ADP 3-13
INFORMATION

NOVEMBER 2023

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Foreword

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.

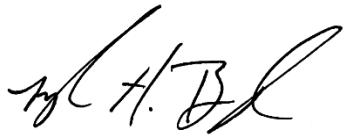
Advancements in information technologies and increased global connectivity continue to shape how we interact with each other and how forces fight. These advancements accelerate and expand the ability of joint and Army forces to collect, process, analyze, store, and communicate information at a scale previously unimaginable. Our primary adversaries now have many of the same capabilities to employ or exploit information the same as the United States does, and they are willing to employ them during competition, crisis, and conflict. In the same way other doctrine changes as the security environment changes, so must our doctrine on the use, protection, and exploitation of information.

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.

ADP 3-13 provides the intellectual underpinnings that describe how Army forces will gain, protect, and exploit information advantages. But doctrine is only the beginning. The hard work begins when we incorporate these ideas into leader development, education, and training. As leaders, it is our obligation to study, understand, and implement the doctrine in ADP 3-13.



MILFORD H. BEAGLE, JR.
LIEUTENANT GENERAL, USA
COMMANDING

Army Doctrine Publication
No. 3-13

Headquarters
Department of the Army
Washington, DC, 27 November 2023

INFORMATION

Contents

Figures

Tables

Vignettes

This page intentionally left blank.

Preface

ADP 3-13 serves as the Army's foundational doctrine for information. It provides the fundamental principles for considering how Army forces use, protect, and attack data and information to achieve objectives while affecting the threat's (adversary or enemy) ability to do the same. As a keystone publication, ADP 3-13 links the Army's applications of information to all warfighting functions and methods of warfare.

ADP 3-13 is applicable to all members of the profession of arms: leaders, Soldiers, and Army Civilian professionals. It applies to Army forces during the conduct of operations as well as to Army forces performing duties at home station. This publication provides the foundation for training and Army education system curricula and future capabilities development across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (known as DOTMLPF-P).

To comprehend the doctrine contained in ADP 3-13, readers must understand the fundamentals of multidomain operations described in ADP 3-0 and detailed in FM 3-0. They must understand the fundamentals of each warfighting function addressed in ADP 2-0, ADP 3-19, ADP 3-37, ADP 3-90, ADP 4-0, and ADP 6-0. Readers should also be familiar with applicable joint and multinational doctrine concerning information, to include information in joint operations described in JP 3-04 and allied information doctrine described in Allied Joint Publication (AJP)-10.1.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations when applying this doctrine. Commanders at all levels ensure their Soldiers operate in accordance with the law of armed conflict and the rules of engagement as discussed in FM 6-27. They also adhere to the Army ethic described in ADP 6-22.

This publication contains copyright material.

ADP 3-13 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and text. ADP 3-13 is the proponent publication (the authority) for some terms. When first defined in the text, ADP 3-13 proponent terms appear in bold italics, and definitions are bolded. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition. The glossary marks ADP 3-13 proponent terms with an asterisk (*).

The proponent of ADP 3-13 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations by email to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@army.mil on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATZL-MCD (ADP 3-13), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; or submit an electronic DA Form 2028.

Acknowledgements

The copyright owner listed here have granted permission to reproduce material from their works. The Source Notes lists all sources of quotations and vignettes.

Sourced by permission from "China's 'Three Warfares' in Theory and Practice in the South China Sea" by Doug Livermore. Copyright © 2018 by Georgetown Security Studies Review.

This page intentionally left blank.

Introduction

> *All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him.*
>
> Sun Tzu

Historically, successful commanders understood the importance of using information to create and exploit an advantage—a condition that puts a force in a favorable geographical, psychological, or moral position. They understood that knowing more than the enemy and acting effectively on that knowledge faster than their opponent provides an advantage. They understood that denying the enemy information or affecting the enemy's ability to communicate enhances friendly chances of success. Successful commanders also understood that using information combined with action or inaction to confuse the enemy creates favorable conditions for the friendly force.

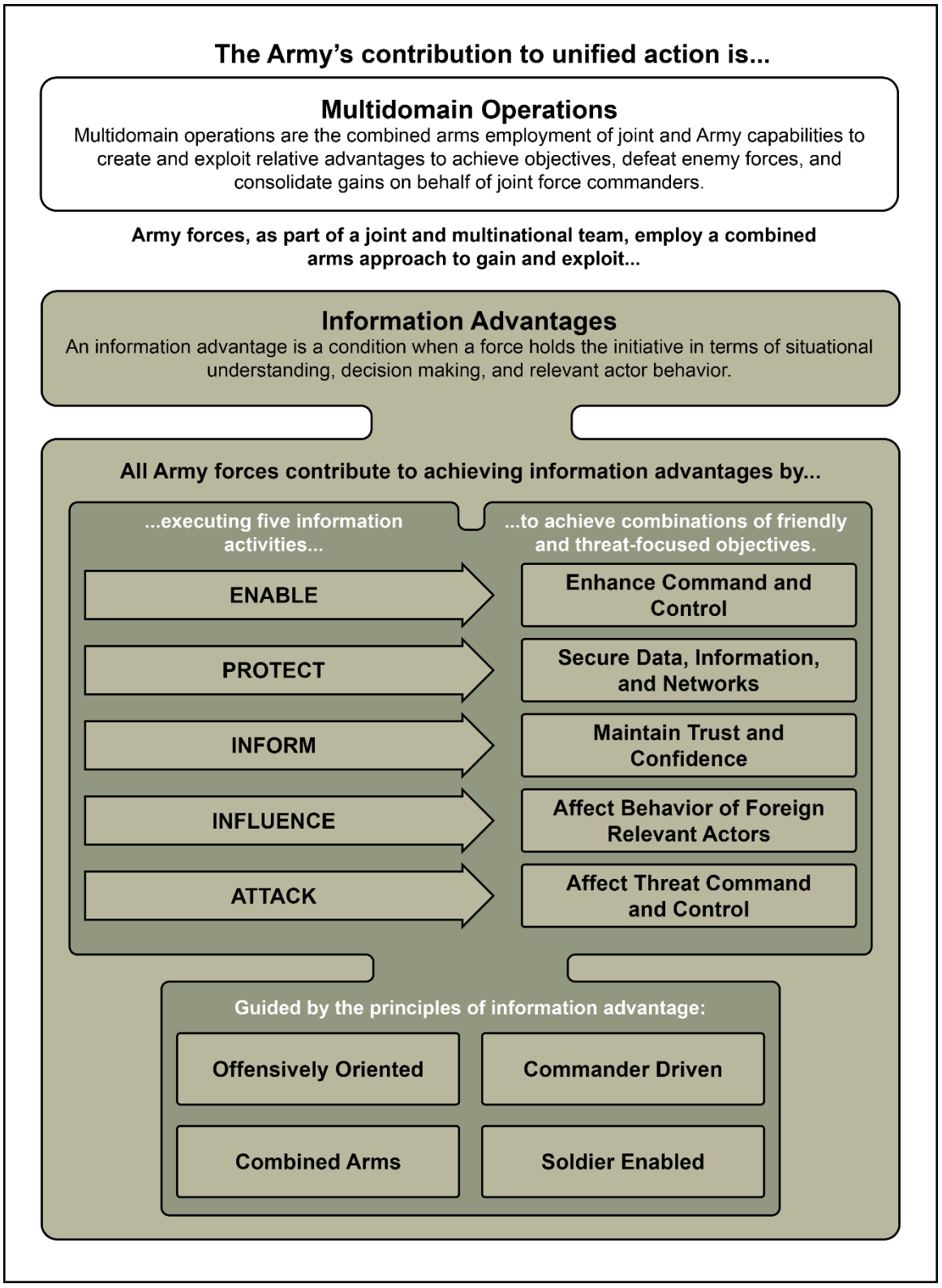
Today, military operations are characterized by the continuous growth of information technologies and data science that accelerate and expand the ability of forces to process, analyze, store, and communicate data and information. Despite friendly advances in information technology and networks, threats (adversaries and enemies) can degrade joint force information advantages held in the past. Within degraded environments, Army leaders at all echelons must have the ability to develop understanding, make decisions, communicate, and act decisively. To achieve this, Army forces fight for, defend, and fight with information as part of a continuous struggle to gain and exploit advantages above and below the threshold of armed conflict.

During operations, Army forces collect, process, analyze, and use data and information to understand situations, make decisions, and issue orders that result in action. They deny threats access to friendly data and information, protect decisions, and defend networks to ensure communications and enable command and control. Army forces communicate information to inform relevant audiences, correct misinformation, and counter threat disinformation. Army forces employ information in combination with physical action to influence threat decision making and behavior. They attack threat data, information, and networks to influence threat perceptions and behavior and to affect the threat's ability to exercise command and control of its own forces.

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.

Introductory Figure 1 on page viii depicts a framework for creating and exploiting information advantages—the use, protection, and exploitation of information to achieve objectives more effectively than the threat. Within this framework, Army forces plan and execute a variety of tasks linked by purpose supporting five information activities:

- Enable.
- Protect.
- Inform.
- Influence.
- Attack.



Introductory figure 1. Information advantage logic chart

Successfully executing information activities and associated tasks can lead to various human, information, and physical advantages. For example, a force that collects, processes, analyzes, and uses information to understand, decide, and act more effectively than the threat has an advantage. A force that effectively communicates and protects its information, while preventing the threat from doing the same, has an advantage. Using information to influence the behavior of foreign relevant actors more effectively than an adversary or enemy is an advantage. Any information advantage can build upon, or enable, physical and human advantages to achieve objectives.

Creating and exploiting relative advantages to achieve objectives is central to multidomain operations. Like physical and human advantages, information advantages are often temporary and change over time depending on the threat and changes in an operational environment. While friendly forces seek information advantages, threats are doing the same. As such, an information advantage is something to create, protect, and exploit across all domains below and above the threshold of armed conflict. To guide Army leaders in pursuit of information advantages, ADP 3-13 introduces four principles of information advantage:

- *Offensively oriented*—seize and exploit the initiative to create, protect, and exploit information advantages in all domains.
- *Combined arms*—integrate all available Army, joint, interagency, and multinational capabilities in pursuit of information advantages.
- *Commander driven*—visualize and describe the deliberate integration of information and capabilities to create maximum effects.
- *Soldier enabled*—understand that all Soldiers have a role in collecting, assessing, processing, communicating, and protecting information.

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.

ADP 3-13 also incorporates joint information doctrine from JP 3-04. JP 3-04 expands on the joint information function and transitions the joint force from information operations to joint operations in the information environment. ADP 3-13 summarizes this doctrine, describes how Army information activities nest with the joint information function, and describes how Army forces support the joint construct of operations in the information environment.

ADP 3-13 contains eight chapters. The following is a brief introduction by chapter.

Chapter 1 describes data and information and their relationship to situational understanding, decision making, and behavior. A discussion of informational power follows. Next, the chapter describes informational trends in the security environment and informational considerations within an operational environment. The chapter concludes by describing threat information warfare.

Chapter 2 provides an overview of Army operations and describes how creating and exploiting information advantages are key components of multidomain operations. The chapter continues by describing the information advantage framework. A description of warfighting functions' contributions to information advantages follows. The chapter then describes information advantage considerations during competition below armed conflict, crisis, and armed conflict. The chapter concludes with the tenets of operations and information principles that guide Army leaders in pursuit of information advantages.

Chapter 3 provides an overview of the enable information activity. A description of the tasks that facilitate situational understanding, decision making, and communications follows. The chapter concludes with considerations that enhance friendly command and control.

Chapter 4 provides an overview of the protect information activity. A description of the tasks that protect friendly data, information, and networks follows. The chapter concludes with considerations for effectively securing data, information, and networks.

Chapter 5 provides an overview of the inform information activity. A discussion of commander's communication synchronization follows. The chapter then describes inform information activity tasks. The chapter concludes with considerations for effectively informing Army, U.S. domestic, and international audiences.

Chapter 6 provides an overview of the influence information activity. A description of the tasks that contribute to influencing threats and other foreign audiences follows. The chapter concludes with considerations for affecting the behavior of foreign relevant actors.

Chapter 7 provides an overview of the attack information activity. A discussion of information attack methods follows. The chapter then describes tasks that affect threat situational understanding, decision making, and communications. The chapter concludes with considerations for degrading threat command and control and affecting threat information warfare capabilities.

Chapter 8 provides an overview of joint and multinational information advantage. A discussion of the relationship of Army information activities and the information joint function follows. The chapter then describes the relationship, planning responsibilities, and integration of Army information activities during operations. The chapter concludes with training and educating the force on information advantage.

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

ADP 3-13 lists new, modified, and rescinded terms in the introductory table.

Introductory table. New, modified, and rescinded terms

Term	***Action***
disinformation	ADP 3-13 becomes proponent
information activity	new term
information advantage	new term
Information for effect	ADP 3-13 becomes proponent
misinformation	ADP 3-13 becomes proponent
technical effects	new term

Chapter 1
Nature of Information

To guess at the intention of the enemy; to divine his opinion of yourself; to hide from him both your intentions and opinion; to mislead him by feigned manoeuvres; to invoke ruses, as well as digested schemes, so as to fight under the best conditions—this is and always was the art of war.

Napoleon

This chapter describes data and information and their relationship to understanding, decision making, and behavior. A discussion of informational power follows. Next, the chapter describes informational trends in the security environment and informational considerations of an operational environment (OE). The chapter concludes by describing threat information warfare.

INFORMATION EXPLAINED

1-1. 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.

DATA AND INFORMATION

1-2. 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.

1-3. 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.

ASSIGNMENT OF MEANING

1-4. 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.

Humans

1-5. 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. (Refer to ADP 6-0 for additional doctrine on the cognitive hierarchy and decision making.)

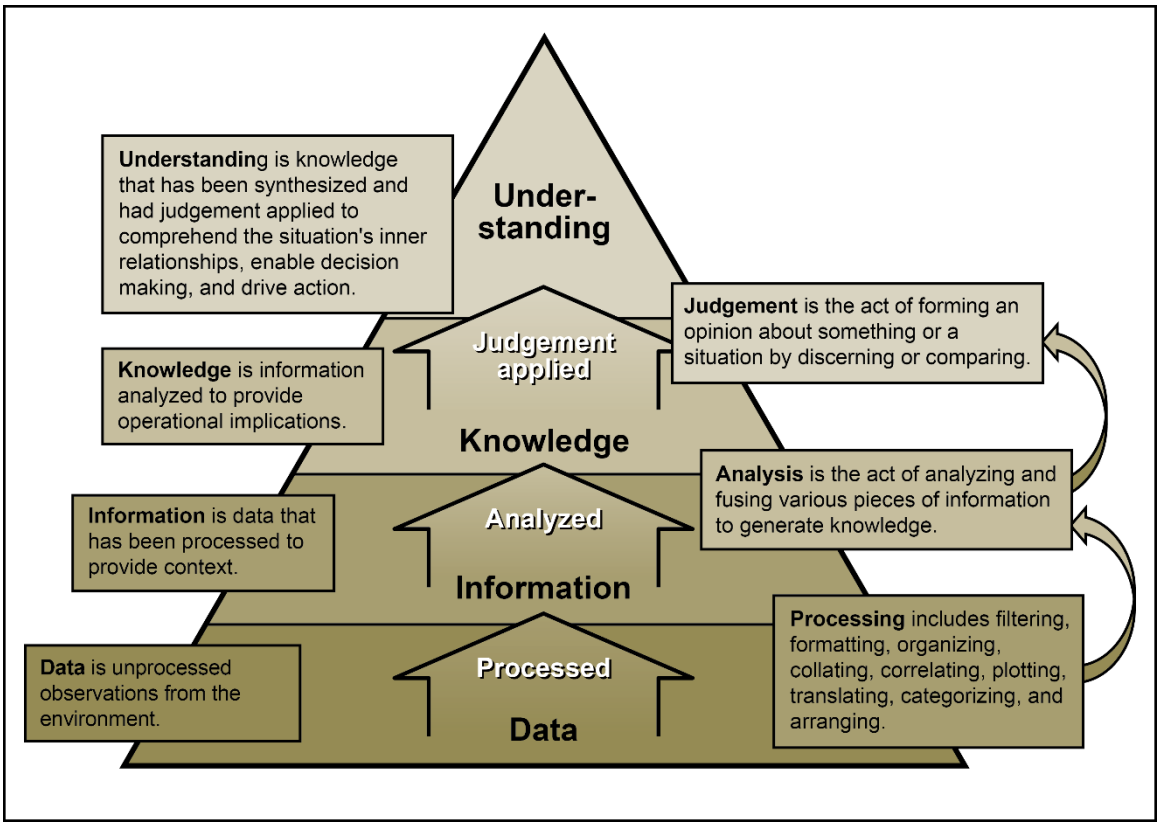


Figure 1-1. Cognitive hierarchy

1-6. 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.
- Drivers of behavior.

Inherent Informational Aspects

1-7. 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.

1-8. 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. Figure 1-2 provides examples of inherent informational aspects of operations and activities.

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. For example, a force in garrison or a force occupying battle positions.

Figure 1-2. Examples of inherent informational aspects

Drivers of Behavior

1-9. 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 the following:

- **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, and 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.

Automated Systems

1-10. Automated systems are a combination of hardware and software that allow computer systems, network devices, or machines to function with limited human intervention. Modern militaries depend on automated systems to perform basic functions such as communications, administration, data analytics, battle tracking, navigation, and detection. Examples of automated systems include integrated air defense, fire control, and supply management systems. These systems have varying degrees of autonomy depending on their programming. The functionality of these systems ranges from basic automation of simple, repetitive tasks to sophisticated artificial intelligence and machine learning.

1-11. Typically, automated systems assign meaning to data based on programming—a set of instructions that determine the actions of an automated system based on environmental conditions and inputs to the system. In some instances, automated systems enabled by artificial intelligence assign meaning and make decisions through environmental experience—apart and beyond base programming. For example, information-focused automated systems can rapidly search, sort, and collate publicly available information; identify events, issues, and trends in public sediment from around the world; and issue alerts to users.

1-12. Automated systems can quickly sort through volumes of data that would overload human decision makers and provide a concise analysis or take an action. When connected by a network, automated systems can exchange data across the globe at nearly light speed. Automated systems, however, are vulnerable to attack. Cyberspace attacks such as data poisoning, electromagnetic attacks, and physical signals such as sounds, visuals, and vibrations can impair an automated system.

INFORMATIONAL POWER

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 objectives.

JP 3-04

1-13. 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

1-14. 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.

1-15. 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. (Refer to JP 3-04 for a summary of the roles and responsibilities of U.S. government departments and agencies in the application of informational power.)

JOINT INFORMATIONAL POWER

1-16. 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.

(See Chapter 8 for a summary of joint information doctrine, to include joint information advantage, the joint information function, and joint operations in the information environment.)

INFORMATION AS A DYNAMIC OF COMBAT POWER

1-17. Army forces create and exploit informational power similarly to the joint force through five information activities (enable, protect, inform, influence, and attack) as described in Chapter 2. 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.

1-18. 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.

1-19. 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 FM 3-0 for more information on combat power.)

Fighting For and With Information

On 5 April 2003, 2d Brigade, 3d Infantry Division (Mechanized) mounted an operation into western Baghdad in preparation for the division's advance on the Iraqi capital. The mission was planned as a battalion-sized reconnaissance in force (coined a thunder run) to determine the composition, strength, and disposition of enemy defenses.

The operation, executed by 1st Battalion, 64th Armor, was considered a reasonable and acceptable risk despite the ambiguity of the enemy situation. Command guidance was simply to "conduct a movement to contact north along Highway 8 to determine the enemy's disposition, strength, and will to fight." This mission-type order allowed for flexibility in seizing the initiative and reacting to the enemy. Unit commanders believed that the superior quality of their forces would mitigate the inherent risk in the operation. They were right. Despite heavy resistance, the armored column reached its objective. Commanders concluded the reconnaissance in force had taken enemy forces completely by surprise and damaged their physical and mental ability to resist.

The operation demonstrated that U.S. armored forces could penetrate Baghdad at their choosing. Moreover, it met the original intent by providing excellent indicators of enemy tactics, strength, and locations—critical information to enable future decisions. Senior commanders came to view the reconnaissance in force as a prelude to additional armored missions in and out of the city that would disrupt the Iraqi defenses and counter enemy propaganda.

