OE spanning geographic, functional, domain, classification, and organizational boundaries.

1. Characterize Overall IE

a. Understand why and how information moves through the OE, how it is received, processed, and employed, by whom, and for what purposes.

b. Establish IE baseline to create a reference point of relevant actor perceptions, beliefs, and attitudes. Assess changes over time.

c. Distinguish relevant information and characterize its sources and methods of movement or transmission.

d. Identify misinformation and disinformation and credible from non-credible sources of information.

e. Understand the information networks and systems used by relevant actors.

f. Understand social/cultural norms needed for effective influence.

2. Identify and Understand Relevant Actors

a. Identify humans and automated systems that are potential relevant actors.

b. Describe what drivers of behavior are most likely to affect relevant actors.

c. Understand how relevant human actors sense and process information to trigger a behavior that can positively or negatively impact joint operations.

d. Understand how relevant automated systems sense and process information.

e. Describe how relevant actors communicate and make decisions.

f. Identify relevant actors that are decision makers, key influencers, or both.

g. Identify key influencers for relevant actors both inside and outside the operational area.

B. Strategy and Course of Action Development

Establish operational approach and develop COA options for attaining and maintaining conditions that enable achievement of JFC intent and advancement of campaign objectives.

1. Initiation: Receive and Refine Planning Guidance

a. Review overall approach to integrating efforts with overall joint force, allies/partners, and Interagency.

b. Describe relevant actor desired behaviors (e.g., specifics in terms of assure, deter, induce, compel)

c. Articulate current authorities for information activities at JFC and subordinate levels.

- CCMD-approved MISO program.
- CCMD-approved CO/MILDEC/Space activity.

d. Identify forces available to conduct or support OIE (via OPCON, TACON, direct support, or general support relationships).

e. Identify risks that can or cannot be accepted related to activities in the IE.

f. Update the information estimate.

g. Provide updates on changes in the IE, status of information forces, and results of information activities.

2. Mission Analysis

a. Analyze planning directives and strategic guidance from HHQ.

- Determine national and HHQ objectives.
- Determine desired relevant actor behaviors.

b. Develop mission narrative.

- Develop JFC operational narrative and supporting themes and messages based on CCMD guidance.

c. Determine facts and planning assumptions.

- Identify relevant actors within context of JFC's objectives.

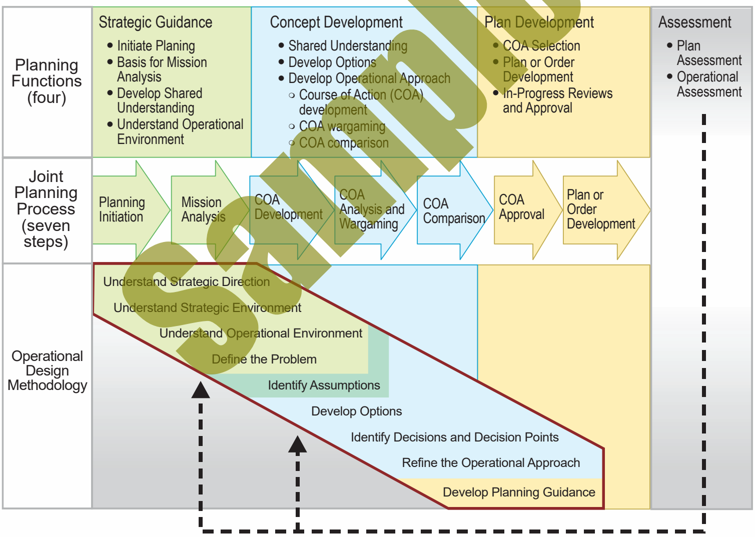
VI. Information & the Joint Planning Process

Ref: JP 3-04, Information in Joint Operations (Sept '22), chap. 4. (See chap. 4.)

The joint planning process (JPP) is an orderly, analytical process that consists of a logical set of steps to analyze a mission, select the best COA and produce a campaign or joint OPLAN or order. Like operational design, it is a logical process to approach a problem and determine a solution. It is a tool to be used by planners but is not prescriptive. Throughout the JPP steps (see Figure IV-3), information planners assist other joint planners in incorporating their understanding of how information impacts the OE to identify how to best support human and automated system decision making and how to best leverage information to achieve the JFC's objectives during operations. The result of the JPP is a plan or order that clearly specifies how the joint force will use and leverage information as part of the overall operation.

See pp. 2-45 to 2-51 for discussion of OIE information planning considerations.

Planning Functions, Process, and Operational Design Methodology



Planning Functions (four)

Strategic Guidance
- Initiate Planing
- Basis for Mission Analysis
- Develop Shared Understanding
- Understand Operational Environment

Concept Development
- Shared Understanding
- Develop Options
- Develop Operational Approach
  - Course of Action (COA) development
  - COA wargaming
  - COA comparison

Plan Development
- COA Selection
- Plan or Order Development
- In-Progress Reviews and Approval

Assessment
- Plan Assessment
- Operational Assessment

Joint Planning Process (seven steps)

Planning Initiation → Mission Analysis → COA Development → COA Analysis and Wargaming → COA Comparison → COA Approval → Plan or Order Development

Operational Design Methodology

Understand Strategic Direction
Understand Strategic Environment
Understand Operational Environment
Define the Problem
Identify Assumptions
Develop Options
Identify Decisions and Decision Points
Refine the Operational Approach
Develop Planning Guidance

Ref: JP 3-04 (Sept '22), fig. IV-3. Planning Functions, Process, and Operational Design Methodology.

Refer to JFODS6: The Joint Forces Operations & Doctrine SMARTbook, 6th Ed. (Guide to Joint Warfighting, Operations & Planning). JFODS6 is updated for 2023 with new/updated material from the latest editions of JP 3-0 Joint Campaigns and Operations (Jun '22), JP 5-0 Joint Planning (Dec '20), JP 3-33 Joint Force Headquarters (Jun '22), and JP 1 Volumes I and II Joint Warfighting and the Joint Force (Jun '20), Additional topics and references include Joint Air, Land, Maritime and Special Operations (JPs 3-30, 3-31, 3-32 & 3-05).

Step 1—Planning Initiation

During planning initiation, information planners use their specific expertise to assist the JPG in:

- Reviewing commander's planning guidance for information activities and explicit and implied tasks that will impact planning.
- Identifying external stakeholders that the joint force should collaborate with for planning and executing information activities (e.g., DOS Global Engagement Center, country teams, JIATF or JIACG). See Chapter III, "Unity of Effort," for organizations to consider.
- Determining initial information planning support requirements to augment the staff (e.g., information professionals to serve as information planners, language/regional/cultural expertise).
- Gathering and analyzing the information required to plan operations that affect relevant actor behavior and identified networks.
- Updating the information estimate, providing updates on changes in the IE, updating the status of information forces, and providing the results of any ongoing information activities.

Step 2—Mission Analysis

The JFC and staff develop a restated mission statement that allows subordinate and supporting commanders to begin their own estimates and planning efforts for higher headquarters' concurrence. The joint force's mission is the task or set of tasks, together with the purpose, that clearly indicates the action to be taken and the reason for doing so. Mission analysis is used to study the assigned tasks and to identify all other tasks necessary to accomplish the mission. Mission analysis focuses the commander and the staff on the problem at hand and lays a foundation for effective planning.

A. Analyze Higher Headquarters' Planning Directives and Strategic Guidance

Information planners contribute to the analysis of strategic guidance and higher headquarters' planning directives by understanding and advising the JFC on how national leadership and higher headquarters intend for the military to support the informational instrument of national power. In particular, information planners determine higher headquarters' perspective of how the military will leverage information to achieve national strategic and military objectives, what behaviors that higher leadership wants from relevant actors to support those objectives, and what role the joint force has in leveraging information to obtain those desired behaviors.

The Operational Mission Narrative

During this step of mission analysis, CCMD and operational-level headquarters staffs use strategic guidance to begin developing the operational mission narrative. The operational mission narrative will include themes and messages that nest under the strategic mission narrative. The development of the operational mission narrative is a collaborative effort that should include planners with regional and cultural expertise. Operational mission narratives focus on the theater/region and seek to advance the legitimacy of the mission while countering adversary narratives. A compelling narrative at this level guides planning, targeting, and execution. Likewise, the joint force should make every effort to ensure operations, activities, words, and images are perceived as being consistent with the narrative, thereby preventing audiences from perceiving a conflict between the joint force's actions and its words.

See facing page.

Operational Mission Narrative

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. IV-16 to IV-18.

When developing the operational mission narrative, planners should recognize that narratives are not created in a vacuum. There are pre-existing narratives in the OE and others may emerge. These narratives may be from adversaries, friendly forces, or relevant neutral groups. These other narratives may reinforce or run counter to the joint force narrative. Awareness of these narratives leads to greater understanding of how to leverage operations and messaging activities to achieve friendly objectives.

Analyzing existing narratives provides insight into the messages that relevant actors are conveying, how they are disseminated and propagated, how the intended audiences and relevant actors react to the themes and messages in those narratives, and potential avenues for influence. In addition to informing mission analysis and the development of the operational mission narrative, the results from narrative analysis should be incorporated into JIPOE and operational assessment processes. Figure IV-4 shows some sample questions that an analysis of existing narratives can answer.

Questions for Narrative Analysis

- How do the relevant actors frame and explain their ideology?
- How do relevant actors make their ideology appear enduring and natural to the local culture?
- Do joint force activities challenge their assumptions, beliefs, and meanings?
- What are the local culture/society goals that the joint force can leverage?
- Are there inconsistencies in a relevant actors' narrative? If so, how does the relevant actor deal with those inconsistencies? Do those inconsistencies present a vulnerability that can be exploited?
- What is the structure of the existing narratives?
- How do existing narratives resonate with relevant actors?

Ref: JP 3-04, (Sept '22), fig. IV-4. Questions for Narrative Analysis.

Additionally, information planners identify operations worldwide in execution and ongoing activities, to include information activities, which will limit the JFC's range of possible COAs, as well as impact plans and operations. This awareness of other ongoing operations and activities includes those of multinational partners.