Using the lessons learned on 5 April, 3d Infantry Division launched a larger operation on 7 April, which resulted in the occupation of downtown Baghdad. Broadcast live by major news outlets worldwide, and reinforced by U.S. Central Command messaging, this operation discredited the Iraqi Minister of Information claims that "No U.S. or British forces were in Baghdad." While fighting continued for several days throughout the city, the second thunder run broke the regime's back as senior Iraqi political and military leaders fled their posts, resulting in the collapse of the Ba'athist government.

INFORMATION IN THE SECURITY ENVIRONMENT

1-20. The strategic security environment consists of national, international, and global factors that affect the decisions of senior civilian and military leaders with respect to employing U.S. instruments of national power. Continued advances in information technologies constantly impact the strategic security environment. Governments, institutions, militaries, commercial organizations, and individuals rely on communications networks to perform basic functions. Informational technologies enable and accelerate global human-to-human, human-to-computer, and computer-to-computer interactions resulting in an exponential growth in the amount of information created, processed, and shared.

1-21. Smart phones, the internet, and social media accelerate and expand collective awareness of events, issues, and concerns within and outside an operational area. These developments have dramatically increased the speed at which information can affect an OE. Billions of people are connected in an instantly responsive network, through which information and ideas are shared worldwide. These ideas ignite passions, spark new

perspectives, and crystallize deeply held beliefs that influence how governments, militaries, organizations, and people act. The exponential growth in computer capability and global connectivity continues to shape the way people interact and how forces fight. These devices and the internet provide threats with an enormous amount of digital information concerning friendly forces, to include location, intentions, timings, and tactics.

1-22. A central challenge to U.S. security is the reemergence of long-term, strategic competition. Adversaries, to include China, Russia, Iran, and North Korea, use informational power to try to gain regional influence and control the global narrative well ahead of potential armed conflict in what are otherwise considered by most societies as times of peace. Competition for information and ideas is continuous and persistent. Adversaries rely on enduring campaigns of influence to achieve their objectives. Media manipulation and censorship, disinformation campaigns transmitted through social media, physical presence and activities, and public diplomacy compose some of a threat's perception management activities used to influence both internal and external audiences. The three warfares strategy vignette illustrates how the Peoples Republic of China applies informational power to gain regional influence.

The Three Warfares Strategy in the South China Sea

The Peoples Republic of China (PRC) uses a strategy to achieve objectives short of open war called the "three warfares:" public opinion and media warfare, psychological warfare, and legal warfare (also referred to as lawfare). The PRC employs the three warfares to assert control of key maritime terrain in the South China Sea without triggering an effective response from, or conflict with, regional neighbors or the United States. Since 2013 the PRC has constructed and militarized many artificial islands across the South China Sea despite international condemnation. This has effectively undermined the ability of the PRC's neighbors to oppose its pursuit of territorial control.

To sow doubt and confusion among its neighbors, the PRC employs paramilitary forces—primarily its maritime militia—to reinforce its claims and prevent a military response. By not taking overt military actions with flagged naval combatants against international ships, the PRC effectively maintains the freedom to operate, enforce claims, and exploit natural resources in the disputed waters unopposed. Additionally, the PRC has engaged in aggressive media messaging using regional and global news outlets and digital media to promote its narrative of rightful historical claims. The combination of physical action, information activities, and political intimidation works effectively.

Even though this narrative is not accepted by most nations in the international community, it is consistent and has become normalized. The observed behavior of the PRC in the South China Sea demonstrates the practical application of the three warfares as a way of combining civil-military posturing, propaganda, physical activities, and legal obfuscation to buy the PRC time—which serves further to strengthen its position and prevent an effective response by its neighbors.

1-23. Nation states remain the principal actors on the global stage, but nonstate actors also threaten the security environment with increasingly sophisticated information capabilities. Terrorists, transnational criminal organizations, hackers, and other malicious nonstate actors seek to transform global affairs with increased abilities. Terrorism remains a persistent threat driven by ideology and unstable political and economic structures. Some of these groups act within the United States. Transnational criminal organizations affect the U.S. economy and negatively affect the nation's security. Hackers are not bound by geography; they can hold worldwide government and commercial entities hostage and steal data and information to sell to threats. (See paragraphs 1-42 through 1-49 for a discussion of threat information warfare.)

INFORMATION WITHIN AN OPERATIONAL ENVIRONMENT

1-24. Within the broader strategic security environment, Army forces conduct operations in specific OEs. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). For Army forces, an OE includes portions of the land, maritime, air, space, and cyberspace domains understood through three dimensions (human, information, and physical). The land, maritime, air, and space domains are defined by their physical areas. The cyberspace domain, a man-made network of networks, transits and connects the other domains through the electromagnetic spectrum as represented by the dots shown in Figure 1-3. (Refer to FM 3-0 for a detailed discussion of each domain.)

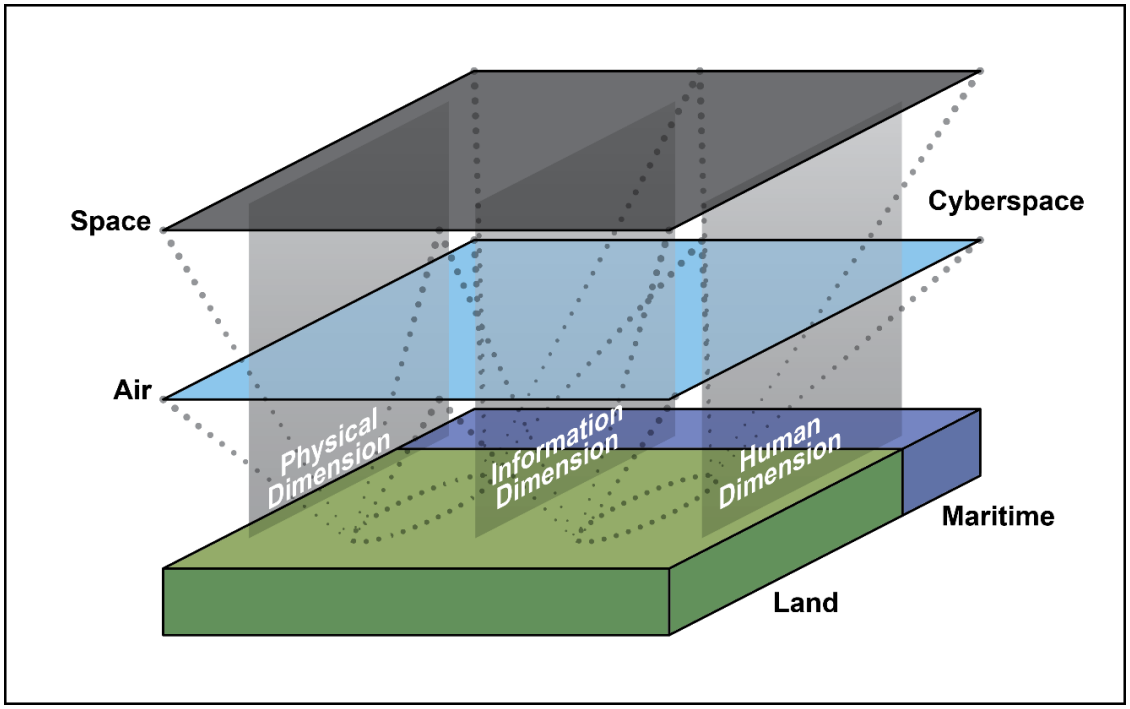


Figure 1-3. Domains and dimensions of an operational environment

1-25. An OE consists of the totality of factors, specific circumstances, and conditions that impact the conduct of operations. Understanding an OE enables leaders to better identify problems; anticipate potential outcomes; and understand the results of various friendly, enemy, adversary, and neutral party actions and the effects these actions have on achieving objectives.

1-26. 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. *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).

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).

1-27. 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.

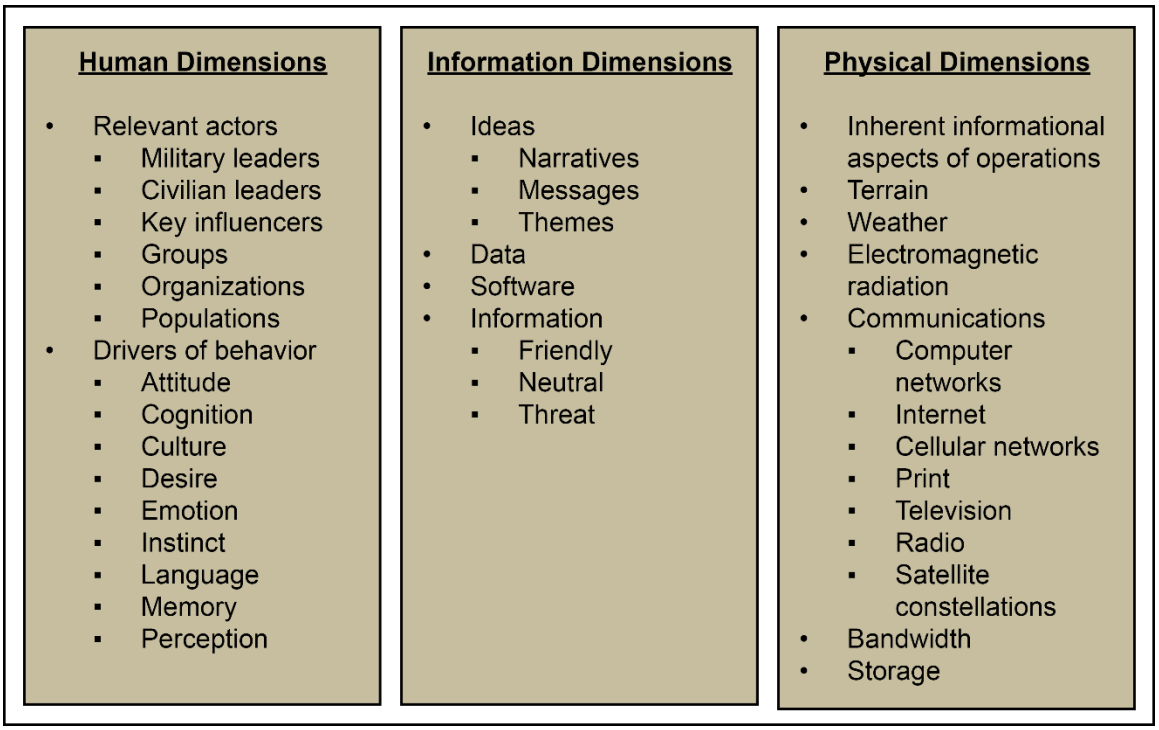


Figure 1-4. Example informational considerations

HUMAN DIMENSION

1-28. The *human dimension* encompasses people and the interaction between individuals and groups, how they understand information and events, make decisions, generate will, and act within an operational environment (FM 3-0). War is shaped by human nature and the complex interrelationship of cognitive (how people think) and psychological (mental or emotional state of a person) factors. Values and ethics are some of the factors that motivate both the cause for going to war as well as restrictions on the conduct of war. Fear, passion, camaraderie, grief, and many other emotions affect war participants' resolve. Emotions affect the behavior of combatants, how and when leaders decide to persevere, and when to give up. Individuals react differently to the stress of war; an act that may break the will of one enemy may only serve to stiffen the resolve of another. The will to act and fight emerges from the complex interrelationships in this dimension. Influencing these factors—by affecting perceptions, attitudes, and motivations—should underpin most, if not all, military objectives. (See paragraph 1-9 for factors that drive human behavior.)

1-29. Informational considerations in the human dimension include identification of human relevant actors, analysis of how relevant actors tend to process information, and prediction of their likely behaviors. A *relevant actor* is an 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 (JP 3-04). Understanding relevant actors and their relationships helps Army leaders to develop ways to influence their behavior through physical and informational means. Those relevant actors which the force intends to affect become audiences to inform or target audiences or targets for deception, physical attack, or other action. In public affairs, an *audience* is a broadly-defined group that contains stakeholders and/or publics relevant to military operations (JP 3-61). A *target audience* is an individual or group selected for influence (JP 3-04). A

target is an entity or object that performs a function for the threat considered for possible engagement or other action (JP 3-60).

INFORMATION DIMENSION

1-30. The *information dimension* is the content and data that individuals, groups, and information systems communicate and exchange, as well as the analytics and technical processes used to exchange information within an operational environment (FM 3-0). Data and information are available globally in near real time. The ability to access data and information—from anywhere, at any time—broadens and accelerates human interaction across multiple levels, including person to person, person to organization, person to government, and government to government. Data and information may be highly controlled as in military classified information or may be publicly available. Publicly available information is information that has been published or broadcast for public consumption. This type of information is available to the public online, on request, through subscription or purchase, or could be seen or heard by a casual observer.

1-31. Informational considerations in this dimension include data and information used by relevant actors. Individuals, groups, and organizations record their perceptions in many formats ranging from spoken history to libraries, both physical and virtual. This body of information, collectively, can provide insights about how various groups, organizations, and countries might interpret Army operations. Although it is difficult to predict an individual's reaction to activities by Army forces, groups tend to be more consistent and predictable. A group, faction, or nation's prevailing narratives can provide a great deal of insight into how that group, faction, or nation might perceive Army operations. Threat doctrine is another example of relevant information that provides insight into how an enemy force may conduct operations and how it may respond to friendly actions.

1-32. Identifying and understanding narratives in an OE are important informational considerations. Narratives—complementary, neutral, and hostile to the friendly force—are essential parts of any OE. A narrative is a way of presenting a situation or events that reflect a particular point of view with reasonable or believable logic. Individuals, groups, organizations, and countries all have narratives with many components that reflect and reveal how they define themselves. Political parties, social organizations, and government institutions, for example, have stories bound chronologically and spatially. They incorporate ideas, historical events, and artifacts tied together with a logic that explains their reason for being.

1-33. Army forces reinforce narratives based upon what they did, what they are doing, and what they can do. Trust in the Army and Army forces is based upon demonstrated performance over time. Themes and messages complement friendly narratives. A theme is a distinct, unifying idea that supports a narrative. There may be multiple themes developed to support a narrative. A *message* is a narrowly focused communication directed at a specific audience to support a specific theme (JP 3-61). Depending on an audience or actor, themes and messages are used in different ways.

> The stated purpose of operations contributes to a narrative, but the most critical factor is performing the activities that themes and messages describe.

1-34. When considering the use of information by friendly, neutral, and threat actors, analysis should identify both malign and benign information including its content, purpose, source, and associated systems and processes. This includes identifying and analyzing misinformation, propaganda, disinformation, and information for effect. ***Misinformation*** **is unintentional incorrect information from any source.** Misinformation is disseminated through ignorance or with the belief that the incorrect information is correct. Misinformation has no malicious intent. Identifying misinformation enables Army leaders to correct the record concerning misinformation about Army and friendly forces, operations, and other activities in an OE.

1-35. Propaganda is information that is biased or misleading and designed to influence the opinions, emotions, attitudes, or behaviors of any group to benefit the sponsor. Both disinformation and information for effect are forms of propaganda. ***Disinformation*** **is incomplete, incorrect, or out of context information deliberately used to influence audiences.** Disinformation creates narratives that can spread quickly and instill an array of emotions and behaviors among groups, ranging from disinterest to violence. Relevant actors employ disinformation to shape public opinion, attract partners, weaken alliances, sow discord among populations, and deceive forces. Disinformation has a malicious intent. Sources of disinformation often rely

on people to promulgate the information unwittingly, unaware that the information is inaccurate. Analysis allows Army forces to determine the source and purpose of information; what may first appear as misinformation may be a result of disinformation.

1-36. ***Information for effect*** **is the use, publication, or broadcast of factual information to negatively affect perceptions and/or damage credibility and capability of the targeted group**. Unlike misinformation and disinformation which is incorrect or intentionally misleading, information for effect is factual and released at a time, at a place, and via means that will generate the most intended effect. Malign use of information for effect sometimes includes images or videos of friendly forces conducting operations that resulted in collateral damage. Videos of improvised explosive devices striking friendly forces provide another example of the use of information for effect to undermine the perceived strength of friendly forces. Friendly forces may mitigate information for effect through timely documentation of friendly force activities and release of statements and audio-visual products showing actions and results in near real time.

PHYSICAL DIMENSION

1-37. The *physical dimension* is the material characteristics and capabilities, both natural and manufactured, within an operational environment (FM 3-0). While war is a human endeavor, it occurs in the physical world conducted with physical things. Each of the domains is inherently physical. Terrain, weather, military formations, electromagnetic radiation, weapons systems and their ranges, and many of the things that support or sustain forces are part of the physical dimension. Operations and activities in the physical dimension create effects in the human and information dimensions.

1-38. Informational considerations in the physical dimension include the natural and man-made aspects of an OE that affect communications—human to human, human to machine, and machine to machine. Geography, distance, and weather directly impact the ability of man-made capabilities to exchange data and information. The electromagnetic spectrum—the entire range of frequencies of electromagnetic radiation—permeates all domains and serves as a vital link for exchanging data and information across networks and information systems. Physical characteristics of the land domain also affect person-to-person communications. For example, a mountain range that separates two populations or groups impacts contact and communications between them. Understanding physical aspects of the domains and the electromagnetic spectrum helps determine the impacts on friendly, threat, and neutral communications capabilities and courses of actions available to employ them.

1-39. Communications capabilities are important physical informational considerations. Analysis of friendly, threat, and commercial communications capabilities and their impact on operations guides communications planning, communications protection, and methods to degrade threat communications. Communications considerations include bandwidth—the maximum amount of data transmitted over a network connection in a given amount of time. Army leaders understand the physical limitation of data transport and exchange, and they develop communications plans that prioritize bandwidth use.

1-40. Important physical informational considerations include threat intelligence and information warfare capabilities. Analysis of threat collections, intelligence, cyberspace, and electromagnetic capabilities informs leaders on ways to protect friendly data and information as well as to help identify threat targets for attack.

Army leaders account for being under constant observation. Air, space, and cyberspace capabilities increase the likelihood that threat forces can gain and maintain continuous visual and electromagnetic contact with Army forces.

1-41. Informational considerations also include the inherent informational aspects of operations. Everything Army forces do impacts an OE either intentionally or incidentally. Whether executing a feint or conducting resupply, all Army activities can be observed and have the potential to affect the behavior of relevant actors. The perceptions that relevant actors draw from observing operations and actions will likely drive their behaviors, potentially making them vulnerable to exploitation to include deception. As such, leaders consider the inherent informational aspects of operations and activities as well as their potential to reinforce, prevent, or change behaviors.

THREAT INFORMATION WARFARE

> *The [People's Liberation Army] defines information attack as any [information warfare] activity intended to weaken or deprive the enemy of control of information. Information attack is the primary means by which information warfare is won, and it is the key to achieving information superiority.*
>
> ATP 7-100.3

1-42. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats may include individuals, groups of individuals, paramilitary or military forces, criminal elements, nation-states, or national alliances. A threat may be a nation-state with an authoritarian government or a nonstate actor that follows an extremist ideology. Threats operate outside and within the United States.

1-43. In general, a threat can be categorized as an adversary or enemy. An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0). An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). An enemy is called a combatant and is treated as such under the law of armed conflict. The most dangerous threats to the United States are peer threats. A peer threat is an adversary or enemy with capabilities and the capacity to oppose U.S. forces across multiple domains worldwide or in a specific region in which it has a significant relative advantage.

1-44. In the context of the threat, information warfare refers to a threat's orchestrated use of information activities (such as cyberspace operations, electromagnetic warfare, psychological warfare, and influence operations) to achieve objectives from the strategic to the tactical levels of warfare. At the tactical level, threat information warfare consists of specifically planned and integrated actions taken to achieve advantages at critical points and times.

Note. There is not a single-source threat doctrine on information warfare. While similar in many ways, each threat nation and threat force will employ informational power based on their capabilities and their understanding of military art and science. TC 7-100.2, *Opposing Forces*, provides a base model for threat tactical information warfare. ATP 7-100.3, *Chinese Tactics*, provides specifics on tactical Chinese information warfare. Future Army techniques publications in development focus on Russian, North Korean, and Iranian information warfare tactics.

1-45. Threat information warfare seeks to blur the divide between peace and war, control access to information, shape an OE with narratives and propaganda, and deny opponents information in armed conflict through systems confrontation and destruction. Peer threats use diverse means to conduct information warfare, which may include—

- Cyberspace operations.
- Psychological warfare.
- Influence operations.
- Movement and positioning of forces.
- Deception.
- Electromagnetic warfare.
- Physical destruction.
- Political and legal warfare.
- Active measures (espionage, sabotage, and assassinations).
- The use of proxies and nonstate actors.