Finally, as part of mission analysis, information planners identify existing authorities and permissions and what additional authorities and permissions that the JFC will require for the conduct of information activities. This is done as early as possible in the JPP because of the time required to obtain those additional authorities and permissions. Use of some capabilities or activities that leverage information to affect behavior may require unique authorities and permissions. Joint force planners should also review the authorities for the use of capabilities and conduct of activities in their own AOR that could affect the OEs of other JFCs through the IE. Achieving a shared understanding of authorities vertically across echelons of command and horizontally across mission partners is key to successful execution. Information planners can advise the planning team on which authorities for leveraging information may require additional time, legal review, or subject matter expertise to request.

Refer to JP 3-04, App. A, Narrative Development.

Chap 3

(Information) CAPABILITIES

** In accordance with the changes in joint and Army doctrine (editor's note, p. 1-2), Army forces will no longer use the terms information operations, information-related capabilities, or information superiority. Neither JP 3-04 (Sept '22) nor ADP 3-13 (Nov '23) provide a specific alternative term in lieu of "information-related capabilities", instead generically referring to "information capabilities." Below outlines how these capabilities are addressed.*

I. Joint Force Capabilities, Operations, and Activities for Leveraging Information (JP 3-0, Jan '22)

In addition to planning all operations to benefit from the inherent informational aspects of physical power and influence relevant actors, the JFC also has additional means with which to leverage information in support of objectives. Leveraging information involves the generation and use of information through tasks to inform relevant actors; influence relevant actors; and/or attack information, information systems, and information networks:

- Key Leader Engagement (KLE)
- Public Affairs (PA)
- Civil-Military Operations (CMO)
- Military Deception (MILDEC)
- Military Information Support Operations (MISO)
- Operations Security (OPSEC)
- Signature Management
- Electronic Warfare (EW)
- Combat Camera (COMCAM)
- Historians
- Space Operations
- Special Technical Operations (STO)
- Cyberspace Operations (CO)

II. Army Doctrine (ADP 3-13, Nov '23) *(See p. 3-4.)*

Although there are multiple mentions of "information capabilities" throughout ADP 3-13, they are neither identified specifically nor listed. Examples, however, are provided under a section on "TECHNICAL TRAINING AND EDUCATION" *(ADP 3-13, p. 8-19).*

...the Army trains and educates technical specialists who possess the ability to counter and defeat threat activities. Examples of technical informational training for select information specialists include—

- Civil affairs operations.
- Counterintelligence (CI).
- Cyberspace operations.
- Electromagentic warfare (EW).
- Information management (IM).
- Intelligence and the various intelligence disciplines
- Knowledge management.
- Military deception (MILDEC).
- Military Information in Support of Operations (MISO).
- Network operations
- Public affairs operations.
- Space operations.
- Operational law.

See following pages for an overview of how these capabilities (and operations) were previously described in FM 3-13 (Dec '16).

Information Operations & the IRCs (* as previously defined in FM 3-13, Dec '16)

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

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).

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.

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.

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 (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.

The information-related capabilities (IRCs) include—

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

All unit operations, activities, and actions affect the information environment. 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 include:

- 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

III. INFO Capabilities (INFO2 SMARTbook)

The INFO2 SMARTbook discusses the following capabilities 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).

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

Electromagnetic Warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

Space Operations *See pp. 3-61 to 3-68.*

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 Capabilities *See pp. 3-69 to 3-72.*

Additional capabilities 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.

Chap 3

I. Public Affairs (PA)

Ref: JP 3-61 (w/Chg 1), Public Affairs (Aug '16) and FM 3-61, Communication Strategy and Public Affairs Operations (Feb '22).

See pp. 1-35 to 1-44 for discussion of the INFORM activity as related to information advantage (ADP 3-13) and p. 2-19 for leveraging information by "informing domestic, international and internal audiences" (JP 3-04).

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

III. Civil-Military Operations and the Levels of War

Ref: JP 3-57, Civil-Military Operations (Jul '18), pp. I-6 to I-8.

The three levels of warfare—strategic, operational, and tactical—link tactical actions to achievement of national objectives. There are no finite limits or boundaries between these levels, but they help commanders design and synchronize operations, allocate resources, and assign tasks to the appropriate command. CMO may be applied at the strategic, operational, and tactical levels of warfare. Specific actions at one level of warfare may affect all three levels simultaneously with different effects at each level. CMO guidance should include higher headquarters objectives and end states synchronized with USG policy and guidance. Individuals and units conducting CMO must understand how tactical CMO actions may have strategic implications.

Civilian and military organizations often have differing perspectives. Some civilian leaders may object to specific CMO because the civilian populations might confuse the military with independent NGO or international organization efforts. Some international organizations or NGOs have filed objections with senior HN or USG officials when they feel CMO have compromised their neutrality. When these differing perspectives cause tactical or operational friction, they may escalate to strategic, time-consuming issues for the JFC. Prevention of such friction may entail military leaders, ensuring non-military entities have the lead in nonmilitary related efforts as opposed to being seen as subordinated to military actions.

Recognizing that military and nonmilitary organizations use different decision-making processes and philosophies can help reduce friction among all stakeholders and set conditions for common understanding. Most civilian agencies do not organize themselves or make decisions based on the tactical, operational, and strategic levels in regards to organizing or decision making. For example, civilian organizations may also organize activities around sectors of activity, such as health services or education, rather than geographically, such as by district or province. Most civilian agencies do not recognize the tactical, operational, and strategic levels in regards to organizing or decision making.

A. Strategic

At the strategic level, CMO focus on larger and long-term issues that may be part of USG shaping, stabilization, reconstruction, and economic development initiatives in failing, defeated, or recovering nations. CMO are an essential tool used to improve the HN in improving the capacity, capability, and willingness required to regain governance. Strategic CMO are part of a geographic combatant commander's (GCC's) SC guidance in the theater campaign plan (TCP). During certain contingency operations, the Secretary of Defense (SecDef) and the Secretary of State will integrate stabilization and reconstruction contingency plans with military contingency plans and develop a general framework to coordinate stabilization and reconstruction activities and military operations.

B. Operational

At the operational level, CMO synchronize stability activities with other activities and operations (offense and defense) within each phase of any joint operation. CMO also integrate the stabilization and reconstruction efforts of USG interagency, international organization, and NGO activities with joint force operations.

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 international organizations and NGOs. Coordination of CMO for current and future operations is conducted at the operational level. Information management (IM) enables CMO and facilitates interorganizational cooperation to efficiently distribute resources and measure success using nontraditional operational indicators.

C. Tactical

A civil-military team or civil-military operations center (CMOC) may facilitate tactical CMO among the military, the local populace, NGOs, and international organizations. Commanders can coordinate, integrate, and synchronize with the civil component through military engagement, civil reconnaissance (CR), a civil-military support element, or through an established CMOC. Tactical CMO are normally focused on specific areas or groups of people and have more immediate effects.

Annex G (Civil-Military Operations) describes CAO and larger CMO in a plan or operation order (OPORD). CMO require coordination among CA, logistical support, maneuver, health service support, military police (MP), engineer, transportation, and special operations forces. 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 OE, such as changes in the military or strategic situation, natural or man-made disasters, or changes in the other operational variables, can divert the joint force's main effort from CMO. By continually analyzing the OE, the JFC can identify warnings of changes in the OE and allocate resources to monitor these changes in order to anticipate changes in force requirements and planning. Branch and sequel planning and preventive action may mitigate disruption of CMO. For example, a branch may call for the use of a show of force to deter aggressive action by a group while CMO are being conducted. The JFC can task a unit with a "be prepared to" mission in order to facilitate execution of branches or sequels. This can occur in the context of the commander on the ground tasking a subordinate element or in a larger context of a GCC tasking a Service component like the Navy with the be-prepared-to mission while the Army conducts the civil-military operation.

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 attack
- Disruption of public utilities, e.g., water, power, sewage, and economic strife due to socioeconomic imbalance
- Increases in dislocated civilians

III. Military Deception (MILDEC)

Ref: FM 3-13.4, Army Support to Military Deception (Feb '19), chap. 1.

Military deception is actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission (JP 3-13.4). Deception applies to all levels of warfare, across the range of military operations, and is conducted during all phases of military operations. When properly integrated with operations security (OPSEC) and other information-related capabilities (IRCs), deception can be a decisive tool in altering how the enemy views, analyzes, decides, and acts in response to friendly military operations.

Deception is a commander-driven activity that seeks to establish conditions favorable for the commander to achieve objectives. It is both a process and a capability. As a process, deception employs an analytic method to systematically, deliberately, and cognitively target individual decision makers. The objective is to elicit specific action (or inaction) from the enemy. As a capability, deception is useful to a commander when integrated early in the planning process as a component of an operation focused on causing an enemy to act or react in a desired manner. Deception greatly enhances the element of surprise. Deception aligns with surprise and the displacement of critical threat capabilities away from the friendly point of action. Due to the potentially sensitive nature of deception activities and selected means, planners must implement appropriate security and classification measures to properly safeguard deception tactics, techniques, and procedures.

I. Functions of Military Deception

Planners must have a thorough understanding of the functions and the scope of what deception can and cannot accomplish. A deception plan serves as a part of the overall mission. Every deception plan must clearly indicate how it supports the commander's objectives. The functions of deception include, but are not limited to—

- Causing delay and surprise through ambiguity, confusion, or misunderstanding.
- Causing the enemy to misallocate personnel, fiscal, and materiel resources.
- Causing the enemy to reveal strengths, weaknesses, dispositions, and intentions.
- Causing the enemy to waste combat power and resources with inappropriate or delayed actions.

II. Categories of Deception

Deception activities support objectives detailed in concept plans, operation plans (OPLANs), and operation orders (OPORDs) associated with approved military operations or activities. Deception applies during any phase of military operations to establish conditions to accomplish the commander's intent. The Army echelon that plans a deception activity 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 authorities, levels of responsibility, and planning. The levels help organize thought and approaches to a problem. Decisions at one level always affect other levels. Table 1-1 shows the three types of deception.

A. Military Deception (MILDEC)

Military deception (MILDEC) is planned, trained, and conducted to support military campaigns and major operations. MILDEC activities are planned and executed to cause adversaries to take actions or inactions that are favorable to the commander's objectives. The majority of MILDEC planned for and executed by the combatant command (CCMD) to create operational-level effects. MILDEC is normally planned before, and conducted during, combat operations. CCMD instructions add guidelines, policies, and processes that must be adhered to in their respective commands. MILDEC is a joint activity to which the Army, as the primary joint land component, contributes. Army forces do not unilaterally conduct MILDEC. MILDEC must adhere to the regulatory requirements found in Army policy and regulations, CJCSI 3211.01 series, and applicable CCMD instructions.

B. Tactical Deception (TAC-D)

Tactical deception is an activity planned and executed by, and in support of, tactical-level commanders to cause enemy decision makers to take actions or inactions prejudicial to themselves and favorable to the achievement of tactical commanders' objectives. Commanders conduct tactical deception (TAC-D) to influence military operations to gain a relative, tactical advantage over the enemy, obscure vulnerabilities in friendly forces, and enhance the defensive capabilities of friendly forces. In general, TAC-D is a related subset of deception that is not subject to the full set of MILDEC program requirements and authorities. In most circumstances, Army commanders can employ TAC-D unilaterally if certain criteria are met. In description, TAC-D differs from MILDEC in four key ways:

- MILDEC is centrally planned and controlled through CCMD-derived authorities, but TAC-D is not. TAC-D can be employed unilaterally by tactical commanders with an approved plan.
- TAC-D actions are tailored to tactical requirements of the local commander and not always linked or subordinate to a greater MILDEC plan.
- The TAC-D approval process differs from the MILDEC approval process in that it is only required to be approved at two echelons higher, provided that it adheres to the joint policy for MILDEC addressed in CJCSI 3211.01. CCMD instructions add guidelines, policies, and processes that must be adhered to in their respective commands.
- Planning for TAC-D is usually more abbreviated, but still focuses on influencing the action or inaction of enemy decision makers, to gain a tactical advantage over an enemy. TAC-D gains this relative advantage using deception activities that affect the enemy's perceptions of friendly activities and possibly targeting lower-echelon enemy combatants to affect their operations.

C. Deception in Support of Operations Security (DISO)

Deception in support of operations security (DISO) is a deception activity that conveys or denies selected information or signatures to a foreign intelligence entity (FIE) and limits the FIE's overall ability to collect or accurately analyze critical information about friendly operations, personnel, programs, equipment, and other assets. The intent of DISO is to create multiple false, confusing, or misleading indicators to make friendly force intentions harder to interpret by FIE. DISO makes it difficult for FIEs to identify or accurately derive the critical information and indicators protected by OPSEC. Deception and OPSEC are mutually supporting activities. DISO prevents potential enemies from accurately profiling friendly activities that would provide an indication of a specific course of action (COA) or operational activity. DISO differs from joint MILDEC and TAC-D plans in that it only targets FIEs and is not focused on generating a specific enemy action or inaction.

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.

IV. Example Joint MISO Activities

Ref: JP 3-61 (w/Chg 1), Public Affairs (Aug '16), fig. IV-1. p. IV-8.

Example MISO Activities (Across the ROMO)

MILITARY ENGAGEMENT, SECURITY COOPERATION, AND DETERRENCE	CRISIS RESPONSE AND LIMITED CONTINGENCY OPERATIONS	MAJOR OPERATIONS AND CAMPAIGNS
Modify the behavior of selected target audiences toward US and multinational capabilities Support the peacetime elements of US national policy objectives, national security strategy, and national military strategy Support the geographic combatant commander's security strategy objectives Support the objectives of the country team Promote the ability of the host nation to defend itself against internal and external insurgencies and terrorism by fostering reliable military forces and encouraging empathy between host nation armed forces and the civilian populace	Mobilize popular support for US and multinational military operations Gain and sustain popular belief in and support for US and multinational political systems (including ideology and infrastructure) and political, social, and economic programs Attack the legitimacy and credibility of the adversary political systems Publicize beneficial reforms and programs to be implemented after defeat of the adversary Shift the loyalty of adversary forces and their supporters to the friendly powers Deter adversarypowers or groups from initiating actions detrimental to the interests of the US, its allies, or the conduct of friendly military operations Promote cessation of hostilities to reduce casualties on both sides, reduce collateral damage, and enhance transition to post-hostilities	Explain US policies, aims, and objectives Arouse foreign public opinion or political pressures for, or against, a military operation Influence the development of adversary strategy and tactics Amplify economic and other nonviolent forms of sanctions against an adversary Undermine confidence in the adversary leadership Lower the morale and combat efficiency of adversary soldiers Increase the psychological impact of US and multinational combat power Support military deception and operations security Counter hostile information activities

US MISO are developed and executed through a multiphase approach. The joint MISO process is a standard framework by which MISO assets and critical enablers plan, execute, and evaluate MISO with proficiency and consistency throughout major campaigns, operations, and peacetime engagements. The integration and execution of MISO hinge upon the proper implementation of this process.

The joint MISO process consists of seven phases: planning; target audience analysis (TAA); series development; product development and design; approval; production, distribution, dissemination; and evaluation. Each of these phases is designed to apply to any type or level of operation. Collectively, the phases address important considerations and include the necessary activities for the proper integration of MISO with the CCDR's military strategy and mission.

V. The Operations Security Process

Ref: JP 3-13.3, Operations Security (Jan '16), chap. II.

The OPSEC process is applicable across the range of military operations. Use of the process ensures that the resulting OPSEC countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous process. The OPSEC process (Figure II-1) consists of five distinct actions: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate OPSEC countermeasures. These OPSEC actions are applied continuously during OPSEC planning. In dynamic situations, however, individual actions may be reevaluated at any time. New information about the adversary's intelligence collection capabilities, for instance, would require a new analysis of threats.

An understanding of the following terms is required before the process can be explained.

Critical Information

These are specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishment.

OPSEC Indicators

Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

OPSEC Vulnerability

A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision making.

A. Identify Critical Information

The identification of critical information is a key part of the OPSEC process because it focuses the remainder of the OPSEC process on protecting vital information rather than attempting to protect all unclassified information. Critical information answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities necessary for adversaries to plan and act effectively against friendly mission accomplishment. There are many areas within an organization where elements of critical information can be obtained. Personnel from outside the organization may also handle portions of its critical information. Therefore it is important to have personnel from each staff section and component involved in the process of identifying critical information. The critical information items should be consolidated into a list known as a CIL.

Critical information is listed in tab C (Operations Security) to appendix 3 (Information Operations) to annex C (Operations) of an OPLAN or OPORD. Generic CILs (Figure II-2) can be developed beforehand to assist in identifying the specific critical information.

B. Threat Analysis

This action involves the research and analysis of intelligence, CI, and open-source information to identify the likely adversaries to the planned operation.

The operations planners, working with the intelligence and CI staffs and assisted by the OPSEC program manager, seek answers to the following threat questions:

- Who is the adversary? (Who has the intent and capability to take action against the planned operation?)
- What are the adversary's goals? (What does the adversary want to accomplish?)

- What is the adversary's COA for opposing the planned operation? (What actions might the adversary take? Include the most likely COA and COA most dangerous to friendly forces and mission accomplishment.)
- What critical information does the adversary already know about the operation? (What information is too late to protect?)
- What are the adversary's intelligence collection capabilities?
- Who are the affiliates of the adversary, and will they share information?

C. Vulnerability Analysis

The purpose of this action is to identify an operation's or activity's vulnerabilities. It requires examining each aspect of the planned operation to identify any OPSEC indicators or vulnerabilities that could reveal critical information and then comparing those indicators or vulnerabilities with the adversary's intelligence collection capabilities identified in the previous action. A vulnerability exists when the adversary is capable of collecting critical information, correctly analyzing it, and then taking timely action. The adversary can then exploit that vulnerability to obtain an advantage.

Continuing to work with the intelligence personnel, the operations planners seek answers to the following vulnerability questions:

(1) What indicators (friendly actions and open-source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

(2) What indicators can the adversary actually collect?

(3) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

(4) Will the application of OPSEC countermeasures introduce more indicators that the adversary will be able to collect?

Refer to JP 3-13.3, app. A, "Operations Security Indicators," for a detailed discussion of OPSEC indicators.

D. Risk Assessment

This action has three components. First, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC countermeasures for each vulnerability. Second, the commander and staff estimate the impact to operations such as cost in time, resources, personnel or interference with other operations associated with implementing each possible OPSEC countermeasure versus the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. Third, the commander and staff select specific OPSEC countermeasures for execution based upon a risk assessment done by the commander and staff.

OPSEC countermeasures reduce the probability of the adversary either observing indicators or exploiting vulnerabilities, being able to correctly analyze the information obtained, and being able to act on this information in a timely manner.

OPSEC countermeasures can be used to prevent the adversary from detecting an indicator or exploiting a vulnerability, provide an alternative analysis of a vulnerability or an indicator (prevent the adversary from correctly interpreting the indicator), and/or attack the adversary's collection system.

OPSEC countermeasures include, among other actions, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against the adversary's intelligence system.

More than one possible measure may be identified for each vulnerability. Conversely, a single measure may be used for more than one vulnerability.

VI(a). Cyberspace Operations (CO)

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), chap. 2.

Cyberspace operations and electromagnetic warfare (EW) can benefit from synchronization with other Army capabilities using a combined arms approach to achieve objectives against enemy forces. Cyberspace operations and EW can provide commanders with positions of relative advantage in the multi-domain fight. Effects that bleed over from the cyberspace domain into the physical domain can be generated and leveraged against the adversary. A cyberspace capability is a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace (JP 3-12).

Electromagnetic Spectrum Superiority

Electromagnetic spectrum superiority is the degree of control in the electromagnetic spectrum that permits the conduct of operations at a given time and place without prohibitive interference, while affecting the threat's ability to do the same (JP 3-85). Electromagnetic warfare (EW) creates effects in the EMS and enables commanders to gain EMS superiority while conducting Army operations. EW capabilities consist of the systems and weapons used to conduct EW missions to create lethal and non-lethal effects in and through the EMS.

See pp. 3-55 to 3-60, Electromagnetic Warfare (EW), for further discussion.