1-46. The Peoples Republic of China's Three Warfares Strategy described on page 1-7 illustrates an example of threat information warfare. The Russian Federation's information warfare concept of reflexive control is another example. Reflexive control is an information-centric theory rooted in manipulating perception and the actions taken to create confusion and paralysis or to influence opponent behaviors and steer events toward Russia's advantage. Reflexive control is a concept that targets geopolitical opponents at the strategic level

down to enemies on the battlefield at the tactical level. Like China's Three Warfares Strategy, Russia's approach to information warfare involves a strong emphasis on disinformation, media, and psychological warfare to target opposing societies, governments, and military organizations as described in the Russian Activities vignette that follows.

Russian Activities in Ukraine 2014

Russia's annexation of Crimea in 2014 is a prime example of a peer threat's use of information warfare in operations. In February 2014, the pro-Russia Ukrainian government in Kyiv was ousted, leading to widespread protests and instability throughout Ukraine. In Crimea, a Ukrainian peninsula along the northern coast of the Black Sea in Eastern Europe, widespread protests occurred against the interim government and demonstrations by pro-Russian separatists.

Russia used the ensuing chaos to insert numerous troops into the region. First, Russian forces used physical attacks to cut fiber-optic communications lines, electromagnetic warfare to jam telephones and radios, and cyberspace attacks to severely degrade news outlets and websites, effectively creating an information blackout. Then Russian forces entered Crimea wearing no identifying insignia and took swift control of key government infrastructure. Rather than being identified as invading Russian forces, they were simply referred to as "little green men." Russian control over information sowed doubt and confusion, delayed the ability to communicate and make decisions, and prevented Ukrainian forces from organizing and resisting. In short order, a large-scale surrender of Ukrainian forces had occurred, and Russia had taken control of Crimea.

Russian activities prior to and after the invasion and annexation of Crimea included—

- **Providing overt and covert support to Crimean separatists.** Separatist elements carefully cultivated an image as polite protectors of the Crimean population and encouraged the ethnic Russian majority's desire for autonomy. Covert Russian agents fomented unrest. They undermined the Ukrainian government in Crimea, overwhelmed pro-Ukrainian security forces, and backed local Crimean separatists as they occupied key government buildings, facilitating the isolation of the Crimean Peninsula.
- **Manipulating and controlling the flow and content of information.** The Russians quietly removed all non-Russian radio and television stations in Crimea and cut the cable carrying internet traffic to and from the peninsula. Russia dominated the media with propaganda and patriotic themes to legitimize Crimea's call for independence and its eventual annexation. Meanwhile, Russia and its local supporters blocked, intercepted, and manipulated pro-Ukrainian media so there was no effective alternative to the Russian ethno-sectarian narrative.
- **Promoting a Russian nationalist narrative in the region and around the world.** Russia intensified its ethno-sectarian narrative while its propaganda characterized pro-Ukrainian forces as Nazis and the North Atlantic Treaty Organization as a threat. In Ukraine, Russia disrupted communication, to include access to internet and other forms of media, inhibiting the Ukrainian response to separatist operations.

1-47. Other threats, such as Iran and nonstate actors like Hamas, use similar theories and concepts to gain positions of relative advantage in or through the human and information dimensions. These positions allow them to exploit vulnerabilities in their opponents and negate physical advantages. The use of information warfare by nonstate actors is akin to the historic use of guerrilla warfare and tactics to gain physical advantages over a stronger and larger force.

1-48. Tactical threat information warfare attacks surveillance and target acquisition sensors, C2 centers and nodes, decision makers, data and information, telecommunications systems and infrastructure, population groups, and relevant actors. Threats typically target information links, such as radio frequency receivers, communications devices, and information protocols. Tactical threat information warfare activities are employed to—

- Destroy or disrupt friendly C2.
- Destroy or deceive friendly reconnaissance, surveillance, and target acquisition.
- Deny friendly situational understanding.
- Isolate key elements of a friendly force, particularly allies and partners.
- Distort or deny information to relevant actors and audiences.

Chapter 2

Fundamentals of Information Advantage

As our present theory is to destroy 'personnel,' so should our new theory be to destroy 'command,' not after the enemy's personnel has been disorganised, but before it has been attacked, so that it may be found in a state of complete disorganisation when attacked.

J.F.C. Fuller

This chapter provides an overview of Army operations and describes how creating and exploiting information advantages is a key aspect of multidomain operations. The chapter continues by describing the information advantage framework. A description of warfighting function contributions to information advantages follows. The chapter then describes information advantages during competition below armed conflict, crisis, and armed conflict. The chapter concludes with the tenets and principles that guide Army leaders in pursuit of information advantages.

ARMY OPERATIONS

2-1. 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. Within these contexts, Army forces shape operational environments (OEs), counter aggression on land during crisis, prevail during large-scale ground combat, and consolidate gains. (See paragraphs 2-37 through 2-48 for an expanded discussion of information advantage and the strategic contexts.)

2-2. Competition below armed conflict exists when two or more state or nonstate adversaries have incompatible interests, but neither seeks armed conflict. Crisis is an emerging incident or situation involving a possible threat to the United States, its citizens, its forces, or its interests in which an actor contemplates military force to achieve its national or strategic objectives. Armed conflict occurs when a state or nonstate actor uses lethal force as the primary means to satisfy its interests. In times of relative peace or in armed conflict, Army forces contribute to the achievement of objectives across a range of military operations as shown in Figure 2-1.

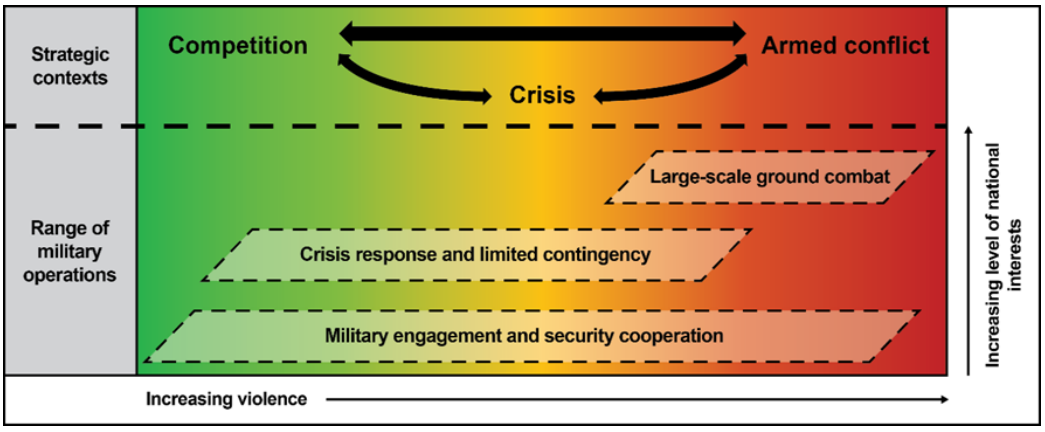


Figure 2-1. Army strategic contexts and range of military operations

2-3. An *operation* is a sequence of tactical actions with a common purpose or unifying theme (JP 1, Volume 1). 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. *Large-scale combat operations* are extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives (ADP 3-0). Whether conducting security cooperation activities or large-scale combat operations, Army forces are guided by the Army's operational concept of multidomain operations. (Refer to FM 3-0 for more information on the strategic contexts and range of military operations.)

MULTIDOMAIN OPERATIONS

2-4. 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.

Army forces integrate land, maritime, air, space, and cyberspace capabilities to create human, information, and physical advantages to achieve objectives.

2-5. 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. Army forces employ organic capabilities in multiple domains, request capabilities from their higher headquarters, and continuously benefit from maritime, air, space, and cyberspace capabilities that they do not control. Space-based global positioning and satellite communications are examples of capabilities from which Army forces benefit but do not necessarily control. Lower echelons may not always notice the opportunities created by higher echelons or other forces that operate primarily in other domains; however, leaders must understand how the absence of those opportunities affects their concepts of operations, decision making, and risk assessment.

2-6. 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.

2-7. Relative advantages are characterized as human, information, or physical, and they complement each other. Physical actions, particularly involving the use of force, usually generate psychological effects. When exploited, these effects can lead to information advantages as friendly forces use information to influence enemy behavior. 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

2-8. 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. Human advantages include, but are not limited to the following:

- 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

2-9. 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. 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.

2-10. 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.

PHYSICAL ADVANTAGE

2-11. 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. Physical advantages include, but are not limited to the following:

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

INFORMATION ADVANTAGE FRAMEWORK

2-12. Figure 2-2 on page 2-4 depicts 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). **An *information activity* is a collection of tasks linked by purpose to affect how humans and automated systems derive meaning from, use, and act upon, or are influenced by, information.** Each information activity incorporates several tasks and subtasks from the warfighting functions to achieve a variety of friendly and threat-based objectives.

Information activities are interdependent. For example, both the protect and inform information activities help protect the force from malign influence. Guided by the principles of information advantage, Army leaders plan, prepare, execute, and assess information activities as part of the operations process discussed in Chapter 8.

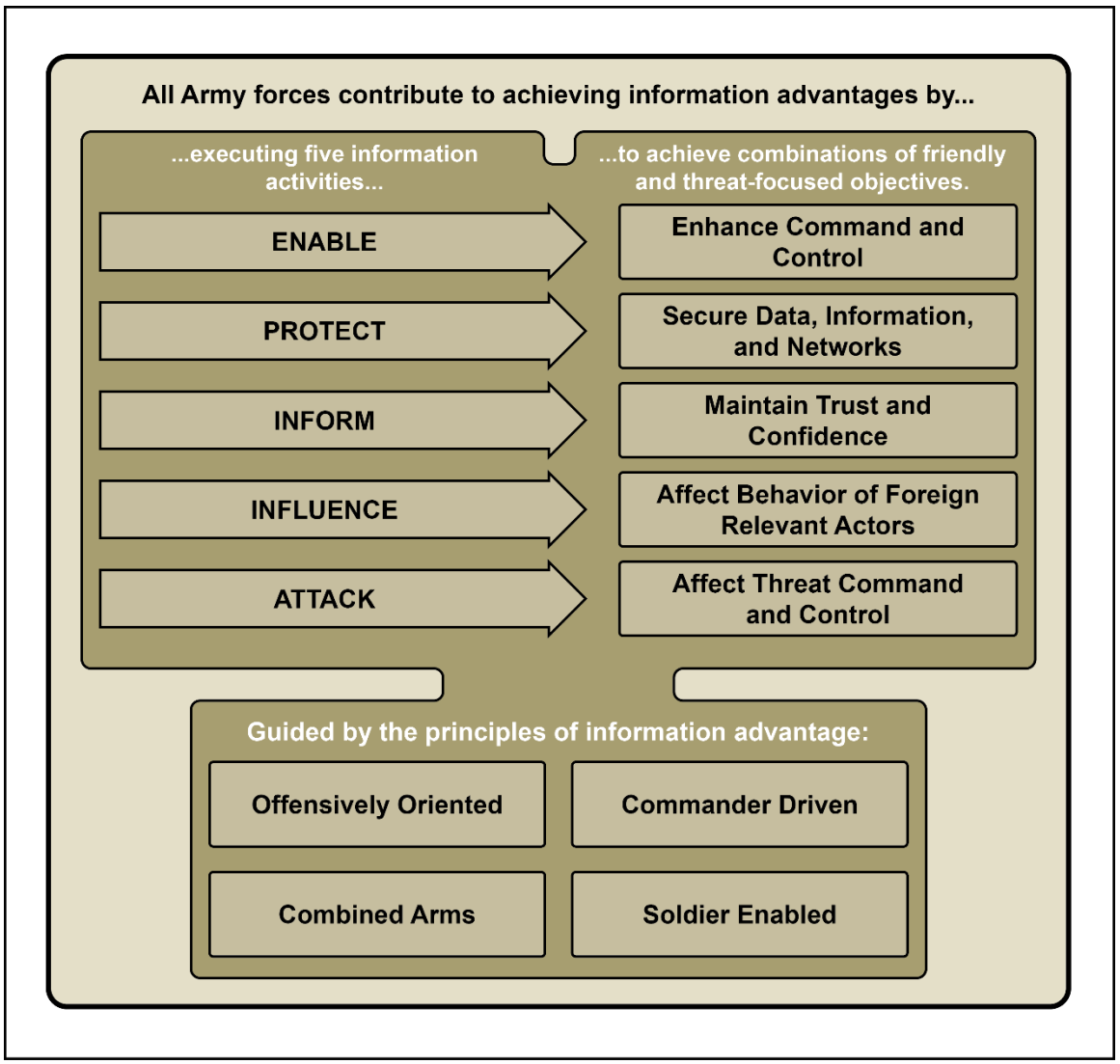


Figure 2-2. Information advantage framework

ENABLE

2-13. The enable information activity includes tasks that enhance friendly C2. The focus of this activity is to improve situational understanding, decision making, and communications. Throughout operations, Army forces collect, process, and analyze information to develop situational understanding that, in turn, facilitates effective decision making. Leaders then communicate their decisions to subordinates and direct actions. Based on feedback and assessment of the situation, Army leaders adjust operations as required. The network provides the backbone for exchanging data and information, enabling shared understanding and enhancing the exercise of C2 of Army forces. Tasks within the enable information activity include—

The force that understands, decides, and acts more effectively than its opponent has an information advantage.

- Establish, operate, and maintain C2 systems.
- Conduct the operations process and coordinate across echelons.
- Execute the integrating processes (intelligence preparation of the operational environment [IPOE] information collection, targeting, risk management, and knowledge management).
- Enhance understanding of an OE.

2-14. While all warfighting functions enhance the exercise of C2, the C2 and intelligence warfighting functions are the largest contributors. The C2 warfighting function tasks and system (people, processes, networks, and command posts) enable commanders to command forces and control operations. The tasks and systems in the intelligence warfighting function enable the exercise of C2 by facilitating the understanding of enemy, terrain, weather, civil considerations, and other aspects of an OE. (See Chapter 3 for a detailed discussion of the enable information activity.)

PROTECT

2-15. The protect information activity includes tasks that secure friendly data, information, and networks. This activity focuses on denying threat access to friendly data and information while preserving friendly communications capabilities. Preventing threat access to friendly data and information not only protects the friendly force but hinders the threat's ability to accurately understand situations and make effective decisions. Defending friendly data, information, and networks enables friendly decision making and ensures functional communications. The tasks within the protect information activity include—

The force that protects its data, information, and ability to communicate more effectively than its opponent has an information advantage.

- Secure and obscure information.
- Conduct security activities.
- Defend the network, data, and systems.

2-16. The protection and movement and maneuver warfighting functions are the largest contributors to the protect information activity. The protection warfighting function consists of tasks and systems that prevent or mitigate friendly detection and mitigate threat effects, to include information protection and operations security (OPSEC). The movement and maneuver warfighting function consists of tasks and systems to employ forces to achieve a position of relative advantage and include security operations that counter threat reconnaissance and surveillance. (See Chapter 4 for a detailed discussion of the protect information activity.)

INFORM

2-17. The inform information activity includes tasks that foster informed perceptions of military operations and activities among various audiences. The focus of this activity is to maintain the trust and confidence of internal (members of the U.S. Army, Army Civilians, contractors, and their family members) and external audiences (U.S. domestic and international audiences). The proactive release of accurate information to Army, domestic, and international audiences puts operations in context, facilitates informed perceptions about the Army, increases friendly force resiliency, and undermines threat disinformation activities. The tasks within the inform information activity include the following:

The force that corrects misinformation, counters disinformation, and informs audiences more effectively than its opponent has an information advantage.

- Inform and educate Army audiences.
- Inform U.S. domestic audiences.
- Inform international audiences.

2-18. The C2 and intelligence warfighting functions are primary contributors to the inform information activity. As part of the C2 warfighting function, commanders and leaders conduct public communication, disseminate command information, correct misinformation, and counter disinformation. The intelligence warfighting function is essential to identifying foreign threat malign information activities, to include disinformation campaigns. (See Chapter 5 for a detailed discussion of the inform information activity.)

INFLUENCE

2-19. The influence information activity includes tasks that affect the thinking and ultimately the behavior of threats and other foreign audiences. This activity focuses on reinforcing or changing how individuals and groups think, feel, and act in support of objectives. Army forces influence threats to decrease combat effectiveness, erode unit cohesion, diminish morale and will, and deceive threat forces about friendly intent. Influence efforts toward other foreign audiences range from strengthening mutual support to discouraging an audience's support for an adversary or enemy. The tasks within the influence information activity include—

The force that combines actions and information to affect the behavior of foreign relevant actors has an information advantage.

- Influence threat perception and behaviors.
- Influence other foreign audiences.

2-20. The inherent informational aspects (see paragraph 1-7 for informational aspects) of all warfighting functions contribute to influencing threats and other foreign audiences. Army forces deliberately plan actions and supporting messages to affect threat perceptions and ultimately threat behavior. As part of operations, commanders direct or coordinate for deception, military information support operations (MISO), civil affairs operations, and Soldier and leader engagements to influence foreign relevant actors. (See Chapter 6 for a detailed discussion of the influence information activity.)

ATTACK

2-21. The attack information activity includes tasks that affect the threat's ability to exercise C2. The focus of this activity is to affect threat data and the threat's physical capabilities used to communicate and conduct information warfare. This includes the data and communications between automated systems such as the communications between radars, fire control systems, and firing systems.

The force that can communicate data and information more effectively than its opponent has an information advantage.

2-22. Threat C2 nodes (command posts, signal centers, networks, and information systems) and sensors (surveillance, target acquisition, and radars) are often high-payoff targets for Army forces. As part of the scheme of fires, Army forces attack these targets using physical destruction, electromagnetic attack, and offensive cyberspace operations to hinder the threat's C2 abilities. Army forces also attack threat data, information, and physical capabilities used to exchange data and information. The tasks within the attack information activity include—

- Degrade threat C2.
- Affect threat information warfare capabilities.

2-23. Informed by intelligence, the fires and movement and maneuver warfighting functions are the primary contributors to the attack information activity. The fires warfighting function enables commanders to target threat C2 systems. This includes the delivery of fires—surface to surface, air to surface, electromagnetic attack, offensive cyberspace operations, and offensive space operations—against threat C2 and information warfare targets. The movement and maneuver warfighting function contributes through the movement and position of forces to destroy or capture threat C2 nodes and capabilities. (See Chapter 7 for a detailed discussion of the attack information activity.)

WARFIGHTING FUNCTION CONTRIBUTIONS

2-24. Information activities organize various tasks and capabilities from the six warfighting functions to help leaders visualize and describe how to create and exploit information advantages. A *warfighting function* is a group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives (ADP 3-0). The warfighting functions are C2, movement and maneuver, intelligence, fires, sustainment, and protection. (Paragraphs 2-25 through 2-36 summarize how each warfighting function contributes to achieving information advantages.)

COMMAND AND CONTROL

The C2 warfighting function assists commanders in integrating the other warfighting functions to achieve objectives and accomplish the mission.

2-25. The C2 warfighting function is the related tasks and a system that enable commanders to exercise authority and direction to accomplish missions. Tasks include command forces, control operations, drive the operations process, and establish the C2 system. The C2 system consists of the people, processes, networks, and command posts (CPs) that support the commander in the exercise of C2.

2-26. The C2 warfighting function significantly contributes to the enable information activity. The entire C2 system is designed to support commanders in their abilities to understand, visualize, describe, direct, lead, and assess faster and more effectively than their opponents. Commanders organize their C2 system to facilitate their decision making, to include organizing the staff into CPs and establishing a battle rhythm to manage their activities. Commanders, supported by their staffs, conduct the operations process (plan, prepare, execute, and assess) and integrating processes to help them exercise C2 throughout the conduct of operations. This processes also aids in integrating capabilities and synchronizing the information activities into the concept of operations and individual schemes of support (intelligence, information collection, maneuver, fires, protection, sustainment, and command and signal). The network portions of the C2 system enable commanders to communicate with higher, adjacent, supporting, and subordinate commands to control all aspects of operations. The network provides the backbone to exchange data and populate and share the common operational picture across the force. (Refer to ADP 6-0 for more information on the C2 warfighting function.)

INTELLIGENCE

The purpose of the intelligence warfighting function is to improve understanding that enhances decision making.