I. Cyberspace Operations *(CYBER1-1, chap. 2.)*

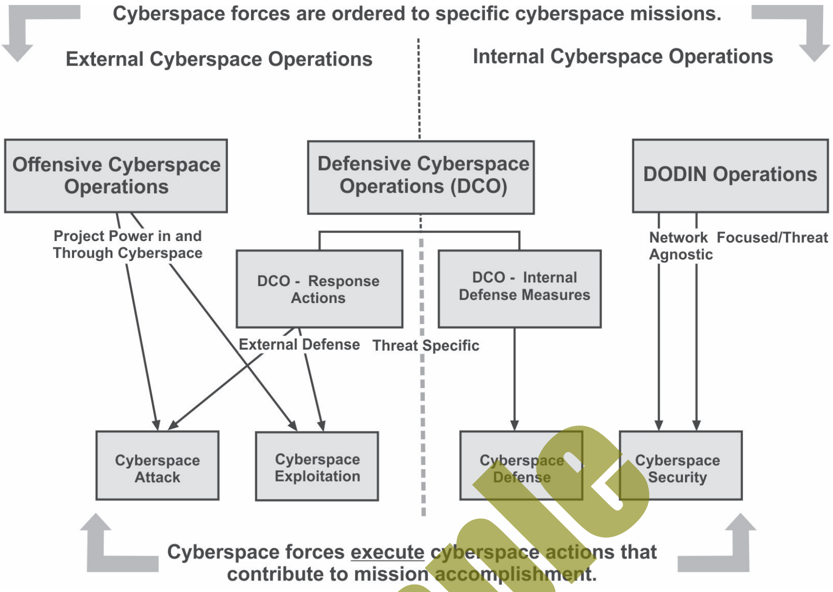
The joint force and the Army divide cyberspace operations into three categories based on the portion of cyberspace in which the operations take place and the type of cyberspace forces that conduct those operations. Each of type of cyberspace operation has varying associated authorities, approval levels, and coordination considerations. An Army taxonomy of cyberspace operations is depicted in figure 2-1, below. The three types of cyberspace operations are—

Cyberspace Operations

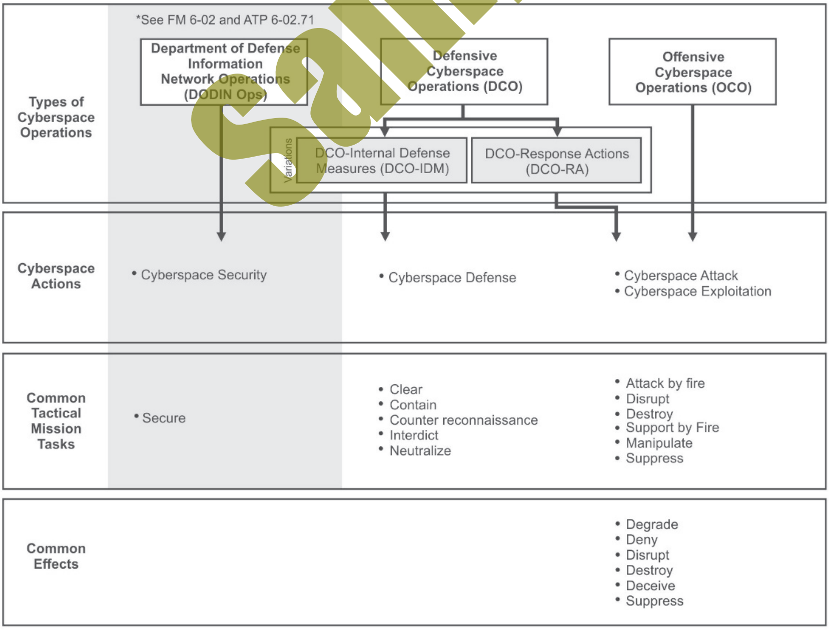
- A DODIN Operations
- B Defensive Cyberspace Operations (DCO)
- C Offensive Cyberspace Operations (OCO)

The Army conducts DODIN operations on internal Army and DOD networks and systems using primarily signal forces. The Army employs cyberspace forces to conduct DCO which includes two further sub-divisions—DCO-IDM and defensive cyberspace operations-response actions (DCO-RA). Cyberspace forces conduct DCO-IDM within the DODIN boundary, or on other friendly networks when authorized, in order to defend those networks from imminent or ongoing attacks. At times cyberspace forces may also take action against threat cyberspace actors in neutral or adversary

Cyberspace Operations (Missions & Actions)


Cyberspace forces are ordered to specific cyberspace missions.
External Cyberspace Operations
Internal Cyberspace Operations
Offensive Cyberspace Operations
Defensive Cyberspace Operations (DCO)
DODIN Operations
Project Power in and Through Cyberspace
DCO - Response Actions
DCO - Internal Defense Measures
Network Agnostic
Focused/Threat
External Defense
Threat Specific
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace forces execute cyberspace actions that contribute to mission accomplishment.

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), fig. 2-2. Cyberspace operations missions and actions.



Types of Cyberspace Operations	Department of Defense Information Network Operations (DODIN Ops)	Defensive Cyberspace Operations (DCO) DCO-Internal Defense Measures (DCO-IDM) DCO-Response Actions (DCO-RA)	Offensive Cyberspace Operations (OCO)
Cyberspace Actions	• Cyberspace Security	• Cyberspace Defense	• Cyberspace Attack • Cyberspace Exploitation
Common Tactical Mission Tasks	• Secure	• Clear • Contain • Counter reconnaissance • Interdict • Neutralize	• Attack by fire • Disrupt • Destroy • Support by Fire • Manipulate • Suppress
Common Effects			• Degrade • Deny • Disrupt • Destroy • Deceive • Suppress

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), fig. 2-1. Cyberspace operations taxonomy.

and other designated systems by defeating on-going or imminent malicious cyberspace activity (JP 3-12). The term blue cyberspace denotes areas in cyberspace protected by the United States, its mission partners, and other areas the Department of Defense may be ordered to protect. DCO are further categorized based on the location of the actions in cyberspace as—

Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM)

Defensive cyberspace operations-internal defensive measures are operations in which authorized defense actions occur within the defended portion of cyberspace (JP 3-12). DCO-IDM is conducted within friendly cyberspace. DCO-IDM involves actions to locate and eliminate cyber threats within friendly networks. Cyberspace forces employ defensive measures to neutralize and eliminate threats, allowing reestablishment of degraded, compromised, or threatened portions of the DODIN. Cyberspace forces conducting DCO-IDM primarily conduct cyberspace defense tasks, but may also perform some tasks similar to cyberspace security.

Cyberspace defense includes actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. (JP 3-12). Cyberspace forces act on cues from cybersecurity or intelligence alerts of adversary activity within friendly networks. Cyberspace defense tasks during DCO-IDM include hunting for threats on friendly networks, deploying advanced countermeasures, and responding to eliminate these threats and mitigate their effects.

Defensive Cyberspace Operations-Response Actions (DCO-RA)

Defensive cyberspace operation-response actions are operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without permission of the owner of the affected system (JP 3-12). DCO-RA take place outside the boundary of the DODIN. Some DCO-RA may include actions that rise to the level of use of force and may include physical damage or destruction of enemy systems. DCO-RA consist of conducting cyberspace attacks and cyberspace exploitation similar to OCO. However, DCO-RA use these actions for defensive purposes only, unlike OCO that is used to project power in and through cyberspace.

Decisions to conduct DCO-RA depend heavily on the broader strategic and operational contexts such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat; the damage the threat has or is expected to cause, and national policy considerations. DCO-RA are conducted by national mission team(s) and require a properly coordinated military order, coordination with interagency and unified action partners, and careful consideration of scope, rules of engagement, and operational objectives.

C. Offensive Cyberspace Operations (OCO)

Offensive cyberspace operations are missions intended to project power in and through cyberspace (JP 3-12). Cyberspace forces conduct OCO outside of DOD networks to achieve positions of relative advantage through cyberspace exploitation and cyberspace attack actions in support of commanders' objectives. Commanders must integrate OCO within the combined arms scheme of maneuver throughout the operations process to achieve optimal effects.

The Army provides cyberspace forces trained to perform OCO across the range of military operations to the joint force. Army forces conducting OCO do so under the authority of a joint force commander. Refer to Appendix C for information on integrat-

I. Electromagnetic Warfare (EW)

Ref: FM 3-12, Cyberspace Operations and Electromagnetic Warfare (Aug '21), pp. 2-8 to 2-15.

I. Electromagnetic Warfare (EW) *(CYBER1-1, chap. 3.)*

Electromagnetic Warfare (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three functions: electromagnetic attack, electromagnetic protection, and electromagnetic support.

Modern militaries rely on communications equipment using broad portions of the electromagnetic spectrum (EMS) to conduct military operations allowing forces to talk, transmit data, and provide navigation and timing information, and command and control troops worldwide. They also rely on the EMS for sensing and awareness of the OE. The Army conducts electromagnetic warfare (EW) to gain and maintain positions of relative advantage within the EMS. The Army's contribution to electromagnetic spectrum operations is accomplished by integrating and synchronizing EW and spectrum management operations.

Electromagnetic Warfare (EW)

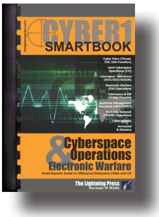
A Electromagnetic Attack (EA)

B Electromagnetic Protection (EP)

C Electromagnetic Support (ES)

***** Electromagnetic Warfare Reprogramming

The three divisions often mutually support each other in operations. For example, radar-jamming EA can serve a protection function for friendly forces to penetrate defended airspace; it can also prevent an adversary from having a complete operating picture.



A. Electromagnetic Attack (EA) *(See p. 1-50.)*

Army forces conduct both offensive and defensive EA to fulfill the commander's objectives in support of the mission. EA projects power in and through the EMS by implementing active and passive actions to deny enemy capabilities and equipment, or by employing passive systems to protect friendly capabilities. Electromagnetic attack is a division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and considered a form of fires (JP 3-85). EA requires systems or weapons that radiate electromagnetic energy as active measures and systems that do not radiate or re-radiate electromagnetic energy as passive measures.

Offensive EA

Offensive EA prevents or reduces an enemy's effective use of the EMS by employing jamming and directed energy weapon systems against enemy spectrum-dependent systems and devices. Offensive EA systems and capabilities include—

- Jammers.
- Directed energy weaponry.
- Self-propelled decoys.
- Electromagnetic deception.
- Antiradiation missiles.

Defensive EA

Defensive EA protects against lethal attacks by denying enemy use of the EMS to target, guide, and trigger weapons that negatively impact friendly systems. Defensive EA supports force protection, self-protection and OPSEC efforts by degrading, neutralizing, or destroying an enemy's surveillance capabilities against protected units. Defensive EA systems and capabilities include—

- Expendables (flares and active decoys).
- Jammers.
- Towed decoys.
- Directed energy infrared countermeasure systems.
- Radio controlled improvised explosive device (RCIED) systems.
- Counter Unmanned Aerial Systems (C-UAS).

Electromagnetic Attack (EA) Effects

EA effects available to the commander include—

- **Destroy**. Destruction makes the condition of a target so damaged that it can neither function nor be restored to a usable condition in a timeframe relevant to the current operation. When used in the EW context, destruction is the use of EA to eliminate targeted enemy personnel, facilities, or equipment (JP 3-85).
- **Degrade**. Degradation reduces the effectiveness or efficiency of an enemy EMS-dependent system. The impact of degradation may last a few seconds or remain throughout the entire operation (JP 3-85).
- **Disrupt**. Disruption temporarily interrupts the operation of an enemy EMS dependent system (JP 3-85).
- **Deceive**. Deception measures are designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce them to react in a manner prejudicial to their interests. Deception in an EW context presents enemy operators and higher-level processing functions with erroneous inputs, either directly through the sensors themselves or through EMS-based networks such as voice communications or data links (JP 3-85).

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 affect space capabilities, space operations, and their terrestrial users. Environmental monitoring support to joint operations gives the JFC awareness of the OE.

Missile Warning

The missile warning mission uses a mix of OPIR and ground-based radars. Missile warning supports the warning mission executed by North American Aerospace Defense Command to notify national leaders of a missile attack against North America, as well as attacks against multinational partners (via shared early warning) in other geographic regions. It also includes notification to combatant commands (CCMDs), multinational partners, and forward-deployed personnel of missile attack and the assessment of a missile attack if the applicable CCMD or multinational partner is unable to do so.

Nuclear Detonation Detection

Nuclear detonation detection capabilities provide persistent, global, and integrated sensors to provide surveillance coverage of critical regions of the globe and provide warning and assessment recommendations to the President, Secretary of Defense (SecDef), and CCDRs, indicating place, height of burst, and yield of nuclear detonations.

Spacelift

Spacelift is the ability to deliver payloads (satellites or other materials) into space.

Satellite Operations

Satellite operations maneuver, configure, operate, and sustain on-orbit spacecraft. In a conflict, satellite operations are critical to the command and control (C2), movement and maneuver, protection, and sustainment of space capabilities.

Space Operations & the Joint Functions

Space-based intelligence collection supports **C2** by providing information used to develop a shared understanding of the threat. A large percentage of the intelligence required to make decisions for employment of forces is obtained from spacecraft.

Spacecraft complement non-space-based **intelligence** sources by providing decision makers with timely, accurate data for information that can create a decisive advantage across the competition continuum.

Space operations support air, land, maritime, and cyberspace **fires** through intelligence, PNT, and communications capabilities. Space operations movement and maneuver include the deployment, repositioning, or re-orientation of on-orbit assets and joint space forces. These movements may support service optimization, protection from environmental hazards, passive defense from threats, or the positioning of assets to enable active defensive or offensive measures.

Protection in space operations includes all measures taken to ensure friendly space systems perform as designed by overcoming attempts to deny or manipulate them. Protection includes all measures to passively neutralize or mitigate threats and man-made and/or environmental hazards, to include enemy attack, terrestrial weather, space weather, on-orbit conjunctions, and non-hostile EMI.

Space operations **sustainment** is conducted through spacelift, satellite operations, force reconstitution, maintenance of a force of space operations personnel, and support to human space flight. Spacelift includes launch systems, launch facilities, and ground personnel capable of placing satellites on orbit.

Space supports the flow of information and decision making. It may also serve as an activity essential to the delivery of specific information in the information environment.

See p. 2-6 for further discussion of the joint functions from JP 3-0.

Chap 4

(Information) PLANNING

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

See p. 1-60 for discussion of planning as related to information advantage (ADP 3-13) and p. 2-45 to 2-51 as related to operations in the information environment (JP 3-04).

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.

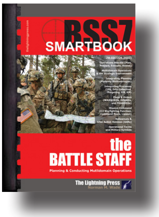
Military Decisionmaking Process (MDMP)

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.

INFO Planning



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.

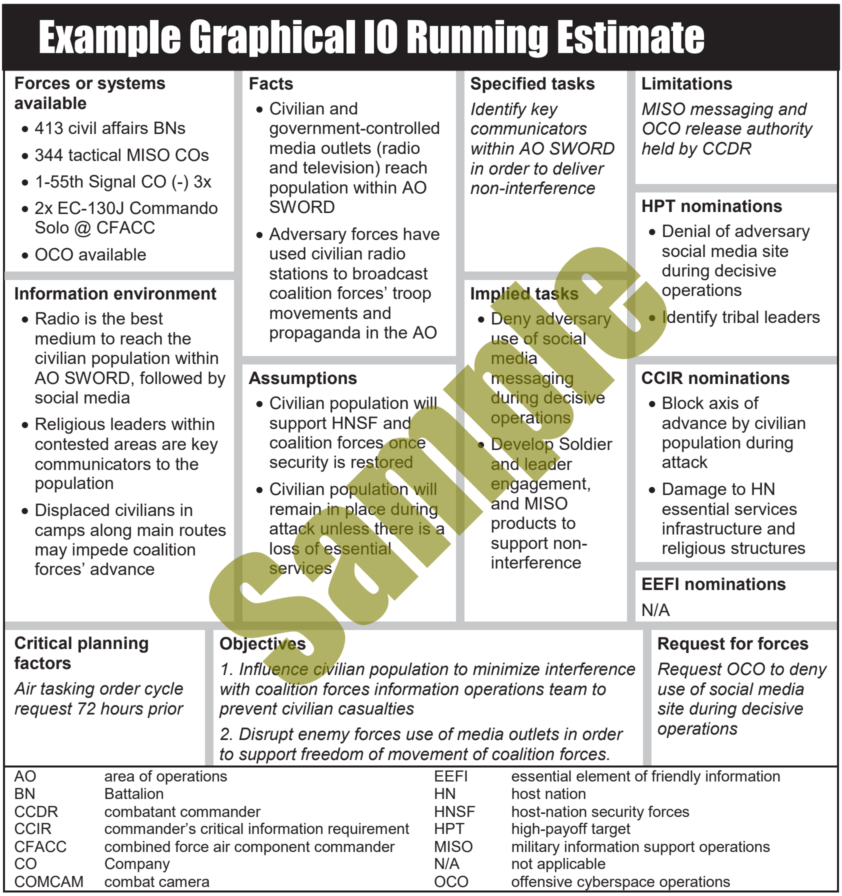
5. COMPARISON. Compare COAs. Rank order COAs for each key consideration. Use a decision matrix to aid the comparison process.

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

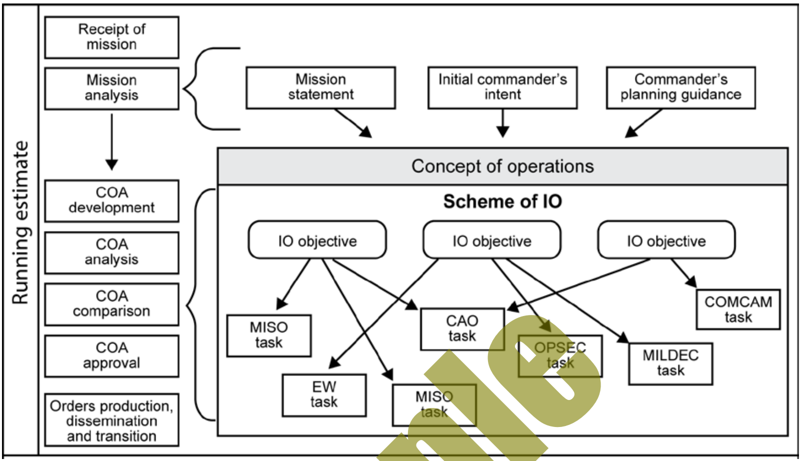
Ref: ATP 3-13.3, fig. 4-3. Example graphical information operations running estimate.

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.

IV. IO Input to Operation Orders and Plans

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



Ref: ATP 3-13.1, fig. 4-7. Relationship of scheme of IO, IO objectives, and IRC tasks.

Base Orders and Plans

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

- Commander's intent, paragraph 3a.
- Concept of operations, paragraph 3b.
- Scheme of IO, paragraph 3c.x (paragraph number varies)
- Tasks to subordinate units, paragraph 3j.
- Coordinating instructions, paragraph 3k.

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

Commanders and staffs use Appendix 15 (Information Operations) to Annex C (Operations) to operation plans and orders to describe how information operations (IO) will support operations described in the base plan or order. The IO officer is the staff officer responsible for this appendix. Products or guidance:

- Combined information overlay. *(See pp. 4-32 to 4-33.)*
- Synchronization matrix. (*See p. 4-16.)*
- Instructions for IRCs not covered by other appendices, such as operations security, visual information, and combat camera.

See pp. 4-61 to 4-64 for a sample annotated format to Appendix 15 (IO) to Annex C (Operations).

A. Mission Statement

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

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

The IO mission statement is a short paragraph or sentence describing what the commander wants IO to accomplish and the purpose for accomplishing it. The IO officer develops the proposed IO mission statement at the end of mission analysis based on the unit's proposed mission statement and IO-related essential tasks. During the mission analysis briefing or shortly thereafter, commanders approve the unit's mission statement and CCIRs. They then develop and issue their commander's intent and planning guidance.

Sample Mission Statement

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

The IO officer may refine a final IO mission statement based on relevant input from the commander's intent and planning guidance and get it approved by the operations officer. The final IO mission statement includes IO effects and most significant IO-related target categories identified in the information environment during mission analysis.