2-27. The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the OE. The intelligence warfighting function synchronizes information collection with primary tactical tasks that support reconnaissance, surveillance, security, and intelligence operations. Intelligence is driven by commanders, and it involves analyzing information from all sources and conducting operations to develop the situation. Army forces execute intelligence, surveillance, and reconnaissance (ISR) through the operations and intelligence processes, with an emphasis on intelligence analysis and information collection.

2-28. The intelligence warfighting function contributes to the integration of all the information activities by providing relevant information and intelligence to decision makers. It directly contributes to developing situational understanding and informs decision making. The intelligence warfighting function contributes to understanding the human, information, and physical dimensions of an OE, to include identifying relevant actors, their relationships, and patterns of thinking. Continuous IPOE helps commanders understand threat information networks and information systems; activities and methods the threat employs to impact friendly decision making, networks, and C2; and ways information may impact a threat's own decision making and drivers of behavior. The intelligence warfighting function supports targeting and helps determine targets for influence and attack. (Refer to ADP 2-0 for more information on intelligence and the intelligence warfighting function.)

MOVEMENT AND MANEUVER

The purpose of the movement and maneuver warfighting function is to gain positions of relative advantage over a threat through direct fire and close combat.

2-29. The movement and maneuver warfighting function is the related tasks and systems that move and employ forces to achieve a position of relative advantage in respect to the enemy. Maneuver directly gains or exploits positions of relative advantage. Commanders use maneuver for massing effects to achieve surprise, shock, and momentum. The movement and maneuver warfighting function directly contributes to the protect, influence, and attack information activities.

2-30. Movement and maneuver creates information advantages by placing units in positions that communicate an explicit or implicit threat to the enemy. Through reconnaissance and security, maneuver forces gain information on the enemy and terrain facilitating friendly decision making. They conduct security operations to protect friendly information and C2 nodes. Commanders also maneuver forces to secure areas to put network transport assets in place.

2-31. The movement and maneuver of forces has inherent informational aspects that create effects and must be accounted for during planning and execution. These include signaling intent, demonstrating capability, and driving tempo to cause confusion and disorder within the enemy system. The movement and maneuver warfighting function also contributes to information advantage through close combat that changes facts on the ground. Maneuver forces destroy enemy forces, to include their C2 systems and infrastructure, seize key terrain, and control physical areas. The moving and positioning of forces as part of deception contributes to confusing and influencing threat decision makers. (Refer to ADP 3-90 for more information on the movement and maneuver warfighting function.)

FIRES

2-32. The fires warfighting function is the related tasks and systems that create and converge effects in all domains against the threat to enable operations across the range of military operations. These tasks and systems create lethal and nonlethal effects delivered from Army, joint, and multinational forces. The fires warfighting function contributes to the enable, protect, influence, and attack information activities.

The purpose of the fires warfighting function is to create and converge effects in all domains.

2-33. The fires warfighting function contributes to enabling the exercise of C2 through the targeting process. The delivery of fires contributes to protecting data and information, affecting threat C2 targets, and influencing target audiences. Through the targeting process, commanders identify, select, and prioritize targets and match the appropriate capability (or delivery platform) to targets to create desired effects. This includes identifying and attacking enemy C2 nodes, information systems, radars, ground control stations, and sensors to affect the enemy's decision cycle. Capabilities used to attack these targets range from cannons, rockets, and missiles to offensive cyberspace operations, electromagnetic attack, and offensive space operations. (Refer to ADP 3-19 for more information on the fires warfighting function.)

SUSTAINMENT

2-34. The sustainment warfighting function is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. Sustainment contributes to all information activities by ensuring the friendly force is healthy, manned, equipped, maintained, and supplied. Sustainment activities also contribute to the influence information activity. Providing sustainment to relevant actors can reinforce or change their behavior. The position of sustainment forces and their activities can contribute to both deception and the communication of a will to fight. (Refer to ADP 4-0 for more information on the sustainment warfighting function.)

The purpose of the sustainment warfighting function is to ensure freedom of action, extend operational reach, and prolong endurance.

PROTECTION

2-35. The protection warfighting function is the related tasks, systems, and methods that prevent or mitigate detection, threat effects, and hazards to preserve combat power and enable freedom of action. Protection encompasses the collective actions and measures required to preserve the potential of a force to be applied at the appropriate time and place. The protection warfighting function contributes to the protect information activities.

The purpose of the protection warfighting function is to preserve the force.

2-36. Protecting friendly data and information involves active and passive methods. Standard methods of protecting friendly information include signature management and OPSEC. Additionally, highly visible defensive measures are used to communicate messages of resolve to threats, while other less visible defensive

measures are used to conceal, reduce, or eliminate friendly critical vulnerabilities. Survivability operations harden C2 facilities and information infrastructure and improve fighting positions, which protects combat power and preserves options for the commander. Physical security procedures help safeguard facilities and the information in them. Department of Defense Information Network (known as DODIN) operations, defensive cyberspace operations, and electromagnetic protection help protect the friendly network. OPSEC—a responsibility of all forces—helps to safeguard information and friendly intentions from threats, which in turn preserves options for the commander. (Refer to ADP 3-37 for more information on the protection warfighting function.)

INFORMATION ADVANTAGES ACROSS STRATEGIC CONTEXTS

2-37. 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:

- Competition below armed conflict.
- Crisis.
- Armed conflict.

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 JP 1, Volume 1 for doctrine on the joint competition continuum. Refer to FM 3-0 for more information on Army operations within the strategic contexts.)

COMPETITION BELOW ARMED CONFLICT

2-38. 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.

2-39. 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—

Threats often employ information warfare capabilities to disrupt infrastructure, collect information, and interfere with commercial and government processes in ways that are not intended to cause the United States and its allies to respond with force.

- 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.

2-40. 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.

2-41. 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.

2-42. 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.

CRISIS

2-43. A *crisis* is an emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives (JP 3-0). A crisis may result from adversary actions, indicators of imminent action, or natural or human disasters. Success during a crisis is a return to a state of competition in which the United States, its allies, and its partners are in positions of increased advantage relative to the adversary. Should deterrence fail, Army forces are better positioned to defeat enemy forces during conflict.

2-44. During a crisis involving natural or human disasters, a rapid response is typically necessary. Such events frequently cause communications systems and networks to break down, disrupting the flow of information and potentially allowing a situation to worsen. Army communications capabilities can help prevent mass movements of people and unrest by disseminating information and influential messages. By providing relevant information about relief aid and the situation, Army forces help maintain calm and patience among affected populations. In addition, when working with local authorities to mitigate the effects of the event and alleviate suffering, Army forces can help bolster the legitimacy of and support for the indigenous government and its organizations.

2-45. During a crisis involving an adversary, opponents are not yet using lethal force as the primary means for achieving their objectives, but the situation potentially requires a rapid response by forces prepared to fight to deter further aggression. When directed, the Army provides a joint force commander with forces to help deter further provocation and sufficient combat power to maintain or reestablish conventional deterrence. The introduction of significant land forces demonstrates the will to impose costs, provides options to joint force and national leaders, and signals a high level of national commitment. As a crisis develops, the responsible joint force commander continues to employ capabilities from all Services to gain and maintain information advantages against the threat. Examples include—

- Extending communications capabilities to friendly forces within an operational area.
- Increasing or rapidly building technical, human, and procedural interoperability with allied and coalition partners.
- Increasing ISR across all domains.
- Executing MISO programs to complicate the decision making of threat leaders and reinforce desirable narratives with target audiences.
- Conducting public affairs and key leader engagements to promulgate information to U.S. domestic and international audiences in support of a friendly narrative, emphasizing the legitimacy of friendly goals and actions.
- Employing defensive cyberspace capabilities to increase protection of critical friendly systems.

- Employing offensive cyberspace, electromagnetic warfare, and offensive space operations to disrupt threat ISR, and communications.
- Planning and executing deception activities to mislead adversary decision makers and to set conditions for success should a crisis result in armed conflict.

2-46. OPSEC is vital to the success of operations during a crisis. Army units deploying to, or operating within, a joint operations area exercise strict OPSEC to protect friendly information and networks against cyberspace attacks. They do this by limiting or restricting the use of personal electronic devices, minimizing electromagnetic emissions, and limiting other communications to the greatest possible extent.

ARMED CONFLICT

2-47. The employment of lethal force is the defining characteristic of armed conflict, and it is the primary function of the Army. Lethality's immediate effect is in the physical dimension—reducing the enemy's capability and capacity to fight. Lethality extends into information and human dimensions where it influences enemy behavior, decision making, and will to fight. The vignette below illustrates how U.S. forces created and exploited information advantages in the 1991 Gulf War.

Information Advantage during Large-Scale Combat

Leaders at all echelons placed major emphasis on creating and exploiting information advantages during OPERATION DESERT SHIELD and OPERATION DESERT STORM. Commanders integrated operations security, military deception, tactical deception, military information support operations (formerly called psychological operations), and electromagnetic warfare efforts to set conditions for successful large-scale ground combat.

During planning, senior leaders identified Iraqi command and control (C2) as a critical vulnerability, that if degraded, would significantly enhance friendly success. As such, Army forces targeted Iraq national-level C2 throughout the campaign. Simultaneously, coalition electromagnetic warfare and interdiction selectively blinded enemy reconnaissance and surveillance, protecting friendly force movements and operations from enemy detection. Deception operations continued to reinforce erroneous enemy perceptions of coalition intentions. Electromagnetic warfare and precision air strikes against operational and tactical C2 targets disorganized and isolated Iraqi forces. Simultaneously, Iraqi ground forces were targeted with messaging to reduce their morale and encourage surrender. When the ground attack commenced, Iraqi forces were scattered with numerous formations unable to coordinate their efforts. Successfully denying Iraqi forces the ability to collect information and to exercise C2 created significant advantages for coalition forces. These advantages reduced friendly casualties and significantly reduced the time required to achieve coalition objectives.

2-48. During armed conflict, Army forces continue to develop situational understanding, protect friendly information and data, and inform audiences while attacking the enemy's ability to exercise C2. Army forces use all military capabilities, including physical destruction, to gain and exploit information advantages. Army forces seek to—

- Affect (degrade, deny, disrupt, corrupt, and destroy) the ability of the enemy to exercise C2.
- Defend, counter, and mitigate the enemy's efforts to affect friendly C2 capabilities.
- Amplify the psychological effects of a destructive or disruptive force.
- Confuse, manipulate, or deceive enemy understanding and decision making.
- Communicate the intent of Army operations and activities to maintain legitimacy.

INFORMATION ACTIVITIES AND THE TENETS OF OPERATIONS

2-49. The tenets of operations are desirable attributes built into all plans and operations, and they directly relate to how Army forces should employ multidomain operations. Commanders use the tenets of operations to inform and assess courses of action throughout the operations process. The degree to which an operation exhibits the tenets provides insight into the probability for success. The tenets of operations are—

- Agility.
- Convergence.
- Endurance.
- Depth.

Paragraphs 2-50 through 2-60 highlight how the tenets apply to planning, preparing, executing, and assessing information activities in support of the commander's intent and concept of operations. (Refer to FM 3-0 for the tenets of operations.)

AGILITY

2-50. Agility is the ability to move forces and adjust their dispositions and activities more rapidly than the enemy. Agility requires shared understanding, sound judgement, and rapid decision making often gained through the creation and exploitation of information advantages. Agility helps leaders influence tempo. *Tempo* is the relative speed and rhythm of military operations over time with respect to the enemy (ADP 3-0). It implies the ability to understand, decide, act, assess, and adapt more effectively than the enemy.

2-51. Information activities contribute to agility and tempo. The enable and protect information activities increase the effectiveness of the friendly decision cycle as shown in Figure 2-3. The influence and attack information activities decrease the effectiveness of the threat's decision cycle. The inform information activity can increase the effectiveness of the friendly decision cycle while decreasing the effectiveness of the threat's decision cycle. The combined effects of enhancing the friendly decision cycle while degrading the threat's create a significant advantage for Army forces.

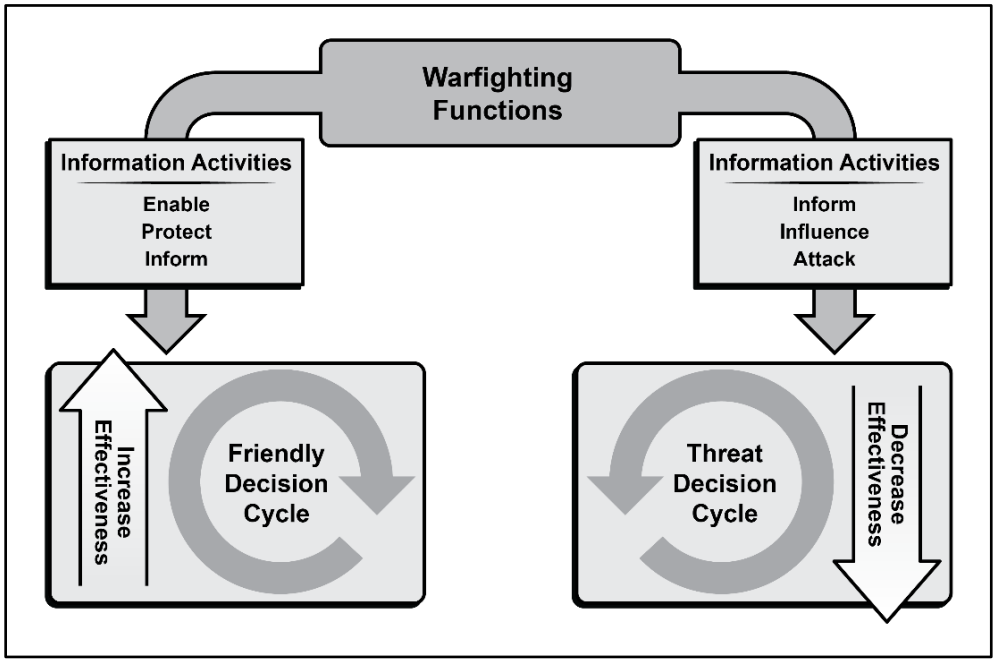


Figure 2-3. Information activities contributions to agility

CONVERGENCE

2-52. Peer threats employ adaptable and durable capabilities and formations over large geographic areas and multiple domains. They cannot be easily defeated in a single, decisive effort. Success requires Army forces to sustain attacks against multiple decisive points over time through convergence. Convergence is an outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area. Its utility derives from understanding the interdependent relationships among capabilities from different domains and combining those capabilities in surprising, effective tactics that accrue advantages over time. Convergence occurs when a higher echelon (normally corps and above) and its subordinate echelons create effects from and in multiple domains in ways that defeat or disrupt threat forces long enough for friendly forces to effectively exploit.

2-53. Convergence requires the integration of relevant Army and joint capabilities and the synchronization of actions at multiple decisive points. Commanders integrate Army capabilities (communications, information collection, fires, electromagnetic warfare, and MISO) into subordinate formations by task organizing forces, establishing support relationships, prioritizing efforts, and delegating execution authorities. For joint informational capabilities, Army commanders generally coordinate for specific informational effects. This includes requesting effects from cyberspace operations, space operations, MISO, fires, maneuver, and special technical operations. The effective integration of joint capabilities into Army operations requires an understanding of multiple joint processes, especially the joint targeting process. (Refer to JP 3-60 for the targeting process.)

2-54. To achieve convergence, Army commanders synchronize information activities into the concept of operations. Based on the commander's intent, operational approach, and planning guidance, planners synchronize information activities and associated tasks within the schemes of intelligence, information collection, maneuver, fires, protection, sustainment, and command and signal. Synchronizing information activities into a concept of operations enables a combined arms approach to operations necessary to achieve convergence. (See Chapter 8 for a more detailed discussion of integrating and synchronizing information activities.)

ENDURANCE

2-55. Endurance enhances the ability to project combat power and extends operational reach. Endurance is the ability to persevere over time throughout the depth of an OE. Endurance is about resilience and preserving combat power while continuing operations for as long as necessary to achieve the desired outcome. Endurance stems from the ability to organize, protect, and sustain a force regardless of the distance from its support area and the austerity of the environment.

2-56. Information activities and their related tasks contribute to endurance. Robust and resilient networks help to maintain continuous communications across echelons. Securing and obscuring friendly data and information helps prevent threat collection and protects the force. Proactively informing internal and external audiences throughout the duration of a campaign helps to preserve will, friendly morale, and human resiliency. Influencing populations and other foreign relevant actors to support friendly objectives over time contributes to endurance. Degrading threat information warfare capabilities helps to preserve friendly combat power throughout the breadth and depth of an operational area.

DEPTH

2-57. *Depth* is the extension of operations in time, space, or purpose to achieve definitive results (ADP 3-0). While the focus of endurance is on friendly combat power, the focus of depth is on enemy locations and dispositions across all domains. Commanders achieve depth by understanding the strengths and vulnerabilities of the enemy's echeloned capabilities, then attacking them throughout their dispositions in simultaneous and sequential fashion. Although simultaneous attacks through all domains in depth are not possible in every situation, leaders seek to expand their advantages and limit enemy opportunities for sanctuary and regeneration. Leaders describe the depth they can achieve in terms of operational reach.

2-58. *Operational reach* is the distance and duration across which a force can successfully employ military capabilities (JP 3-0). Staffs assess operational reach based on available sustainment, the range of capabilities

and formations, and courses of action compared with the intelligence estimates of enemy capabilities and courses of action. This analysis helps the commander understand the limits on friendly operations, risks inherent in the mission, and likely points in time and space for transitions.

2-59. Information activities contribute to depth. Army signal forces add depth by maintaining communications infrastructures throughout an area of responsibility and establishing networks in joint operations areas. These networks facilitate world-wide communications of both joint and Army forces. The joint force land component command creates depth by facilitating access to joint and Army capabilities, especially space, cyberspace, and electromagnetic warfare, to degrade enemy networks and systems in the extended deep area. Corps and division forces employ fires into deep areas to degrade enemy C2 and disrupt communications, to include communications between sensors and shooters. Inform information activities provide depth in friendly morale and will, public willingness to support operations, and reassurance of commitment to allies and partners.

2-60. Leaders enhance the depth of their operations by orchestrating effects in one dimension to amplify effects in the others. For example, a commander might decide to destroy an elite enemy formation first because it undermines the confidence of the enemy's other units. Commanders exploit this destruction through information activities to reduce the will of other enemy forces to fight.

PRINCIPLES OF INFORMATION ADVANTAGE

> *A* principle *is a comprehensive and fundamental rule or an assumption of central importance that guides how an organization approaches and thinks about the conduct of operations.*
>
> ADP 1-01

2-61. Gaining and exploiting an information advantage involves four principles. These principles provide a starting point for thinking about the use of information and the employment of capabilities to create and exploit information advantages. The principles of information advantage include the following:

- Offensively oriented.
- Combined arms.
- Commander driven.
- Soldier enabled.

OFFENSIVELY ORIENTED

2-62. Offensively oriented suggests that offensive action, or maintaining the initiative, is the most effective and decisive way to achieve objectives. Any information advantage not sought or defended is potentially ceded to the threat. As such, Army leaders take the initiative to create, protect, and exploit information advantages in all domains.

> The force that anticipates better, thinks more clearly, decides and acts more quickly, and adapts more rapidly, stands the greatest chance to seize, retain, and exploit the initiative over an opponent.

2-63. No matter the echelon, the force that retains the initiative through offensive action forces its opponent to react. While it is necessary to defend or protect, Army leaders maintain an offensive mindset and anticipate events in pursuit of various information advantages throughout the conduct of operations. They aggressively collect and use information to understand, decide, and act while actively denying the threat from doing the same. In addition to passive measures to protect data and information, Army forces target and attack threat capabilities to hinder the threat's ability to collect and communicate information about friendly forces. Army leaders proactively release accurate and timely information to various audiences as opposed to just reacting to threat propaganda.

COMBINED ARMS

2-64. The combined arms approach to operations is foundational to creating and exploiting information advantages. *Combined arms* is the synchronized and simultaneous application of arms to achieve an effect greater than if each element was used separately or sequentially (ADP 3-0). Leaders combine available

organic, joint, and multinational capabilities in complementary and reinforcing ways to create and exploit information advantages in the same way they do with human and physical advantages. For example, Army forces precede or follow a massed artillery strike with surrender appeals through MISO.

2-65. All military capabilities can be employed for information advantage. For example, an infantry battalion can deceive an enemy by conducting a feint. A field artillery brigade can destroy enemy radars, communications, and CPs. The commitment of Army sustainment units to an area during competition can influence an adversary's decision making. Additionally, some Army, joint, and multinational units are specifically designed for the use, protection, denial, or manipulation of information. Signal, cyberspace, electromagnetic warfare, psychological operations, space, civil affairs, and public affairs units are examples. Commanders and staffs do not restrict their thinking to a select few specialized units or capabilities but consider all available capabilities in a combined arms approach to enable C2; protect data, information, and networks; and inform audiences, influence relevant actors, and attack threat C2. (Refer to FM 3-0 for more information about combined arms.)

COMMANDER DRIVEN

2-66. Commanders at every level require and use information to seize, retain, and exploit the initiative and achieve decisive results. Therefore, commanders must understand information, integrating it in operations as carefully as fires, maneuver, protection, and sustainment. Commanders think of information as a resource to achieve situational understanding, a tool to induce ambiguity and uncertainty in the threat, and the primary means to direct Army forces. Commanders direct the use of information and capabilities to penetrate threat decision-making processes, exploit information dependencies, achieve surprise, and disrupt the threat from within.

2-67. The decision to conceal or reveal information is a constant push and pull between advantages and disadvantages that inform risk. Throughout operations, commanders weigh the risks and benefits to revealing and concealing information. For example, revealing information about the friendly force as part of deterrence can also provide valuable intelligence to a threat force.

2-68. Commanders ensure information activities are integrated into the concept of operations through the operations process. This requires commanders to understand, visualize, and describe how they intend to use information and capabilities to create and exploit information advantages. Commanders direct information activities through orders while leading and assessing progress throughout operations. Based on changes in a situation that reveal opportunities and threats, commanders adjust information activities and related tasks as required.

SOLDIER ENABLED

2-69. Informational considerations—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—are not just for commanders, planners, and specialists. All Soldiers must protect information, help overcome their unit's disadvantages, and create and exploit information advantages. Developing and maintaining data literacy—the ability to derive meaningful information from data—is an important Soldier skill. Considerations such as OPSEC, physical security, noise and light discipline, and electromagnetic emission control apply to every individual Soldier and are critical to ensuring information advantage.

2-70. Every Soldier consumes, communicates, and relies on information to accomplish the mission. As representatives of the Army and the United States, Soldiers understand that their presence, posture, and actions always communicate a message that is open to interpretation. High visibility offers great opportunity as well as potential risk. Effective Soldiers at all levels understand the impact that their actions and messages communicate. This requires all Soldiers to understand the broader purpose of operations as communicated to them from commanders and other leaders. It also requires practicing OPSEC and disciplined communication through all forms of media—including personal media accounts—both in operations and while at home station. (See Chapter 8 for a more detailed discussion on digital readiness training.)

This page intentionally left blank.

Chapter 3
Enable

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

Sun Tzu

Chapter 3 begins with an overview of the enable information activity. A description of the tasks that facilitate situational understanding, decision making, and communications follows. The chapter concludes with considerations that enhance friendly command and control (C2).

ENABLE OVERVIEW

3-1. 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.

3-2. 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.

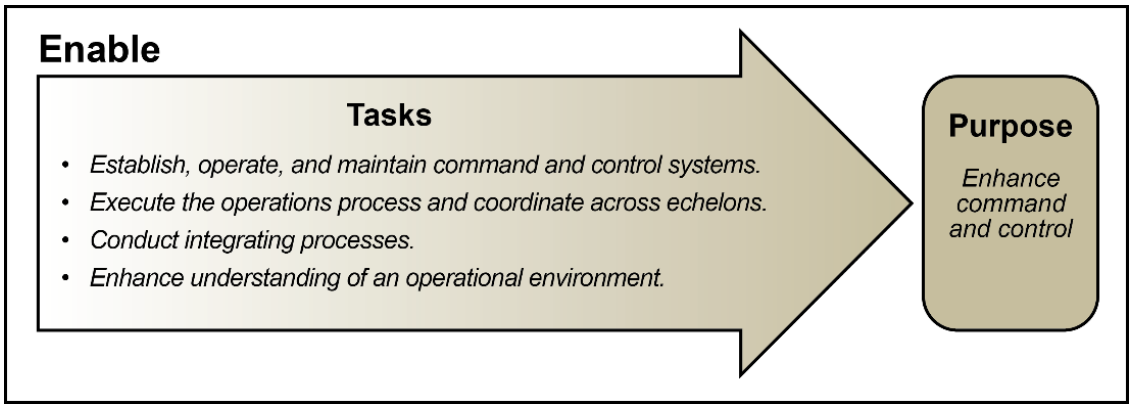


Figure 3-1. Tasks and purpose of the enable information activity

ESTABLISH, OPERATE, AND MAINTAIN COMMAND AND CONTROL SYSTEMS

3-3. *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). Figure 3-2 illustrates the components of a C2 system.

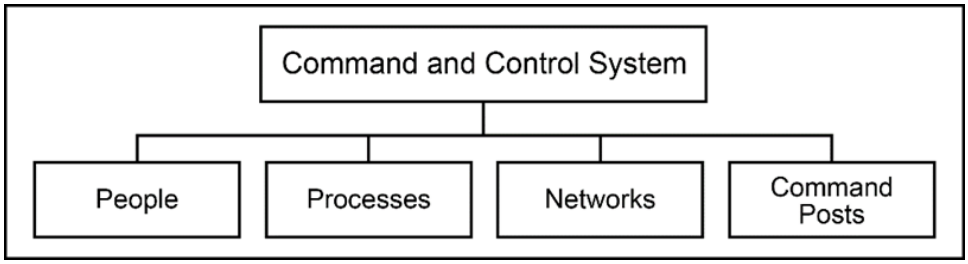


Figure 3-2. The command and control system

3-4. A C2 system has many purposes, all of them information centric. Commanders organize their personnel, processes, networks, and command posts (CPs) to facilitate the exchange of information, inform their decision making, direct action, and control operations. (Refer to FM 6-0 for detailed doctrine on organizing and operating the C2 system.)

ORGANIZE PEOPLE

3-5. The most important component of the C2 system is its people—commanders, seconds in command, and staffs. Coordinating, special, and personal staff sections are the building blocks for organizing a headquarters for the conduct of operations. Staff sections support commanders in making and implementing decisions. They provide relevant information and analysis, make running estimates and recommendations, prepare plans and orders, assess operations, and assist in controlling operations. Commanders consider the following when organizing the staff for operations:

- Staff sections.
- CP cells.
- Augmentation.
- Working groups and boards.

Staff Sections

3-6. Staff sections consist of groupings of personnel with a common field of interest. Personnel, intelligence, and signal staff sections are examples. The unit's modified table of organization and equipment establishes the specialty or functional area and grade of each member of a staff section. Based on the situation, commanders may reorganize personnel within the staff to fit their C2 requirements. For example, a division or corps commander may decide to expand the G-39, information plans and operations staff section, by adding additional signal, cyberspace, electromagnetic warfare, and psychological operations personnel. (See Chapter 8 for staff responsibilities concerning information activities.)

Note. The G-39 staff section is a relatively new addition to division, corps, and some theater armies tables of organization and equipment. The G-39 staff section is led by a senior functional area 30 information operations officer who helps the commander, operations officer, and other staff members integrate information activities into the concept of operations.

Command Post Cells

3-7. During operations, staff sections are cross-functionally organized into CPs and CP cells. CP cells are groupings of personnel and equipment organized by warfighting function or by planning horizon. Functional cells group personnel and equipment by warfighting function (movement and maneuver, intelligence, fires, sustainment, and protection). There are multiple staff sections and elements of staff sections in each functional cell. For example, the movement and maneuver cell consists of operations, airspace control, aviation, information plans and operations, and cyberspace and electromagnetic activities staff sections.

3-8. Integrating cells group personnel and equipment by *planning horizons*—a point in time commanders use to focus the organization's planning efforts to shape future events (ADP 5-0). The three planning horizons are long-, mid-, and short-range. They are associated with the plans cell, future operations cell, and current operations integrating cell respectively. The plans cell develops operation plans and operation orders, to include branches and sequels to an operation. The future operations cell develops fragmentary orders and branches to the current operation order. The current operations integrating cell develops fragmentary orders and controls the execution of operations. Based on the commander's intent and planning guidance, the integrating cells synchronize activities (to include information activities) into the concept of operations to achieve objectives. (Refer to FM 6-0 for more information on CPs and CP cells.)

Augmentation

3-9. Many situations require augmentation to a unit's headquarters. Commanders anticipate and request augmentation requirements as early as possible. Ideally, theater armies develop and submit augmentation requirements when developing plans to support the joint force commander's requirements. Typically, augmentation focused on enhancing information activities includes, but is not limited to—

- Psychological operations units.
- Mobile public affairs detachments.
- Civil affairs planning teams.
- Cyberspace operations mission elements.
- Electromagnetic warfare elements.
- Army space support teams.
- Combat camera teams.
- Legal support teams.
- Linguists.
- Assessment teams.
- Multinational and interagency liaison officers.
- Digital liaison detachments.
- Individual augmentation.

Working Groups and Boards

3-10. Working groups and boards further cross-functionally organize a staff. Members of working groups and boards include the staff; the commander and staff; or the commander, subordinate commanders, staff, and others as necessary. Who attends depends on the focus. Working groups and boards present and exchange information, solve problems, coordinate action, provide recommendations, and make decisions.

3-11. The primary difference between working groups and boards is the level of authority granted to a board by the commander. A *working group* is a grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function (FM 6-0). Typical working groups include assessment, airspace control, civil-military operations, cyberspace and electromagnetic activities, information collection, knowledge management, protection, sustainment, and targeting working groups. A *board* is a grouping of predetermined staff representatives with delegated decision authority for a particular purpose or function (FM 6-0). The commander or a senior leader chairs boards with members of the boards consisting of staff elements, subordinate commands, and other organization representatives as required. Typical boards found on the unit's battle rhythm include assessment, plans, sustainment, and targeting boards. (See FM 6-0 for examples of working groups and boards typically held in Army headquarters.)

ORGANIZE PROCESSES

3-12. Commanders use various processes to enhance C2. The operations process—plan, prepare, execute, and assess—is the overarching process for the exercise of C2 (see paragraphs 3-21 through 3-34 for details on the operations process). Within the operations process, commanders and staffs conduct several integrating processes (intelligence preparation of the operational environment [IPOE], information collection, targeting,

risk management, and knowledge management) to enhance C2 (see paragraphs 3-35 through 3-46 details on the integrating processes).

The unit's battle rhythm organizes the various processes and activities that occur within a headquarters, and with higher, lower, supporting, and supported headquarters.

3-13. The unit's battle rhythm synchronizes various processes, activities, and reports within the operations process. A *battle rhythm* is a deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations (FM 6-0). The battle rhythm synchronizes information inputs and outputs of meetings (to include briefings, working groups, and boards) into a logical order. These inputs establish information requirements, to include subordinate friendly reporting requirements. The outputs facilitate decision making, requests for support from higher headquarters, and coordination across echelons. An effective battle rhythm—

- Facilitates decision making.
- Facilitates interactions among the commander, staff, and subordinate commanders.
- Supports building and maintaining shared understanding throughout the headquarters.
- Establishes a routine for staff interaction, coordination, and integration.
- Establishes subordinate reporting requirements.

3-14. The chief of staff (COS) or executive officer oversees the unit's battle rhythm. The chief of staff or executive officer ensures activities are logically sequenced so that the output of one activity informs another activity's inputs. This is important within the headquarters and with higher echelon headquarters. The battle rhythm ensures that the staff and subordinate units provide information and recommendations pertinent to decisions and enhance coordination among echelons. (Refer to FM 6-0 for additional information on battle rhythm.)

ESTABLISH, OPERATE, AND MAINTAIN NETWORKS

3-15. Headquarters at all echelons rely on networks to collect, process, store, display, and disseminate information. Without a robust, resilient, and protected network, commanders cannot effectively exercise C2. Networks provide infrastructure for voice, data, and video connectivity to support operations. Networks enable commanders to communicate with higher, lower, adjacent, supporting, and supported commands.

3-16. The network serves as the backbone for populating and sharing the common operational picture (COP) across the entire force. With tactical radio systems able to pass digital information, networks extend as low as the individual Soldier across the battlefield. Commanders establish, organize, and maintain networks to maximize data and information flow and to minimize communications disruptions.

3-17. Planning for successful communications requires detailed planning by every staff section, not just the signal staff section. Communications planners must understand the commander's intent, understand the concept of operations, and have a clear picture of the overall communications architecture. Network and communications considerations include—

- Enemy situation and threats, to include threat information warfare capabilities.
- Communications capability requirements for all warfighting functions.
- Capabilities and limitations of all available end-user applications.
- Potential joint, interorganizational, and multinational communications requirements.
- Detailed line-of-sight analysis.
- Redundancy, to include establishing primary, alternate, contingency, and emergency (known as PACE) communications plans.
- The integration of all available signal assets.
- A method of deployment so assets are sequenced to coincide with the arrival of forces.
- Locations of all CP communications systems.
- The use of retransmission, digital network links, and node placement.
- Requirements for transferring, transmitting, and receiving audiovisual, visual, multimedia, and audio files.

- Electromagnetic spectrum deconfliction.
- Satellite communications requirements.
- Spectrum requirements for emitters, sensors, radars, or any other assets that rely on a frequency.
- Initial task organization and expected changes.
- Proper signal and communications security procedures.
- Cybersecurity activities.
- Communications rehearsals.
- Unified action partner network access.

(Refer to FM 6-02 for details on networks and signal support to operations. See Chapter 4 for more information on protecting data, information, and networks.)

ORGANIZE COMMAND POSTS

3-18. Effective C2 requires continuous, and often immediate, close coordination, synchronization, and information sharing across the staff. To promote this, commanders organize their staffs and other components of the C2 system into CPs to assist them in effectively conducting operations. A *command post* is a headquarters, or a portion there of, organized for the exercise of command and control (FM 6-0). Commanders organize their CPs flexibly to meet changing situations and requirements of different operations. They enhance C2 by organizing their CPs for effectiveness while balancing effectiveness considerations with survivability. In many cases, these considerations work against each other, and therefore neither can be optimized simultaneously.

3-19. Commanders arrange personnel, equipment, and facilities to facilitate coordination, exchange of information, and rapid decision making. A CP must effectively communicate with higher, subordinate, adjacent, supporting, and supported units and move as required. Commanders enhance C2 by arranging the CP to—

- Increase information flow between staff sections.
- Optimize user interface with communications systems.
- Locate information displays for ease of use.
- Integrate complementary information on maps and displays.
- Provide adequate workspace for the staff and commander.

3-20. CP survivability is vital to mission success. Survivability considerations make collaboration and coordination more difficult. Depending on the threat, CPs need to remain small and highly mobile—especially at lower echelons. CP survivability measures are closely related to the protect information activity because threats continuously seek to collect information about their composition and location. Many survivability methods focus on creating ambiguity or denying the threat that information. Considerations for CP survivability include dispersion, electromagnetic signature, redundancy, mobility, camouflage, obscuration, and concealment. (For more information on survivability, see FM 3-13.4.)

CONDUCT THE OPERATIONS PROCESS AND COORDINATE ACROSS ECHELONS

3-21. The Army's framework for exercising C2 is the *operations process*—the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0). Commanders use the operations process to drive the conceptual and detailed planning necessary to understand, visualize, and describe their OE and the operation's end state; make and articulate decisions; and direct, lead, and assess operations. An effective operations process depends upon the exchange of information and data. (Refer to ADP 5-0 for fundamentals of the operations process.)

3-22. The activities of the operations process are not discrete; they overlap and recur as circumstances demand. While planning may start an iteration of the operations process, planning does not stop with the production of an order. After the completion of the initial order, the commander and staff continuously revise the plan based on changing circumstances. Preparation for a specific mission begins early in planning and continues for some subordinate units during execution. Execution puts a plan into action and involves

adjusting the plan based on changes in the situation and the assessment of progress. Assessing is continuous and influences the other three activities.

3-23. Both the commander and staff have important roles within the operations process. The commander's role is to drive the operations process through the activities of understanding, visualizing, describing, directing, leading, and assessing operations as shown in Figure 3-3. The staff's role is to assist commanders with understanding situations, making and implementing decisions, controlling operations, and assessing progress. The staff assists commanders in coordinating with higher, subordinate, adjacent, supporting, and supported units.

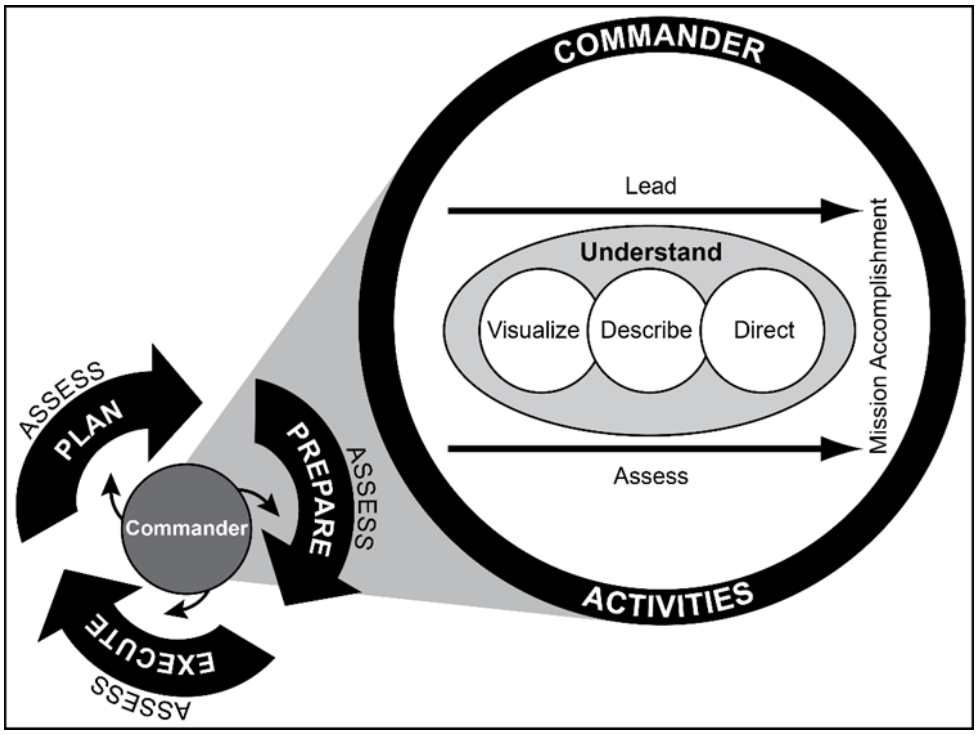


Figure 3-3. The operations process

3-24. A goal of the operations process is to understand the situation, make decisions, and act faster and more effectively than the enemy. A tempo advantageous to friendly forces puts pressure on the enemy. Throughout the operations process, making and communicating decisions faster than the enemy can react produces multiple dilemmas for the enemy to overcome. These decisions include assigning tasks; prioritizing, allocating, and organizing forces and resources; and selecting the critical times and places to act. Decision making during execution includes knowing how and when to adjust previous decisions. The speed and accuracy of a commander's actions to address a changing situation is a key contributor to agility and largely dependent upon the quality of information available.

3-25. How well the commander organizes the C2 system directly affects the efficiency with which the commander and staff conduct the operations process. The most important way that information enables the operations process and enhances C2 is by building and maintaining situational understanding and then by communicating that understanding across all echelons. Commanders enhance the operations process and coordinate across echelons in many ways, to include—

- Prioritizing information requirements.
- Maintaining running estimates.
- Creating, maintaining, and disseminating the COP.
- Establishing liaisons.

PRIORITIZE INFORMATION REQUIREMENTS

3-26. Information is pervasive in every OE. Essential to effective C2 is identifying what information is extraneous and what information is relevant to maintaining situational understanding and making effective decisions. *Relevant information* is all information of importance to the commander and staff in the exercise of command and control (ADP 6-0). Commanders, supported by their staffs, use relevant information to maintain their running estimates, to build shared understanding across the force, and to direct, coordinate, and synchronize the action of subordinate units.

3-27. Relevant information provides the basis for running estimates and for creating and maintaining the COP. This information facilitates situational understanding, decision making, and the ability to provide timely orders and guidance. Relevant information generally has the following characteristics:

- Accurate: it conveys the true situation.
- Timely: it is available in time to make decisions.
- Usable: it is portrayed in common, easily understood formats and displays.
- Complete: it provides all information necessary.
- Precise: it contains the necessary detail.
- Reliable: it is trustworthy and dependable.