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

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

B. Scheme of Information Operations

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

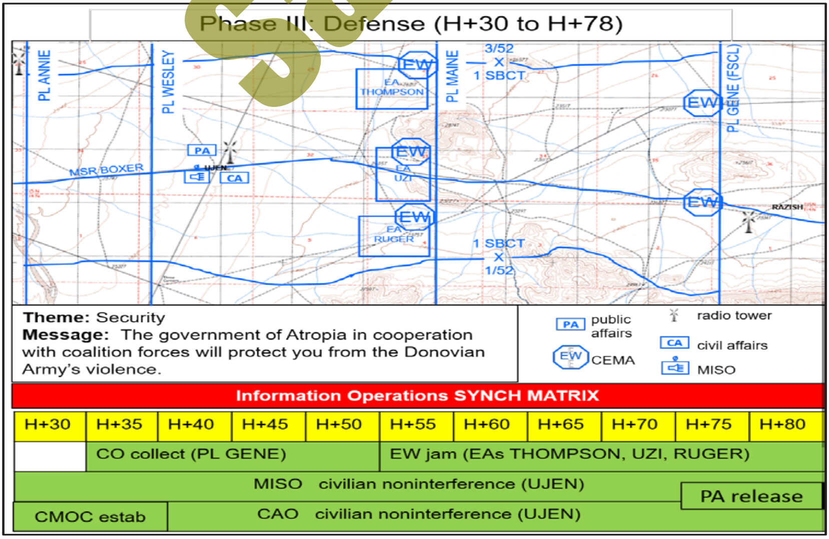
The scheme of IO begins with a clear, concise statement of where, when, and how the commander intends to employ synchronized IRCs to create effects in and through the information environment to support the overall operation and accomplish the mission. Based on the commander's planning guidance, the IO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



Theme: Security
Message: The government of Atropia in cooperation with coalition forces will protect you from the Donovian Army's violence.

Information Operations SYNCH MATRIX

H+30	H+35	H+40	H+45	H+50	H+55	H+60	H+65	H+70	H+75	H+80
	CO collect (PL GENE)				EW jam (EAs THOMPSON, UZI, RUGER)					
MISO civilian noninterference (UJEN)									PA release	
CMOC estab		CAO civilian noninterference (UJEN)								

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

Information Environment Analysis

*Ref: *ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-1 to 2-2.*

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

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

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

Table 2-1. Information environment dimensions. See pp. 1-7 and 2-10 for further discussion of the three dimensions.

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

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

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

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

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):

- Define the information environment (*See pp. 4-22 to 4-23.)*
- Describe the information environment's effects. (*See pp. 4-24 to 4-27.)*
- Evaluate the threat's information situation. (*See pp. 4-28 to 4-33.)*
- Determine threat courses of action in the information environment. (*See p. 4-34.)*

A. Threat Templates

*Ref: *ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-12 to 2-13.*

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

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

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

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

Decision-Making Template

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

Information Infrastructure Template

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

Information Tactics Template

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

B. Threat Center of Gravity Analysis

*Ref: *ATP 3-13.1, The Conduct of Information Operations (Oct '18), pp. 2-13 to 2-15.*

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

COG analysis, with an emphasis on the information environment, is used to—

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

Identify Potential Threat Centers of Gravity

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

Identify Critical Capabilities

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

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

Identify Critical Requirements for Each Critical Capability

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

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

Identify Critical Vulnerabilities for Each Critical Requirement

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

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

Prioritize Critical Vulnerabilities

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

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

The resulting analysis provides a prioritized list of objectives or targets that can then be discussed in context of each possible COA, aiding COA analysis. Each COA will dictate the capability to be employed.

Refer to ATP 3-05.20 for an overview of Army special operations forces targeting methodology that includes COG analysis and CARVER criteria; see ATP 2-33.4 and ATP 3-60 for the Army use of CARVER as a target value analysis tool).

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

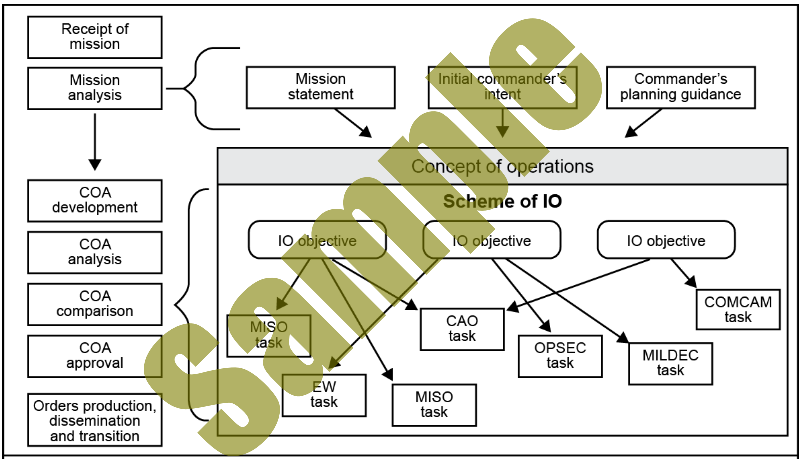
III. IO & the MDMP

*Ref: *FM 3-13, Information Operations (Dec '16), pp. 4-2 to 4-29. (*See note p. 1-2.)*

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).

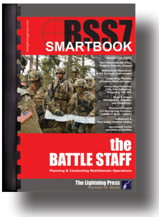
IO planning is integral to several other processes, to include intelligence preparation of the battlefield (IPB) and targeting. The G-2 (S-2) and fire support representatives participate in the IO working group and coordinate with the IO officer to integrate IO with their activities and the overall operation.



CAO	civil affairs operations	IO	information operations
COA	course of action	MILDEC	military deception
COMCAM	combat camera	MISO	military information support operations
EW	electronic warfare	OPSEC	operations security

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).*



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).

IV. Appendix 15 (IO) to Annex C (Operations)

*Ref: *FM 3-13, Information Operations (Dec '16), annex A. (*See note p. 1-2.)*

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. 4-10 for related discussion of IO input to operation orders and plans.

MDMP Task	Inputs	IO Officer Actions	IO Officer Outputs
Orders Production, Dissemination and Transition	• Approved COA • Refined commander's guidance • Refined commander's intent • IO running estimate • Execution matrix • Finalized mission statement, scheme of IO, objectives, and tasks	• Ensure input is placed in tasks to subordinate units and coordinating instructions • Produce Appendix 14 (MILDEC) to Annex C (Operations) • Produce Appendix 15 (IO) to Annex C (Operations) • Produce Appendix 3 (OPSEC) to Annex E (Protection) • Coordinate tasks with IRC staff officers • Conduct other staff coordination. • Refine execution matrix • Transition from planning to operations	• Synchronization matrix • Approved Paragraph 3.k. (10) • Approved Appendix 14 to Annex C • Approved Appendix 15 to Annex C • Approved Appendix 3 to Annex E • IO input to AGM and TSM • Subordinates understand the IO portion of the plan or order
AGM attack guidance matrix **COA** course of action **IO** information operations **IRC** information-related capability **MDMP** military decisionmaking process **MILDEC** military deception **OPSEC** operations security **TSM** trunk signaling mission			

Ref: FM 3-13, table 4-6. Orders production, dissemination and transition.

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

Commanders and staffs use Appendix 15 (Information Operations) to Annex C (Operations) to operation plans and orders to describe how information operations (IO) will support operations described in the base plan or order. The IO officer is the staff officer responsible for this appendix. Products or guidance:

- Combined information overlay. *(See pp. 4-32 to 4-33.)*
- Synchronization matrix. (*See p. 4-16.)*
- Instructions for IRCs not covered by other appendices, such as operations security, visual information, and combat camera.

See following pages (pp. 4-62 to 4-64) for an annotated format of appendix 15 (Information Operations) to Annex C (Operations). The figure is a guide and should not limit the information contained in an actual Appendix 15. Appendix 15 should be specific to the operation being conducted; thus, the content of actual Appendix 15s will vary greatly.

(Information) PREPARATION

*Ref: *FM 3-13, Information Operations (Dec '16), chap. 5. (*See note p. 1-2.)*

See p. 1-62 for discussion of preparation as related to information advantage (ADP 3-13).

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.

IO Preparation Activities

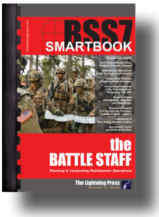
Peacetime preparation by units or capabilities involves building contingency plan databases about the anticipated area of operations. These databases can be used for IO input to IPB and to plan IO to defend friendly intentions, such as network protection and operations security (OPSEC). IO portions of contingency plans are continuously updated.

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.



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

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.

OPLAN/OPORD refinement includes developing branches and sequels. Branches and sequels are normally identified during war-gaming (COA analysis). However, the staff may determine the need for them at any time. The G-3 (S-3) prioritizes branches and sequels. The staff develops them as time permits. The IO officer participates in their development as with any other aspect of planning.

A key focus during preparation is on assessment of the current state of the information environment. This assessment is performed to establish baselines, which are subsequently used when assessing whether IO objectives and IRC tasks were effective in creating desired effects.

C. Conduct Coordination and Liaison

IO requires all units and elements to coordinate with each other continuously, as well as liaise. Coordination begins during planning; however, input to a plan alone does not constitute coordination. Coordination involves exchanging the information

Chap 6

(Information) EXECUTION

*Ref: *FM 3-13, Information Operations (Dec '16), chap. 6. (*See note p. 1-2.)*

See p. 1-63 for discussion of execution as related to information advantage (ADP 3-13) and pp. 2-52 to 2-54 as related to operations in the information environment (JP 3-04).

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.

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.

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.)

IO Working Group

Roles & Responsibilities

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

Representative	Responsibility
hformation 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		12 min
	Part 4: Attack efforts	• Guidance and comments	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. Fires (INFO 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 (OIE Considerations) *(See p. 2-43.)*

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. III-4 to III-6.

Fires is the use of weapon systems or other actions to create specific lethal or nonlethal effects on a target. The nature of the target or threat, the conditions of the mission variables (i.e., mission, enemy, terrain and weather, troops and support available, time available, and civil considerations), and desired outcomes determine how lethal and nonlethal capabilities are employed. Operations in the information environment (OIE) may **leverage the inherent informational aspects of joint fires.** Fires in and through the IE encompass a number of tasks, actions, and processes, including targeting, coordination, deconfliction, and assessment (e.g., BDA).