Note. The intelligence warfighting function requires relevant information to be predictive as well as tailored.

Commanders use commander's critical information requirements to prioritize information collection and friendly reporting on relevant information they need to support their understanding and visualization and to make key decisions.

3-28. To focus the staff and subordinate units on collecting and providing relevant information, the commander establishes information requirements. This includes establishing commander's critical information requirements (CCIRs). A *commander's critical information requirement* is specific information identified by the commander as being essential to facilitate timely decision making (JP 3-0). Commanders designate an information requirement as a CCIR to focus the collection of information needed to make a decision. Always promulgated by a plan or order, commanders limit the number of CCIRs to focus the efforts of limited collection assets. A CCIR falls into one of two categories:

- Priority intelligence requirement (PIR).
- Friendly force information requirement (known as FFIR).

Note. Although not a CCIR, commanders also identify and prioritize the information they want protected as essential elements of friendly information (EEFIs).

3-29. PIRs help to focus intelligence collection. A *priority intelligence requirement* is an intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support (JP 2-0). PIRs identify the information about an enemy force and other aspects of an OE that a commander considers most important to the plan or decisions. Intelligence officers manage PIRs for commanders as part of the intelligence process. See paragraphs 3-37 and 3-38 for more information on PIRs.

3-30. Friendly force information requirements help to focus friendly reporting. A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0). Friendly force information requirements identify the information about the mission, troops and support available, and time available for friendly forces that the commander considers most important to the plan or decisions. In coordination with staffs, the operations officers manage friendly force information requirements for commanders. Friendly information includes the location, disposition, and status of friendly forces.

3-31. Additionally, commanders describe information they want protected as an EEFI. An *essential element of friendly information* is a critical aspect of a friendly operation that, if known by a threat would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection (ADP 6-0). Although EEFIs are not CCIRs, they have the same priority. EEFIs establish elements of information to protect rather than ones to collect. Their identification is the first step in the operations security (OPSEC) process and central to the protection of information. (See Chapter 4 for more information about the protect information activity.)

Note. Joint doctrine uses the term *critical information* vice *essential element of friendly information. Critical information* is specific facts about friendly intentions, capabilities, and activities needed by an enemy or adversary for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (JP 2-0).

MAINTAIN RUNNING ESTIMATES

3-32. Each staff section maintains relevant information concerning its specific area of expertise in its running estimate. 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 consist of information that assists commanders and staffs with understanding situations, assessing progress, and making decisions throughout an operation. Staffs share running estimates across echelons to promote understanding and coordination. Effective plans and successful execution hinge on current and accurate running estimates. When building and maintaining a running estimate, staff sections monitor current operations and continuously consider the following in context of the operation:

Running estimates consist of information that assists commanders and staffs with understanding situations, assessing progress, and making decisions throughout an operation.

- Facts.
- Assumptions.
- Analysis of the mission variables, to include informational considerations.
- Conclusions and recommendations.

(Refer to FM 5-0 for more information on running estimates.)

CREATE, MAINTAIN, AND DISSEMINATE THE COMMON OPERATIONAL PICTURE

3-33. The *common operational picture* is a display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (ADP 6-0). The COP helps commanders at all echelons achieve shared situational understanding and facilitates planning, preparation, executing, and assessing operations. The COP—

- Assists the commander in providing intent and issuing planning guidance.
- Helps the commander, staff, and subordinate leaders focus on relevant information.
- Enhances collaboration and thus allows more efficient planning, directing, and backbriefs.
- Promotes subordinate unit parallel planning.
- Allows for rapid decision making during execution.
- Reduces the risk of fratricide with enhanced situational understanding.
- Promotes better battle tracking and helps leaders measure, analyze, and report unit performance during operations.
- Supports the planning of branches and sequels to react to anticipated change.
- Enhances multinational interoperability and unity of effort.

ESTABLISH LIAISONS

3-34. *Liaison* is that contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action (FM 6-0). Mostly used for establishing and maintaining close communication, liaison continuously enables direct, physical communication between commands. Liaison enables C2 by facilitating—

Commanders use liaison during operations to help facilitate coordination between organizations, de-conflict efforts, and build shared understanding.

- Cooperation and understanding among commanders and staffs of different headquarters.
- Coordination on operational matters to achieve unity of effort.
- Synchronization of lethal and nonlethal effects across different domains.
- Understanding of implied or inferred coordination measures to achieve synchronized results.
- Technical, procedural, and human interoperability with multinational partners.

(Refer to FM 6-0 for more information on liaison.)

CONDUCT THE INTEGRATING PROCESSES

3-35. Within the operations process, commanders and staffs conduct several integrating processes to implement situational understanding, make decisions, and synchronize activities (to include information activities) into the concept of operations. An integrating process consists of a series of steps that incorporates multiple disciplines to achieve a specific end. Integrating processes begin in planning and continue during preparation and execution. Key integrating processes include—

- IPOE. (Refer to FM 2-0 for more on intelligence.)
- Information collection. (Refer to FM 3-55 for more on information collection.)
- Targeting. (Refer to FM 3-60 for more on targeting.)
- Risk management. (Refer to ATP 5-19 for more on risk management.)
- Knowledge management. (Refer to ATP 6-01.1 for more on knowledge management.)

CONDUCT INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

3-36. IPOE is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. This includes informational considerations pertaining to the enemy, terrain, weather, and civil considerations. Continuous holistic IPOE contributes to creating and exploiting information advantages by improving understanding of an OE. A holistic approach—

- Describes the totality of relevant aspects of an OE that may impact friendly, threat, and neutral forces.
- Accounts for all relevant domains that may impact friendly and threat operations.
- Identifies windows of opportunity to leverage friendly capabilities against threat forces.
- Allows commanders to leverage positions of relative advantage at a time and place most advantageous for mission success with the most accurate information available.

CONDUCT INFORMATION COLLECTION

3-37. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). An information collection capability is any human or automated sensor, asset, or processing, exploitation, and dissemination (known as PED) system directed to collect information that enables better decision making and expands understanding of an OE. Some collection efforts may be persistent or long term; others are mission specific according to specific information gaps.

Imperative of operations: See yourself, see the enemy, and understand the operational environment.

3-38. Information collection contributes to information advantages by aligning reconnaissance, surveillance, security, and intelligence assets to collect information on identified information gaps. It begins early in planning and continues throughout the operations process. Information collection consists of the following:

- Plan requirements and assess collection.
- Task and direct information collection.
- Execute collection.

CONDUCT TARGETING

3-39. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). It is an integral part of the operations process that organizes the efforts of the commander and staff to integrate and synchronize fires in operations. Targeting seeks to create specific desired effects through lethal and nonlethal actions. There are four functions associated with the Army's targeting process. They are—

- Decide.
- Detect.
- Deliver.
- Assess.

3-40. This methodology (also known as D3A) facilitates engagement of the right target, at the right time, with the most appropriate assets to meet the commander's targeting guidance. It optimizes integration and synchronization of fires, intelligence, and C2. The targeting process contributes to information advantages by degrading threat C2 and intelligence, surveillance, and reconnaissance (ISR) through the delivery of fires. Offensive cyberspace operations, electromagnetic attack, and offensive space operations are forms of fires employed in combinations with surface-to-surface and air-to-surface fires in support of the scheme of maneuver. Some effects such as space and cyber can be limited in the time they can be effective, so commanders must closely synchronize these effects with other activities to achieve the overall targeting objectives.

3-41. The chief of staff or executive officer normally leads the targeting team. Fire support, G-2 or S-2, G-3 or S-3, and Air Force representatives form the team's core. Other coordinating and special staffs participate as required. For example, these representatives can come from cyber electromagnetic warfare, space operations, psychological operations, special technical operations, and staff judge advocate organizations.

3-42. The targeting process is cyclical. The unit's battle rhythm determines when the targeting team meets. Targeting begins in planning and continues throughout the operations process. The decide function occurs concurrently with planning. The detect function occurs during preparation and execution. The deliver function occurs primarily during execution, although some targets may be engaged while the command is planning or preparing for the overall operation. The assess function occurs throughout the operations process, but it is most intense during execution.

CONDUCT RISK MANAGEMENT

3-43. Risk—the exposure of someone or something valued to danger, harm, or loss—is inherent in all operations. Because risk is part of all military operations, it cannot be avoided. Identifying, mitigating, and accepting risk is a function of command and a key consideration during planning and execution. *Risk management* is the process to identify, assess, and mitigate risks and make decisions that balance risk cost with mission benefits (JP 3-0). Commanders and staffs use risk management throughout the operations process to identify and mitigate risks associated with hazards that have the potential to cause friendly and civilian casualties, damage or destroy equipment, or otherwise impact mission effectiveness. Like targeting, risk management begins in planning and continues through preparation and execution. Risk management consists of the following steps:

- Identify hazards.
- Assess hazards.
- Develop controls and make risk decisions.

- Implement controls.
- Supervise and evaluate.

3-44. All staff elements incorporate risk management into their running estimates and provide recommendations to mitigate risk within their areas of expertise. This includes identifying and mitigating risk to friendly data, information, and communications.

CONDUCT KNOWLEDGE MANAGEMENT

3-45. Knowledge management enables better decision making. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). The goal of knowledge management is to get the right information to the right person on time to facilitate effective decision making. The purpose of knowledge management is to align people, processes, and tools within an organizational structure to achieve shared understanding. This alignment improves collaboration and interaction between leaders and subordinates. Unit knowledge managers assist commanders and staffs in developing knowledge management plans and implementing knowledge management techniques throughout the headquarters. Sound knowledge management practices include—

- Collaboration among personnel at different locations.
- Rapid knowledge transfer between units and individuals.

3-46. Information management supports, underpins, and enables knowledge management. *Information management* is the science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products (ADP 6-0). Information management is a technical discipline conducted by signal Soldiers that involves the planning, storing, and controlling of data and information in support of the commander and staff. (Refer to FM 6-02 for more discussion on information management.)

ENHANCE UNDERSTANDING OF AN OPERATIONAL ENVIRONMENT

> *When I took a decision, or adopted an alternative, it was after studying every relevant—and many an irrelevant—factor. Geography, tribal structure, religion, social customs, language, appetites, standards—all were at my finger-ends. The enemy I know almost like my own side. I risked myself among them a hundred times to* learn.
>
> T.E. Lawrence

3-47. 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.
- Identify likely behavior of relevant actors.

ANALYZE THE OPERATIONAL AND MISSION VARIABLES

3-48. The operational and mission variables are tools to assist commanders and staffs in developing situational understanding. 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. (Refer to FM 5-0 for details on the operational variables.)

3-49. 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. The

mission variables—METT-TC (I)—are mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations.

3-50. 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.

IDENTIFY AND DESCRIBE RELEVANT ACTORS

3-51. 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. This analysis makes it possible for Army forces to identify who or what is a relevant actor based on the mission. The staff conducts this analysis during planning and continues to refine knowledge of relevant actors throughout the operations process.

Relevant Human Actors

3-52. 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.

3-53. 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. This includes identifying what drives the Army and other relevant actor behavior, what narratives affect actors' use for their worldview, and how relevant actors will likely interpret the intent of friendly activities. Commanders and staffs need to understand how relevant actors use information to communicate, so this description should encompass a discussion of each relevant actors' preferred means, context, and patterns of communications.

Relevant Automated Systems

3-54. 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 analysist can.

3-55. 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. Understanding relevant automated systems includes analysis that determines and describes the programming and logic that then lead to automated system decision making and behavior.

3-56. Second, staffs describe what effects informational and physical aspects of the environment have on each automated system. This includes describing the decision-making processes of the automated systems in question. It also involves identifying the programming that allows the systems to detect, react to, and learn from the sensory inputs in their environments; act upon that detection based upon programming and experience; and adjust their sensing and actions based upon feedback received. This also involves

determining the means, context, and patterns of automated system communications and how automated systems receive input and communicate decisions and actions, thereby providing an understanding of the range of potential behaviors.

IDENTIFY BEHAVIORS OF RELEVANT ACTORS

3-57. 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. The staff uses its specific expertise to—

- 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.

3-58. Identifying the behavior of relevant actors provides the commander and staff with the information necessary to determine which relevant actor actions in a given time and space can help or hinder friendly operations. This determination enables the staff to plan for activities that affect drivers of relevant actor behavior in support of achieving objectives.

3-59. Once the staff identifies relevant actors and their behaviors, the commander selects the appropriate means to affect behavior. While the staff can determine current behaviors, the staff must anticipate unexpected second- and third-order effects and plan for how to assess the effectiveness of friendly actions. The staff continually assesses the behaviors of relevant actors relative to friendly forces activities to ensure activities achieve the desired results in relevant actors, and if not, make appropriate recommendations to the commander on other methods to achieve the desired effects.

CONSIDERATIONS FOR ENHANCING COMMAND AND CONTROL

In war obscurity and confusion are normal. Late, exaggerated or misleading information, surprise situations, and counterorders are to be expected.

Infantry in Battle

3-60. Army doctrine provides numerous considerations to enhance C2 depending on the topic. For example, ADP 6-0 provides considerations for effective command and considerations for effective control. ADP 5-0 provides the principles of the operations process and considerations for effectively planning, preparing, executing, and assessing operations. FM 6-02 provides fundamental principles of signal support. In addition to the considerations above, Army commanders and staffs weigh several methods to enhance C2, to include—

- Applying the principles of mission command.
- Ensuring digital readiness.
- Developing and maintaining digital literacy.

MISSION COMMAND

3-61. Applying the principles of mission command significantly enhances friendly C2. *Mission command* is the Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation (ADP 6-0). Mission command is necessary because operations are inherently chaotic and uncertain. No plan can account for every possibility, and most plans must change rapidly during execution to account for changes in the situation. No single person is ever sufficiently informed to make every important decision, nor can a single person keep up with the number of decisions that need to be made during combat. Subordinate leaders often have a better understanding of what is happening during

a battle than higher leaders do. Thus, subordinate leaders are more likely to respond effectively to threats and fleeting opportunities if allowed to make decisions and act.

3-62. Mission command facilitates subordinate ingenuity, innovation, and decision making to achieve the commander's intent when conditions change or current orders are no longer relevant. Subordinate decision making and decentralized execution appropriate to the situation help manage uncertainty and enable necessary tempo at each echelon during operations. Successful mission command is enabled by the principles of—

- Competence.
- Mutual trust.
- Shared understanding.
- Commander's intent.
- Mission orders.
- Disciplined initiative.
- Risk acceptance.

3-63. Mission command requires competent forces and an environment of mutual trust and shared understanding among commanders, staffs, and subordinates. It requires effective teams and a command climate in which subordinates are required to seize opportunities and counter threats within the commander's intent. Commanders issue mission orders that focus on the purpose of an operation and essential coordination measures rather than on the details of how to perform assigned tasks. This issuance gives subordinates the latitude to accomplish those tasks in a manner that best fits the situation. This minimizes the number of decisions a single commander makes and allows subordinates the greatest possible freedom of action to accomplish tasks. (Refer to ADP 6-0 for a detailed discussion of the principles of mission command.)

DIGITAL READINESS

Digital readiness is part of a unit's overall readiness. It includes the ability of individuals, teams, crews, and formations to effectively operate information systems to enable command and control.

3-64. Digital readiness is the ability of an individual and organization to maintain and operate information systems. Information systems help leaders process, store, and disseminate information concerning a warfighting function or functional area. Within a CP, there are multiple types of information systems that support C2, intelligence, fires, maneuver, air space control, air and missile defense, personnel management, transportation, and sustainment. When merged into a single integrated network, these information systems significantly enhance situational understanding, communications, and the exercise of C2. (Refer to FM 6-0 for the types of information systems commonly found in CPs by echelon.)

3-65. Digital readiness involves ensuring that unit information systems are manned with trained personnel, including the capability to maintain the network and information systems to ensure they are fully mission capable. It includes leader development to ensure that officers and noncommissioned officers understand the capabilities, limitations, and risks of an information system. Risks may stem from data compromise, accuracy or latency of data, and emission signatures. Understanding information systems' capabilities, limitations, and risk, and understanding ways to fully integrate these capabilities significantly contributes to commanders' effectively exercising C2.

3-66. Commanders direct individual and collective training to maintain digital proficiency. Individual training focuses on Soldiers and leaders being fully capable of operating their assigned information systems. Collective training involves developing teams, crews, and staff sections to integrate their information systems into the COP and with higher, lower, supported, and supporting units. Digital and signal master gunners—personnel trained to operate, maintain, integrate, and train others on information systems and the network—assist leaders in ensuring digital readiness. A digitally ready force is resilient to failures and attacks on its information systems and can continue to leverage its data and information systems to create information advantage in a contested, degraded, and disconnected environment.

DATA LITERACY

3-67. Army and joint forces rely on the collection, processing, and analysis of data to understand situations, to make human and automated decisions, and for the exercise of C2. Data has become increasingly important to the Army mission. Soldiers and leaders must be more capable of drawing knowledge and understanding from data and information to create and exploit information advantages. Soldiers and leaders must be equally informed about the potential limitations, threats, and risk associated with data. This requires improvements in data literacy—the ability to derive meaningful information from data so that it can be applied effectively to actions and outcomes. Data literacy includes the skills, knowledge, and attributes to read, manipulate, analyze, and communicate with data to effectively enable commanders to make accurate and timely decisions.

3-68. Data literacy is an essential skill for all leaders and for personnel in specialized fields of interest such as intelligence, assessments, procurement, talent management, and sustainment. To improve data literacy across the force, the Army employs data literacy programs of instruction across the Army's education system. Leaders and Soldiers should engage in self-study on data literacy, including topics addressing data science and data analytics.

3-69. Data analytics includes the science of analyzing data to inform decisions, optimize performance, and gain a useful understanding from non-obvious associations. Army operations research/systems analysis personnel can assist units and leaders in employing data science and data analytic tools to solve problems, plan operations, and assess progress of activities, programs, and operations.

This page intentionally left blank.

Chapter 4
Protect

Leaders must assume they are under constant observation from one or more domains and continuously ensure they are not providing lucrative targets for the enemy to attack.

FM 3-0

Chapter 4 begins with an overview of the protect information activity. A description of the tasks that secure, obscure, and defend information and networks follows. The chapter concludes with considerations for effectively protecting data, information, and networks.

PROTECT OVERVIEW

4-1. 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.

4-2. Understanding the threat is the first step to protecting friendly data, information, and networks. Threats possess a wide range of land-, maritime-, air-, space-, and cyberspace-based reconnaissance and surveillance capabilities that can detect and collect data and information on U.S. forces. Army forces are typically in continuous influence, visual, and electromagnetic contact with threats. Persistent surveillance by threat space and cyberspace capabilities may extend to home station and follow forces through deployment and redeployment. Threats also possess space, cyberspace, and electromagnetic warfare capabilities that can disrupt friendly networks, data, and systems. Threats target friendly command and control (C2) centers and nodes, surveillance and target acquisition sensors, telecommunications systems and infrastructure, and networks. Information links, such as radio frequency receivers, radars, communications devices, and information protocols are targeted by threats to degrade communications, navigation, and fire control.

4-3. A force that can protect its data, information, and intentions while maintaining the ability to communicate has an advantage. The protect information activity contributes to this advantage through three related tasks: secure and obscure friendly information; conduct security activities; and defend the network, data, and systems as shown in Figure 4-1 on page 4-2. Denying the threat's access to friendly information degrades the threat's ability to understand the situation and act effectively. Defending the friendly network, data, and systems ensures communications among humans and automated systems.

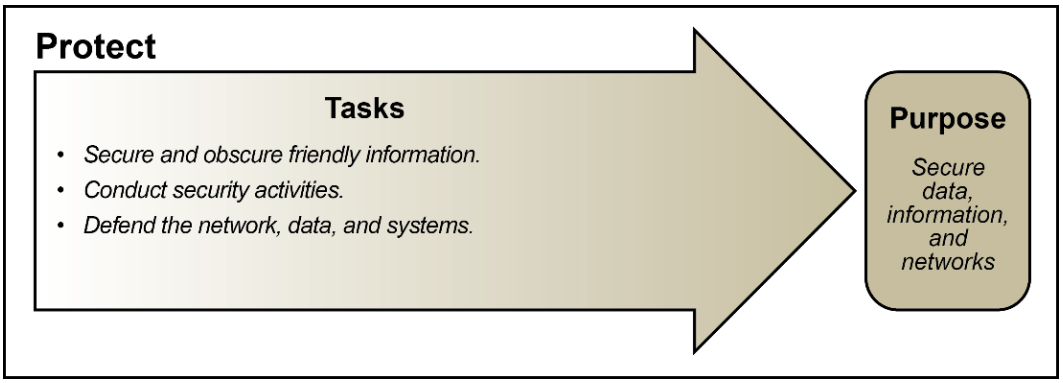


Figure 4-1. Tasks and purpose of the protect information activity

SECURE AND OBSCURE FRIENDLY INFORMATION

4-4. 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.

4-5. 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. Leaders must understand that threats will leverage all available data and information relating to friendly forces, which includes data from public and commercial sources. Based on their understanding of the friendly data and information signature, Army leaders use many techniques to reduce or shape that signature. Tasks that secure and obscure friendly information include—

Imperative of operations: Account for being under constant observation and all forms of enemy contact.

- Implement operations security (OPSEC).
- Conduct deception in support of OPSEC.
- Employ camouflage, concealment, and obscuration.

IMPLEMENT OPERATIONS SECURITY

> *Operations Security (OPSEC) as a concept is probably as old as war itself. Nevertheless, the fact that poor OPSEC practices have been costly in loss of human life and lost objectives in every American war demonstrates that, despite its venerated age, Operations Security as a doctrine needs to be learned afresh by each generation.*
>
> National Security Agency, 1993

4-6. OPSEC is a process that identifies and controls essential elements of friendly information (EEFIs), indicators of friendly force actions, and the measures or activities to reduce the risk of a threat exploiting friendly vulnerabilities. In operations security usage, an *indicator* is data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities (JP 3-13.3). OPSEC prevents threats from gathering and exploiting information about friendly forces, to include friendly force disposition, composition, and intent. OPSEC is fundamental to all operations that drive the planning and execution of activities to protect friendly data and information. Effective OPSEC is a cumulative outcome of adherence to disciplined tactics, techniques, and procedures and enforcement of standards across every echelon, down to the individual Soldier.

Operations security is both a process and a mindset adopted by all Soldiers to reduce the threat's ability to collect information and discern friendly force intentions.

4-7. A threat could compile and correlate enough information through observation or publicly available information to predict and counter Army operations. To counter the threat's ability to aggregate information about Army forces, commanders integrate OPSEC into all aspects of training, planning, and operations. Steps of the OPSEC process are—

- Identify EEFIs.
- Conduct threat analysis.
- Conduct vulnerability analysis.
- Conduct risk assessment.
- Apply OPSEC measures and countermeasures.

4-8. Army leaders implement OPSEC countermeasures to help secure friendly information and intentions. In general, selected OPSEC measures and countermeasures minimize predictability, conceal indicators of key capabilities and potential objectives, and counter inherent vulnerabilities in mission processes and technologies. Countermeasures may also directly attack the threat's collection system. Table 4-1 provides examples of OPSEC measures and countermeasures. (Refer to ATP 3-13.3 for more information on the OPSEC.)

Table 4-1. Example operations security measures and countermeasures

Type of measure or countermeasure	***Sample measures and countermeasures***
Administrative	• Conceal administrative (supply, logistics, and finance) requests related to preparations for operations. • Burn or shred paper documents, including unclassified information, to prevent the inadvertent disposal of classified and controlled unclassified information.
Counter reconnaissance and intelligence	• Defeat enemy intelligence and information collection and processing capabilities. • Conduct counterintelligence activities.
Deception	• Employ deception in support of operations security to distract threats from, or provide concealment for, unit operations and supporting activities. • Employ decoys and a cover story to provide alternate stimuli and focus for threat collection assets to prevent identification of essential elements of information.
Operations and logistics	• Avoid developing predictable patterns of tactics, procedures, or activities. • Employ forces in a way that conceals the location, identity, command relationships, and intent of friendly units.
Technical	• Implement electromagnetic protection techniques, including terrain masking. • Implement emission controls. • Avoid using unsecured channels of communications. • Locate antennas away from command posts.

DECEPTION IN SUPPORT OF OPERATIONS SECURITY

4-9. Indicators revealed at any level can contribute to the failure of an operation. To mitigate the risk of an OPSEC compromise, commanders can plan and reveal false indicators to the threat through deception in support of operations security (DISO). OPSEC and military deception (MILDEC) both affect the threat's decision-making processes, which can lead to the threat making an erroneous or untimely decision. OPSEC accomplishes this by concealing important information; MILDEC accomplishes it by conveying misleading information. The two processes are related.

Commanders employ deception in support of operations security to create multiple false indicators that confuse enemy or adversary forces operating in the unit's area of operations, making unit intentions harder to interpret.

4-10. DISO is a deception activity that conveys or denies selected information or signatures to a foreign intelligence entity (FIE). DISO also 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 a 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 or operational activity.

4-11. DISO differs from MILDEC and tactical deception in that it only targets FIEs and is not focused on generating a specific enemy action or inaction. Because DISO does not target a specific enemy decision maker, the DISO approval process differs from the MILDEC approval process. DISO can be approved at two levels higher if it adheres to the joint policy for MILDEC in CJCSI 3211.01F and is developed in support of an approved OPSEC plan. Combatant command instructions add guidelines, policies, and processes that must be adhered to in their respective commands. (See FM 3-13.4 for more information on DISO.)

EMPLOY CAMOUFLAGE, CONCEALMENT, AND OBSCURATION

To design and effectively integrate camouflage and concealment activities, personnel must constantly consider an enemy's point of view.

ATP 3-37.34

4-12. Threat forces collect information about Army forces for two basic reasons—target acquisition and intelligence production. Camouflage and concealment are OPSEC measures used to protect friendly forces and activities from threat detection—observation and surveillance. Camouflage and concealment help obscure friendly data and information.

4-13. Camouflage and concealment are materials and techniques. Friendly forces use them to hide, blend, disguise, or disrupt their appearance as military targets and their backgrounds to prevent visual and electromagnetic detection. Employing camouflage and concealment helps prevent an enemy from detecting or identifying friendly troops, equipment, activities, and installations.

4-14. Camouflage uses natural or man-made materials on personnel, objects, and tactical positions to confuse, mislead, or evade the enemy. It contributes to survivability by causing the enemy to not consider these things as targets; or it confuses the enemy as to the nature, parameters, or specifics associated with those potential targets. For instance, camouflage nets may be used to conceal vehicles, tents, shelters, and equipment, while vegetation is generally used to disrupt the outline of the target rather than completely hide it. Concealment makes use of terrain and other natural or man-made features to protect from observation and surveillance. Along with cover, concealment is one of the five military aspects that leaders use to analyze terrain. Leaders consider concealment when identifying potential friendly positions such as assembly areas, routes, assault positions, and battle positions. (Refer to ATP 3-37.34 for camouflage and concealment techniques.)

4-15. A major enabler of concealment is obscuration—the effects of weather, battlefield dust, and debris, or the use of smoke munitions (or other potential obscurants) to hamper observation and target-acquisition capability or to conceal activities or movement. Battlefield obscuration is typically provided by fires or hand-employed devices. (Refer to ATP 3-11.50 for additional information about the employment of obscurants.)

4-16. Electromagnetic masking is a form of obscuration. *Electromagnetic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-85). Electromagnetic masking disguises, distorts, or manipulates friendly electromagnetic radiation to conceal critical information or present false perceptions to threat commanders. Electromagnetic masking is an essential component of deception, OPSEC, and signals security. (Refer to ATP 3-12.3 for more information on electromagnetic masking.)

CONDUCT SECURITY ACTIVITIES

4-17. 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—

- Conduct security operations.
- Implement physical security.
- Implement the personnel security program.
- Conduct counterintelligence.

CONDUCT SECURITY OPERATIONS

4-18. 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, and area security. (See FM 3-90 for more information on security operations.)

4-19. 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.

4-20. Destroying enemy reconnaissance assets allows friendly force commanders to gain an advantage relative to the enemy. Denying the enemy's ability to see the area of operations denies the enemy commander the ability to act with sufficient situational understanding, and thus make poor decisions relative to friendly forces. Eventually, the enemy's inability to see the battlefield leads to disorganized enemy actions and renders those enemy forces more vulnerable to action by friendly forces. The staff considers the enemy's ability to conduct reconnaissance to determine if operations require additional maneuver or sustainment assets.

4-21. Threat unmanned aircraft systems carry a variety of surveillance and reconnaissance capabilities, ranging from high-resolution video to infrared or electromagnetic reconnaissance. Threat militaries use these systems to collect information about friendly troop locations, dispositions, and compositions for intelligence collection and targeting. Compounding the risk, threats can equip small, unmanned aircraft systems which are difficult to detect with attack capabilities. Unmanned aircraft systems carry a range of capabilities, to include surveillance, reconnaissance, targeting, electromagnetic attack, and air-to-surface weapons. Army units counter threat unmanned aircraft systems through—

- Radar—warning and tracking.
- Electromagnetic attack—directed energy or jamming of control systems.
- Air defense artillery.
- Small arms fire.
- Camouflage and concealment.

IMPLEMENT PHYSICAL SECURITY

4-22. 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.)

IMPLEMENT PERSONNEL SECURITY PROGRAM

4-23. 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.)

CONDUCT COUNTERINTELLIGENCE

4-24. *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.

4-25. 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.

4-26. 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.)

DEFEND THE NETWORK, DATA, AND SYSTEMS

Threat cyberspace and [electromagnetic warfare] capabilities jeopardize U.S. freedom of action in cyberspace and the electromagnetic spectrum. Because communications are a key command and control enabler, U.S. military communications and information networks present high-value targets.

ATP 6-02.12

4-27. Army and joint forces secure and defend the network to preserve the C2 system, protect friendly communications and network capabilities, and defeat threat cyberspace and electromagnetic reconnaissance. Various threats constantly attack Army networks. During competition, threats seek vulnerabilities and attempt to penetrate Army networks and systems to gather information and set conditions for future attacks. During armed conflict, threats attempt to destroy Army networks and corrupt and manipulate friendly information and data. Army forces conduct tasks to defend the network, data, and systems, including—

- Conduct cyberspace security.
- Conduct defensive cyberspace operations.
- Conduct communications security.
- Conduct electromagnetic protection.
- Conduct defensive space operations.

CONDUCT CYBERSPACE SECURITY

4-28. *Cyberspace security* is actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers and networks, including platform information technology (JP 3-12). The term "protected cyberspace" includes Department of Defense (DOD)-owned and -leased communications and computing software, data, security services, associated services, national security systems, and other relevant systems and services.

4-29. A threat's pathway into an Army network is often via a compromised individual-user device. All Soldiers conduct cybersecurity by knowing the techniques that threats use to penetrate Army networks. These techniques include unusual emails, odd attachments, compromised links, or other methods. Cybersecurity specialists keep Army personnel informed of new and evolving methods that threats might use to penetrate Army networks.

Threats use known vulnerabilities of existing systems. Users must comply with directives to patch systems or log their computers into networks for automatic patching.

4-30. Cybersecurity professionals perform the technical aspects of cybersecurity. These include continuously monitoring the network for any anomalies that might indicate intrusion, ensuring firewalls are emplaced, and updating antivirus software. Cybersecurity includes ensuring critical network infrastructure has sufficient physical security to prevent either direct access or sabotage. Classified networks have additional communications security, data encryption, physical security, and procedures based on both regulations and assessed risk. Cybersecurity secures networks and systems by systematically applying—

- The risk management framework.
- Configuration management and patching.
- Antivirus protection.
- Intrusion monitoring and detection.

Conduct Defensive Cyberspace Operations

4-31. *Defensive cyberspace operations* are missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity (JP 3-12). Defensive cyberspace operations and cyberspace security share a common objective of a secure network. While cyberspace security serves as the first line of protection against threat cyberspace attacks, defensive cyberspace operations involve deliberate measures to counter a specific threat attack, exploitation, or malware that is anticipated or has breached security measures.

Note. Joint doctrine list three categories of cyberspace: blue, red, and gray. The term "blue cyberspace" denotes U.S. cyberspace (areas in cyberspace owned or controlled by the United States Government or a U.S. person) and other areas of cyberspace the DOD is ordered to protect. The term "red cyberspace" refers to those portions of cyberspace owned or controlled by, or on behalf of, an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, "controlled" means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray cyberspace." The Army refers to blue, red, and gray cyberspace as friendly, neutral, and threat cyberspace respectively. (Refer to JP 3-12 for more information on cyberspace.)

4-32. *Cyberspace defense* includes actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures (JP 3-12). Cyberspace defenders act on cues from cyberspace security or intelligence alerts of threat activity within friendly networks. Cyberspace defense tasks include monitoring for threats on friendly networks, deploying advanced countermeasures, and responding to eliminate these threats and mitigate their effects. (Refer to FM 3-12 for more information about defensive cyberspace operations.)

Conduct Communications Security

4-33. *Communications security* is actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study (JP 6-0). Communications security includes—

- Crypto-security—protects user data and system data.
- Transmission security—anti-jamming or encryption of the transmission path.
- Emissions security—equipment shielding and emission control.
- Physical security—protects communications security material and information.

4-34. While communications security's primary aim is to protect classified information and communications, it also protects against the loss of controlled unclassified information to prevent threats from gaining access to critical indicators. Communications security helps Army forces maintain OPSEC and achieve surprise in operations by denying adversaries and enemies any foreknowledge of friendly forces' capabilities and intentions. Units employ communications security devices to secure communications networks, including tactical radio networks. (Refer to FM 6-02 for more information about communications security measures.)

Conduct Electromagnetic Protection

4-35. *Electromagnetic protection* is a division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). Electromagnetic protection measures eliminate or mitigate the negative impact resulting from friendly, neutral, enemy, or naturally occurring electromagnetic interference. Army forces execute a variety of electromagnetic protection tasks depending on threat capabilities and operational environments (OEs). Some of the most common tasks include—

- Emission control.
- Electromagnetic compatibility.
- Electromagnetic hardening.

(Refer to ATP 3-12.3 for more information about electromagnetic protection.)

Emission Control

4-36. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan (JP 3-85). Emission control enables OPSEC by decreasing detection probability and countering detection range by enemy sensors. Units practice emission control by—

- Using devices selectively—turning off unnecessary emitters and using necessary emitters only when they are needed.
- Controlling power—using the minimum transmission power needed to communicate.
- Preventing continuous use that enables enemy detection—keeping radio transmissions to a maximum of 15 seconds.

Electromagnetic Compatibility

4-37. The staff determines how to mitigate electromagnetic compatibility challenges. *Electromagnetic compatibility* is the ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response (JP 3-85). The staff uses spectrum planning, coordination, and management of the electromagnetic spectrum to mitigate electromagnetic compatibility challenges. Soldiers train to recognize potential compatibility issues and report suspected issues up the chain of command. Spectrum managers immediately consult with other staff members to determine the cause. Some issues initially identified as compatibility issues may indicate threat interference. In either case, Army forces act to reduce compatibility issues or eliminate the threat interference.

Electromagnetic Hardening

4-38. *Electromagnetic hardening* consists of action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-85). Electromagnetic hardening can protect friendly spectrum-dependent devices from the impact of electromagnetic interference or attack by lasers, high-powered microwaves, or electromagnetic pulses. An example of electromagnetic hardening includes installing electromagnetic conduits made of conductive or magnetic materials to shield against undesirable effects of electromagnetic energy.

CONDUCT DEFENSIVE SPACE OPERATIONS

4-39. The Army relies on space capabilities and systems to provide global positioning, satellite communications, weather and related environmental conditions, and intelligence collection platforms. These systems are critical enablers the Army uses to plan, communicate, navigate, maneuver, engage the enemy, provide missile warning, maintain situational understanding, protect, and sustain forces. Space capabilities are regularly used by every element of the Army and the joint force. Planning and coordination with national, joint, and theater resources takes place through liaison with space operations officers. Army and joint space forces conduct space operations to enable freedom of action in the space domain for the United States and its allies, to defeat efforts to interfere with U.S. and multinational space systems, and to deny threat freedom of action in the space domain. Defensive space operations—actions taken to preserve friendly freedom of action in space—is a key component of space operations.

4-40. Defensive space operations are actions taken to protect friendly satellite communications and other space capabilities from attack, interference, unauthorized intrusions, and hazards. Defensive space operations are focused on responding to man-made threats which may affect the terrestrial and space systems. These actions safeguard assets from hazards such as space debris, radio frequency interference, and naturally occurring phenomenon such as radiation and space weather.

4-41. Robust defensive space operations influence enemies' perceptions of space capabilities and make them less confident in successfully interfering with those capabilities. Friendly forces may be warned when enemy space-based reconnaissance and surveillance assets will be able to view and record activity. An example of defensive space operations enabled by space situational awareness is forces using camouflage, concealment,

and deception techniques to protect themselves when notified of potential space-based observations. Passive defensive space operations measures such as encryption and electronic hardening of Global Positioning System receivers increases the likelihood Soldiers will receive information in degraded space environments. Active defensive space operations protection actions such as geo-locating jamming sources assist Soldiers to find, fix, and destroy jammers.

PROTECT CONSIDERATIONS

4-42. Gaining and maintaining information advantage requires Army leaders to protect against threat attempts to access or affect friendly data, information, and communications. To do this, commanders and staffs incorporate protect information tasks into the operations process using a combined arms approach. To formulate plans for protecting friendly data, information, and networks, Army leaders must understand friendly vulnerabilities and be aware of what information the friendly force may be revealing to the threat. This understanding guides threat analysis and aids development of mitigation measures. Several fundamentals guide commanders and staffs in the planning and execution of tasks within the protect information activity:

- See yourself physically and virtually.
- See the threat and account for being under constant observation.
- Employ combinations of active and passive protection measures.

SEE YOURSELF PHYSICALLY AND VIRTUALLY

4-43. Protecting data, information, and networks begins with an awareness of the physical and virtual signatures (information footprint) the friendly force presents to the threat. Army leaders must understand how their headquarters and formations appear to a threat from each domain and from the electromagnetic spectrum. This understanding, combined with an understanding of threat information collection and attack capabilities, provides the basis for directing protect activities to mitigate friendly vulnerabilities.

Observable signatures increase an enemy's likelihood of successfully detecting, collecting information about, and targeting Army formations and critical command and control nodes.

4-44. Friendly troop activities, gatherings of key leaders, patterns of life, social media posts, and physical signatures all help the threat paint a picture of the disposition, composition, and intent of the friendly force. For example, Soldier behaviors in garrison, out in the public, and online can indicate an upcoming deployment and provide insight into unit readiness. Troop movements and communications during crisis can highlight when forces deploy, where they deploy, what type of forces deploy, and for what purpose. During armed conflict, friendly forces emanate electromagnetic signatures that when aggregated can identify the size and composition of forces in a certain location.

Electromagnetic Signatures

4-45. Multiple electromagnetic emissions are common to command posts (CPs). Many weapon platforms include radios, digital enablers, and active sensors that present a significant detectable signature in the electromagnetic spectrum. Threats have well-developed capabilities to locate electromagnetic signatures using ground-based, space-based, and aerial electromagnetic warfare systems. Appropriate mitigation measures can significantly reduce an enemy's ability to locate friendly systems, collect information, and target systems with lethal or nonlethal effects. Units mitigate electromagnetic signatures with electromagnetic protection and emissions control as discussed in paragraphs 4-35 and 4-36.

4-46. In addition to military equipment, personal electronic devices, such as smart phones, tablets, and watches, produce electromagnetic signatures. Their inherent technical characteristics enable threats to easily locate cell phones with precision. Cell phones communicate with a cellular network infrastructure. Threats can deploy systems to imitate a legitimate cell phone infrastructure and gather subscriber and location data. By locating heavy concentrations of cell phone users in an area, particularly outside urban areas, threats can pinpoint large formations and target them with lethal fires.

Personal Electronic Devices

Personal electronic devices pose a significant operations security risk to friendly forces. Even the seemingly benign use of online fitness tracking devices and services has developed into a significant information risk for U.S. personnel. For example, in 2018, an international fitness tracking company published an online interactive map displaying the aggregate running and cycling routes of millions of personal fitness device users from around the world. Among the users were thousands of personnel deployed to forward operating bases (FOBs) in Iraq, Syria, and Afghanistan. The maps included accurate Global Positioning System coordinates, depicted perimeters, identified daily life patterns, and outlined internal structures within the FOBs. Such information could prove useful to enemy targeting efforts. By August 2018, the Department of Defense issued instructions that prohibited personnel from using geolocation features and functionality—applications and services—while in operational areas unless authorized by combatant commanders.