OIE tasks and capabilities **leverage information** through fires to create specific effects. To integrate effectively, information planners participate in the joint targeting process by selecting and prioritizing targets for fires or TAs for other actions. OIE units create fires that typically result in nonlethal effects. OIE can also indirectly create effects that result in physical destruction (e.g., manipulating computers that control physical processes). Additionally, OIE can leverage the inherent informational aspects of fires to reinforce the psychological effect of those fires. OIE may rely on joint fires support to transmit information to relevant actors and to deliver **nonlethal payloads** to affect information, information systems, and information networks (e.g., leveraging CO to deliver computer code designed to deny network access to an adversary, PA releases to inform friendly audiences, or MISO products to influence foreign audiences).

Joint Force Capabilities, Operations, and Activities for Leveraging Information *(See p. 2-19.)*

Ref: JP 3-04, Information in Joint Operations (Sept '22), pp. II-6 to II-15.

When commanders leverage information, they expand their range of options for the employment of military capabilities beyond the use of or threatened use of physical force. JFCs leverage information in two ways. First, by planning and conducting all operations, activities, and investments to deliberately leverage the inherent informational aspects of such actions. Second, by conducting OIE.

INFORM Domestic, International, and Internal Audiences

Inform activities are the release of accurate and timely information to the public and internal audiences, to foster understanding and support for operational and strategic objectives by putting joint operations in context; facilitating informed perceptions about military operations; and countering misinformation, disinformation, and propaganda. Inform activities help to ensure the trust and confidence of the US population, allies, and partners in US and MNF efforts; and to deter and dissuade adversaries and enemies from action. PA is the primary means the joint force uses to inform; however, civil-military operations (CMO), key leader engagement (KLE), and military information support operations (MISO) also support inform efforts.

INFLUENCE Relevant Actors

The purpose of the influence task is to affect the perceptions, attitudes, and other drivers of relevant actor behavior. Regardless of its mission, the joint force considers the likely psychological impact of all operations on relevant actor perceptions, attitudes, and other drivers of behavior. The JFC then plans and conducts every operation to create desired effects that include maintaining or preventing behaviors or inducing changes in behaviors. This may include the deliberate selection and use of specific capabilities for their inherent informational aspects (e.g., strategic bombers); adjustment of the location, timing, duration, scope, scale, and even visibility of an operation (e.g., presence, profile, or posture of the joint force); the use of signature management and

MILDEC operations; the employment of a designated force to conduct OIE; and the employment of individual information forces (e.g., CA, psychological operations forces, cyberspace forces, PA, combat camera [COMCAM]) to reinforce the JFC's efforts. US audiences are not targets for military activities intended to influence.

ATTACK AND EXPLOIT Information, Information Networks, and Information Systems

The joint force targets information, information networks, and information systems to affect the ability of adversaries and enemies to use information in support of their own objectives. This activity includes manipulating, modifying, or destroying data and information; accessing or collecting adversary or enemy information to support joint force activities or operations; and disrupting the flow of information to gain military advantage. Attacking and exploiting information, information networks, and information systems supports the influence task when it undermines opponents' confidence in the sources of information or the integrity of the information that they rely on for decision making. Activities used to attack and exploit information include offensive cyberspace operations (OCO), electromagnetic warfare (EW), MISO, and CA operations. PA also contributes to this task by publicly exposing malign activities.

Nonlethal Effects

Ref: JP 3-0, Joint Campaigns and Operations (Jun '22), p. III-36.

Joint force capabilities can create nonlethal effects. Some capabilities can produce nonlethal effects that limit collateral damage, reduce risk to civilians, and reduce exploitation 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 goodwill of the local populace. Some capabilities are nonlethal by design and include blunt impact and warning munitions, acoustic and optical warning devices, and vehicle and vessel stopping systems.

Cyberspace Attack *(See p. 3-54.)*

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

Electromagnetic Attack (EA) *(See p. 3-56.)*

EA involves the use of EM energy, DE, or antiradiation weapons to attack personnel, facilities, or equipment to degrade, neutralize, or destroy enemy combat capability. EA can be against a computer when the attack occurs through the EMS. Integration and synchronization of EA with maneuver, C2, and other joint fires are essential. EW is a component of JEMSO used to exploit, attack, protect, and manage the EME to achieve the commander's objectives. EW can be a primary capability or used to facilitate OIE through the targeting process.

Military Information in Suport of Operations (MISO) *(See p. 3-33.)*

MISO actions and messages can generate effects that gain support for JFC objectives; reduce the will of the enemy, adversary, and sympathizer; and decrease the combat effectiveness of enemy forces. MISO are effective throughout the competition continuum. JFCs and their component commanders are the key players in fully integrating MISO into their plans and operations. MISO require unique budget, attribution, and authorities that are coordinated and approved prior to employment. Commanders carefully review and approve MISO programs that comply with mission-tailored, product approval guidelines from national-level authorities. An approved program does not necessarily constitute authority to execute a mission. Commanders obtain required authorities through a MISO-specific execute order (EXORD) or as a task specified in an EXORD for an operation.

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. (*See note p. 1-2.)*

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	BDA	COA	HPT	HVT	IO	PIR
attack guidance matrix	battle damage assessment	course of action	high-payoff target	high-value target	Information operations	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.

I. 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.

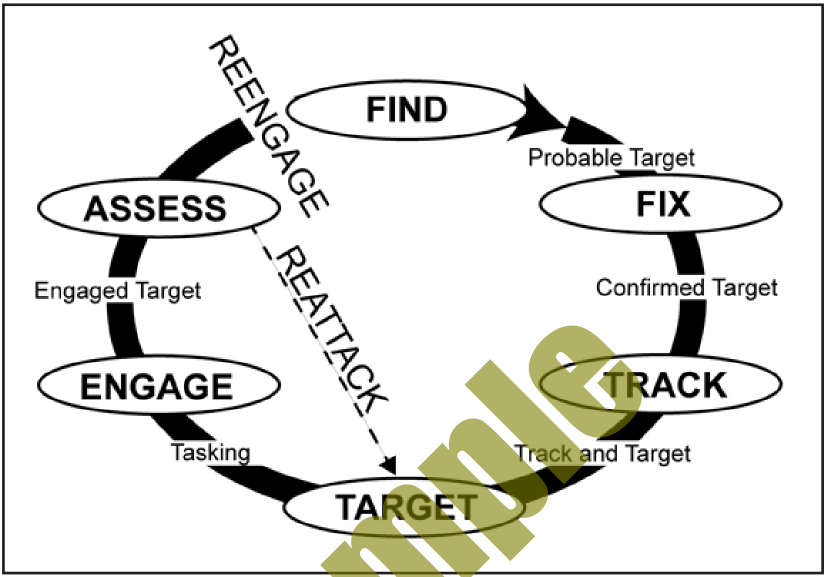
The targeting team develops or contributes to these products throughout the MDMP. The commander approves them during COA approval. The IO officer ensures they include information necessary to engage IO-related targets. IO-related vulnerability analyses done by the G-2 (S-2) and IO officer provide a basis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

III. Dynamic Targeting (F2T2EA)

*Ref: *FM 3-13, Information Operations (Dec '16), p. 7-7.*

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



Ref: ATP 3-13.1, fig. 5-2. Dynamic targeting.

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

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

Ref: ATP 3-13.1, table 5-5. Information operations inputs and activities to support F2T2EA.

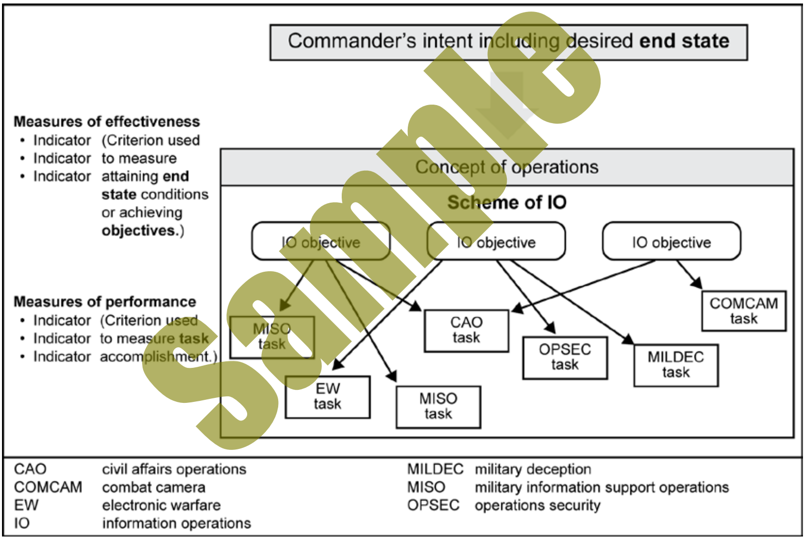
(Information) ASSESSMENT

*Ref: *ATP 3-13.1, The Conduct of Information Operations (Oct '18), chap. 6 and *FM 3-13, Information Operations (Dec '16), chap. 8. (*See note p. 1-2.)*

See p. 1-63 for discussion of assessment as related to information advantage (ADP 3-13) and p. 2-54 as related to operations in the information environment (JP 3-04).

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.


Commander's intent including desired end state
Measures of effectiveness
• Indicator (Criterion used
• Indicator to measure
• Indicator attaining end state conditions or achieving objectives.)
Measures of performance
• Indicator (Criterion used
• Indicator to measure task
• Indicator accomplishment.)
Concept of operations
Scheme of IO
IO objective
IO objective
IO objective
MISO task
CAO task
OPSEC task
MILDEC task
COMCAM task
EW task
MISO task
CAO civil affairs operations
COMCAM combat camera
EW electronic warfare
IO information operations
MILDEC military deception
MISO military information support operations
OPSEC operations security

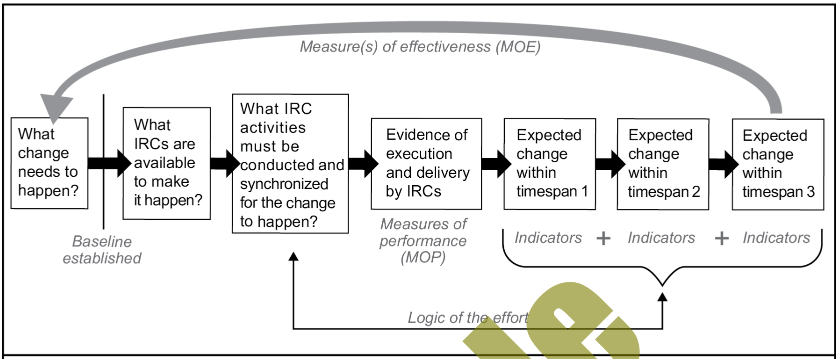
Ref: ATP 3-13.1, fig. 6-1. Framework for assessment.

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.

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.


Measure(s) of effectiveness (MOE)
What change needs to happen?
Baseline established
What IRCs are available to make it happen?
What IRC activities must be conducted and synchronized for the change to happen?
Evidence of execution and delivery by IRCs
Measures of performance (MOP)
Expected change within timespan 1
Expected change within timespan 2
Expected change within timespan 3
Indicators
+
Indicators
+
Indicators
Logic of the effort

IRC information-related capability

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.

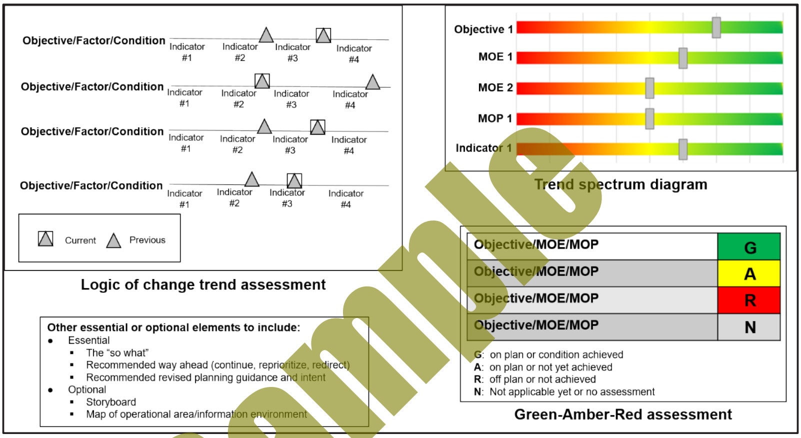
Developing informational, behavioral and sentiment baselines often requires significant time and resource investments. Sentiment baselines, such as those determined through surveys or interviews, may require contracted labor to accomplish. The IO officer must factor in the lead time necessary to contract 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.

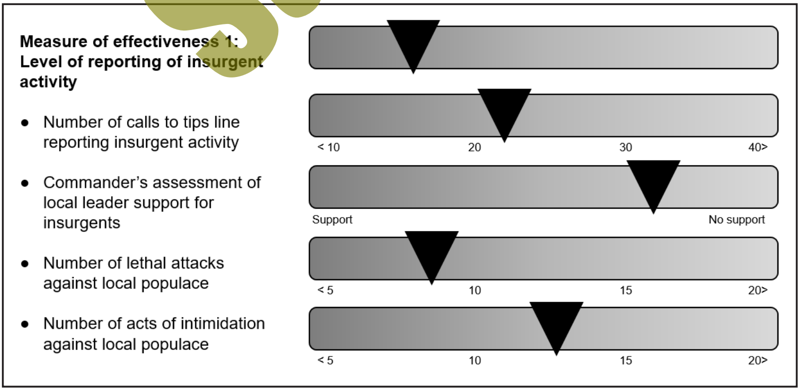


Other essential or optional elements to include:
- Essential
  - The "so what"
  - Recommended way ahead (continue, reprioritize, redirect)
  - Recommended revised planning guidance and intent
- Optional
  - Storyboard
  - Map of operational area/information environment

Objective/MOE/MOP	G
Objective/MOE/MOP	A
Objective/MOE/MOP	R
Objective/MOE/MOP	N

G: on plan or condition achieved
A: on plan or not yet achieved
R: off plan or not achieved
N: Not applicable yet or no assessment

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."

(INFO2) Index

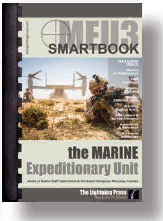
dept of defense
air force
navy
marines
interagency
army
coast guard
joint staff
multinational
Sample

SMARTbooks

INTELLECTUAL FUEL FOR THE MILITARY

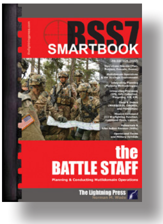
MILITARY REFERENCE: SERVICE-SPECIFIC

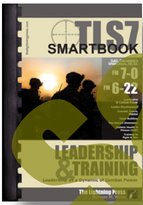
Recognized as a "whole of government" doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.

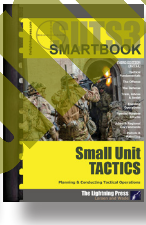


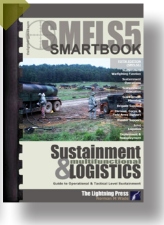
MILITARY REFERENCE: MULTI-SERVICE & SPECIALTY

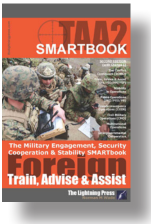
SMARTbooks can be used as quick reference guides during operations, as study guides at professional development courses, and as checklists in support of training.





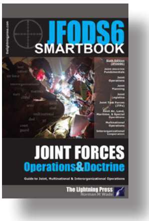




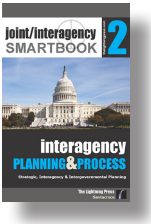

TAA2 SMARTBOOK
The Military Engagement, Security Cooperation & Stability SMARTbook
Foreign Train, Advise & Assist
The Lightning Press

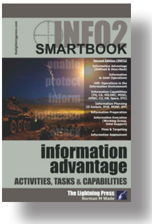
JOINT STRATEGIC, INTERAGENCY, & NATIONAL SECURITY

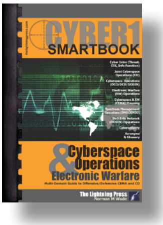
The 21st century presents a global environment characterized by regional instability, failed states, weapons proliferation, global terrorism and unconventional threats.



Joint/Interagency SMARTBOOK 1
joint strategic & operational PLANNING
The Lightning Press





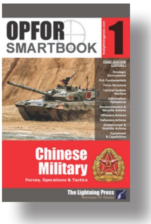


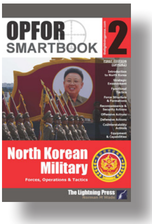
The Lightning Press is a **service-disabled, veteran-owned small business,** DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

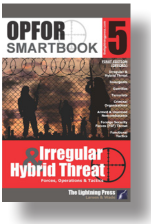
RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

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.

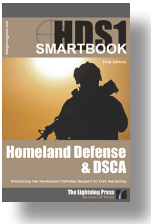


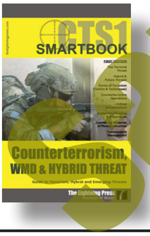


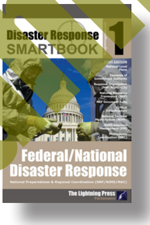


HOMELAND DEFENSE, DSCA, & DISASTER RESPONSE

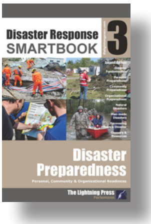
Disaster can strike anytime, anywhere. It takes many forms—a hurricane, an earthquake, a tornado, a flood, a fire, a hazardous spill, or an act of terrorism.






Disaster Response SMARTBOOK 1
Federal/National Disaster Response
The Lightning Press

Disaster Response SMARTBOOK 2
Incident Command System (ICS)
On-Scene, All-Hazards Incident Management
The Lightning Press



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.

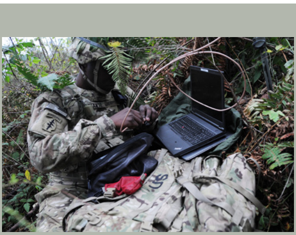
We accept and process both **Government Purchase Cards** (GCPC/GPC) and **Purchase Orders** (PO/PR&Cs).

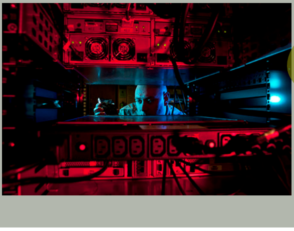
Keep your SMARTbook up-to-date with the latest doctrine! In addition to revisions, we publish incremental "**SMARTupdates**" when feasible to update changes in doctrine or new publications. These SMARTupdates are printed/produced in a format that allow the reader to insert the change pages into the original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

VISA MasterCard AMERICAN EXPRESS Cards PayPal

INFO2 thelightningpress.com

(INFO2 SMARTbook) information advantage (ACTIVITIES, TASKS & CAPABILITIES)





Information is central to everything we do—it is the basis of intelligence, a fundamental element of command and control, and the foundation for communicating thoughts, opinions, and ideas. As a **critical resource**, Army forces fight for, defend, and fight with information while attacking a threat's ability to do the same.

We **no longer regard information as a separate consideration** or the sole purview of technical specialists. Instead, we view information as a resource that is integrated into operations with all available capabilities in a **combined arms approach** to **enable** command and control; **protect** data, information, and networks; **inform** audiences; **influence** threats and foreign relevant actors; and **attack** the threat's ability to exercise command and control.

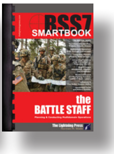
Army forces create and exploit **informational power** similarly to the joint force through five **information activities** (enable, protect, inform, influence, and attack). As a **dynamic of combat power,** Army forces fight for, defend, and fight with information to create and exploit **information advantages**—the use, protection, and exploitation of information to achieve objectives more effectively than enemies and adversaries do.

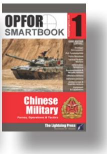
Throughout the competition continuum, the joint force commander integrates **operations in the information environment (OIE)** into joint plans and synchronizes it with other operations to create desired behaviors, reinforce or increase combat power, and gain advantage in the **information environment (IE)**.

DIME is our DOMAIN!™

SMARTbooks: Reference Essentials for the Instruments of National Power

Part of our "Military Reference" Series





ISBN 9781935886976
90000 >
9 781935 886976

www.TheLightningPress.com