Commanders weigh the potential risks that personal electronic devices pose to operations and take measures to balance operations security with Soldiers' quality of life. This example also demonstrates the need to educate Soldiers on the risks of personal electronic device use and methods to safeguard their data.

4-47. Many personal electronic devices are computers—from cell phones and tablets to video games and car navigation systems. While computers provide increased features and functionality, they also introduce new risks. For example, an attacker may be able to infect a cell phone with a virus, steal phone or wireless service, or access the data on those devices. Not only do these activities have implications for personal information, but they could also have serious consequences if users store operational information on the devices.

Visual Signatures

4-48. Threats can gather a great deal of information about Army force locations, dispositions, and activities by direct visual observation from land, air, and space. Units minimize the visual signatures to mitigate threat reconnaissance capabilities. Camouflage, concealment, dispersion, the use of decoys, and light discipline help mitigate visual signatures.

Radar Signatures

4-49. Threat forces use radar to locate Army forces and provide guidance for precision munitions. The radar signature, or radar cross-section, of a CP, weapon system, or formation indicates how detectable it is to a threat radar. Even concertina wire exhibits a measurable cross-section at radar frequencies. Units protect against detection and targeting by mitigating their radar signatures. Radio frequency reflective camouflage netting reduces the radar signature of CPs and equipment. Emplacing concertina wire to follow natural terrain features, when possible, reduces its radar signature. Units take advantage of natural terrain and man-made structures to mask formations from threat radar systems.

Infrared (Heat) Signatures

4-50. Power generators, vehicles, and other heat sources produce thermal signatures that enemy surveillance and target acquisition sensors can readily detect. Emplacing heat-producing equipment and other thermal sources in defilade positions, in structures, or under natural cover mitigates their infrared signatures. Heat diffusers that disperse and vent vehicle exhaust away from the threat expediently reduce thermal signature.

Noise Signatures

4-51. The power generation equipment can generate significant noise signatures a threat may detect either through reconnaissance or passive acoustic (noise) detectors. Such noise is created by radars,

communications equipment, large CPs, tanks, and wheeled vehicles. During site selection, leaders consider measures to mask and diffuse the noise from generators and vehicles.

Social Media Signatures

4-52. Army organizations, Soldiers, and family members use the internet to communicate and exchange information. This includes official social media platforms and internet sites maintained by Army organizations and personal social media accounts established and used by Soldiers and family members. Official social media sites often list organizational missions and goals, subordinate organizations, and public affairs releases. The information on these sites is available to the public and can be consumed by any audience, intended or not intended, domestic or foreign. While used to communicate and provide transparency, Army leaders continuously assess the timing and content of information on these sites to ensure they do not provide OPSEC indicators. Commanders release public information consistent with security restraints in DODI 5200.01 and the principles of information outlined in DODD 5122.05.

4-53. Most Soldiers and their families are active on one or more social media platforms. Most of this social media activity is publicly available for anyone to view. Threats routinely and persistently monitor social media to gather information about Soldiers, Army units, and operations. By aggregating seemingly minor indicators, a threat actor may be able to develop a relatively complete understanding of U.S. force strength, locations, capabilities, intentions, and morale. Threats also attempt to impersonate DOD employees and Service members to distract audiences, discredit information, or manipulate audiences. AR 360-1 establishes guidance for official and personal social media use and online conduct. For personal use of social media, commanders at every level persistently and comprehensively stress individual responsibility and the OPSEC ramifications of social media activity. Leaders educate Soldiers and family members on hardening social media through privacy settings to counter adversaries' collection.

See the Threat and Account for Being Under Constant Observation

4-54. In addition to understanding the signatures that friendly forces present, Army leaders must understand the threat's ability to collect on those signatures. The nine forms of contact provide a framework to account for threat observation. Air, space, and cyberspace capabilities increase the likelihood that threat forces can gain and maintain continuous visual, electromagnetic, and virtual contact with Army forces during competition, crisis, and armed conflict. (Refer to FM 3-0 for more information on the forms of contact.)

There are nine forms of contact: direct; indirect; non-hostile; obstacle; chemical, biological, radiological, and nuclear; aerial; visual; electromagnetic; and influence.

4-55. Peer threats possess a wide range of land-, maritime-, air-, and space-based intelligence, surveillance, and reconnaissance (ISR) capabilities that can detect and collect information on U.S. forces. During competition and crisis, threat forces employ multiple methods of collecting on friendly forces to develop an understanding of U.S. capabilities, readiness status, and intentions. They do this in and outside the continental United States. They employ space-based surveillance platforms to observe unit training and deployment activities. Threats can use this information to target Army forces during conflict. The proliferation of personnel using network-enabled electronic devices exacerbates this risk. Soldiers and their families must consider how their use of telecommunications, the internet, and social media makes them or their units vulnerable to adversary surveillance.

4-56. Leaders assume they are always under constant observation from one or more domains in all contexts, from home station through deployment, and while conducting operations. Leaders continuously assess and account for various information collection methods the threat uses to collect and exploit information that friendly forces generate. The intelligence process, intelligence preparation of the operational environment (IPOE), information collection, and the OPSEC process all facilitate understanding threat collection capabilities and methods.

EMPLOY COMBINATIONS OF ACTIVE AND PASSIVE PROTECTION MEASURES

4-57. The threat seeks to gather, deny use of, and corrupt friendly data, information, and communications using many capabilities. Army leaders take a combined arms approach to counter threat information collection and attack methods by directing combinations of active and passive information protection measures.

4-58. When Army forces execute active protection measures, they act directly against threat information collection and information warfare capabilities to either deny or limit their use against Army forces. Active protection includes responding to ongoing attacks against Army data, information, and networks to limit the damage from threat information warfare activities. Army forces actively protect information while conducting operations in all the strategic contexts. Examples of active information protection include counterreconnaissance and cyberspace defense operations.

4-59. When Army forces execute passive information protection measures, they act to indirectly reduce the effectiveness of threat information collection and information warfare capabilities. While not all Army forces have the capabilities to take active information protection measures, all Army forces employ passive measures to disrupt the threat's ability to collect relevant information. Passive protection requires Soldiers actively considering what information they receive and what indicators their actions portray to the threat and other relevant actors. Examples of passive information protection include employing camouflage, noise, and light discipline; hardening critical infrastructure; and reducing electromagnetic emissions. Dispersion of CPs and having redundant capabilities are other examples.

This page intentionally left blank.

Chapter 5

Inform

When what we do is different from what we say or the images we share, the public whose support we need cannot be sure which one to believe—the words, the images or the actions.

JDN 2-13

Chapter 5 begins with an overview of the inform information activity. A discussion of commander's communication synchronization follows. The chapter then describes inform information activity tasks. The chapter concludes with considerations for effectively informing various audiences.

INFORM OVERVIEW

Regardless of what audience Army leaders seek to inform, the information provided has the potential to be seen by audiences all over the world.

5-1. 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.

5-2. 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.

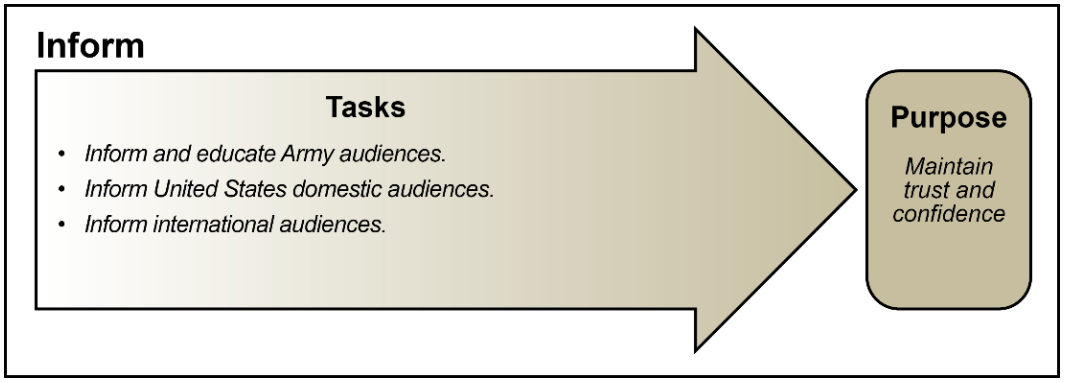


Figure 5-1. Tasks and purpose of the inform information activity

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).

COMMANDER'S COMMUNICATION SYNCHRONIZATION

5-3. For inform information activity tasks to be effective, Army words, images, and deeds must match. Commander's communication synchronization (CCS) is the process that helps do this. *Commander's communication synchronization* is a process to coordinate and synchronize narratives, themes, messages, images, operations, and actions to ensure their integrity and consistency to the lowest tactical level across all relevant communication activities (JP 3-61). Within this context, communication is the imparting or interchange of information, thoughts, and opinions by sending themes, messages, and facts through engagements and traditional and digital media platforms to designated audiences. CCS helps develop the commander's communication strategy that guides the execution of tasks that inform Army, U.S. domestic, and international audiences.

5-4. CCS is a top-down process starting at the U.S. government level and nesting down to Army tactical forces. At the national level, CCS focuses efforts for leaders to understand and communicate with key audiences to create, strengthen, or preserve favorable conditions to advance U.S. interests, policies, and objectives through coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.

5-5. Joint force commanders support the national security narrative by developing themes appropriate to their mission and authority. A theme is a distinct, unifying idea that supports a narrative. Sometimes commanders develop multiple themes to support a narrative. Operational-level themes are often created for each phase of an operation. Commanders continually nest operational themes with strategic themes and enduring national narratives to mitigate risks that phase-by-phase themes appear to give conflicting messages.

5-6. Messages support themes by delivering tailored information to a specific public audience. Commanders can also tailor messages for a specific time, place, and communications method. While messages are dynamic, they support enduring themes of higher headquarters and subordinate organizations. The dynamic nature inherent in messages provides joint force commanders and planners with agility in reaching various audiences.

The proactive release of accurate information to Army, U.S. domestic, and international audiences puts operations in context, facilitates informed perceptions about military operations, undermines threat propaganda, and helps achieve an information advantage.

5-7. Army commanders nest their communication strategy with the joint force. As the principal advisor for public information, command information, crisis communications, visual information, and community engagement, the public affairs officer manages the CCS process for Army commanders. Based on the commander's intent and planning guidance, the public affairs officer coordinates with other members of the staff to implement higher-headquarters communication guidance to coordinate themes, messages, talking points, and images with Army operations. Part of this coordination includes determining the implications that a public message may have to non-primary audiences and recommended potential follow-on messaging. This continuous process requires deliberate planning in competition, crisis, and conflict. (See FM 3-61 for more information on public affairs and CCS.)

INFORM AND EDUCATE ARMY AUDIENCES

5-8. 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—

- Informing internal audiences.
- Educating Soldiers.

INFORM INTERNAL AUDIENCES

5-9. 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.

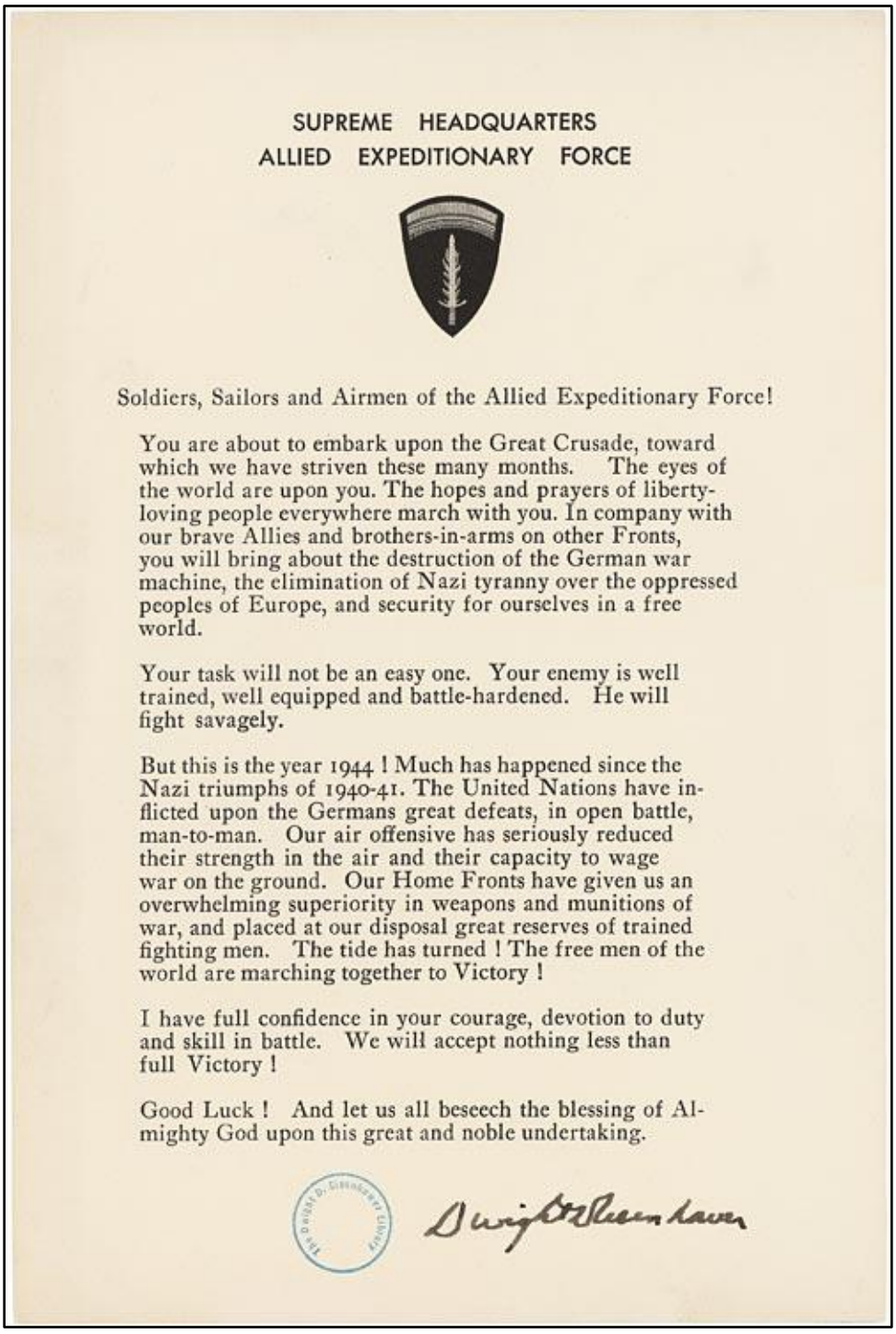
5-10. An effective command information program combined with community engagement aids commanders in informing internal audiences. *Command information* is communication by a military organization directed to the internal audience that creates an awareness of the organization's goals, informs them of 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). All Army echelons participate in providing command information to their organizations.

5-11. The Army uses installation and organizational publications and multimedia services to communicate directly with the internal audience on its installations. While installation and organizational publications offer traditional ways of communicating, digital forms of communication, augmented by data-driven insights to optimize engagement, are the dominant means for most organizations. Social media and internet-based communication provide additional, two-way communication between a military organization and its audiences. As technology and capabilities evolve, managing digital and social media becomes an essential component for communicating effectively. (Refer to DODI 5400.17 for policy concerning official use of social media.)

5-12. While command information is intended to communicate internally, commanders recognize that any information they release becomes readily available to national and international audiences. When providing command information, commanders consider the information they disseminate and its potential release to external audiences. (See FM 3-61 for more information on command information.)

A human advantage occurs when a force holds the initiative in terms of training, morale, perception, and will.

5-13. 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. Figure 5-2 on page 5-4, General Eisenhower's letter to the Soldiers, Sailors, and Airmen of the Allied Expeditionary Force, provides an example of communicating purpose. Published as the order of the day for June 6, 1944, the order was distributed to all members of the expeditionary force on the eve of the Normandy invasion.



SUPREME HEADQUARTERS
ALLIED EXPEDITIONARY FORCE

Soldiers, Sailors and Airmen of the Allied Expeditionary Force!

You are about to embark upon the Great Crusade, toward which we have striven these many months. The eyes of the world are upon you. The hopes and prayers of liberty-loving people everywhere march with you. In company with our brave Allies and brothers-in-arms on other Fronts, you will bring about the destruction of the German war machine, the elimination of Nazi tyranny over the oppressed peoples of Europe, and security for ourselves in a free world.

Your task will not be an easy one. Your enemy is well trained, well equipped and battle-hardened. He will fight savagely.

But this is the year 1944 ! Much has happened since the Nazi triumphs of 1940-41. The United Nations have inflicted upon the Germans great defeats, in open battle, man-to-man. Our air offensive has seriously reduced their strength in the air and their capacity to wage war on the ground. Our Home Fronts have given us an overwhelming superiority in weapons and munitions of war, and placed at our disposal great reserves of trained fighting men. The tide has turned ! The free men of the world are marching together to Victory !

I have full confidence in your courage, devotion to duty and skill in battle. We will accept nothing less than full Victory !

Good Luck ! And let us all beseech the blessing of Almighty God upon this great and noble undertaking.

Dwight D. Eisenhower

Figure 5-2. Eisenhower's order of the day (6 June 1944)

EDUCATE SOLDIERS

5-14. 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, online 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.

5-15. 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.
- The Army profession.

Threat Influence Methods

5-16. 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. Alternatively, the threat may choose an indirect attack by targeting a weapon or information system used by Soldiers to reduce their confidence in their equipment. These threat influence methods are often enabled by the digital signatures created by Soldiers in their daily lives. Education about threat influence tactics and techniques and ways to mitigate threat efforts such as online awareness, digital signature management, and critical thinking increase Soldiers' ability to resist the negative effects on their morale and will.

5-17. Leaders ensure their subordinates know that threats actively monitor social media sites and collect open-source information. Threat intelligence specialists analyze collected information to generate intelligence. Soldiers may inadvertently violate operations security (OPSEC) by posting departures, arrivals, or locations of operations. Even without posting specific information, effective threat intelligence might correlate enough information to produce relevant intelligence. Soldiers may also unintentionally violate OPSEC by posting geotagged photos or social media posts. Unintentional violations can still seriously damage the success of Army operations and place fellow Soldiers at risk. The Army's Threat Awareness and Reporting Program helps educate Soldiers on threat espionage and required reporting of threat activity.

The Army Profession

5-18. 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. Understanding that they are part of something bigger than themselves and a member of a unique profession imbues Soldiers with the moral courage, resilience, morale, and will to prevail against threat information warfare.

5-19. Beginning with their induction into the Army, Soldiers learn that they are now part of a profession with associated values. The Army Values, Warrior Ethos, and Soldier's Creed provide the common foundation that enables all Soldiers to have a common understanding of what to expect of one another. When Soldiers encounter information that portrays Army operations contrary to these values, they apply critical thinking skills to assess that information as a member of a profession founded upon mutual trust and shared understanding. (See ADP 6-22 for more information on the Army profession.)

INFORM UNITED STATES DOMESTIC AUDIENCES

5-20. 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.

5-21. 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. (Refer to FM 3-61 for more information on public communication and community engagement.)

CONDUCT PUBLIC COMMUNICATION

5-22. 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.

5-23. 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.

CONDUCT COMMUNITY ENGAGEMENT

5-24. 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 operations. Community engagement places special emphasis on two-way communications with public communities surrounding military installations. Effective relationships with key stakeholders must be enduring; trust cannot be built after a crisis occurs.

5-25. The Army relies on communities and regions surrounding its installations for direct and indirect support. Communities provide the Army access to resources needed to train and maintain readiness as well as extend support to families of mobilized or deployed Soldiers. Commanders recognize that a positive rapport between the Army and its host communities is mutually beneficial, supporting the Army as an institution as well as its individual Soldiers.

5-26. Members of the Army National Guard and United States Army Reserve live and work in the community and are integral members of their hometowns. A community's positive relationship with a local installation depends upon the command. A commander considers potential implications of every installation activity, operation, or major training activity. This is especially important during crisis management, mobilization, deployment, and redeployment operations, even if the installation or reserve unit is not directly involved. A commander also considers potential implications during national events concerning politically sensitive or controversial Department of the Army or DOD issues. During such times, the information requirements of internal and external audiences increase dramatically. Installation and reserve unit commanders and their staffs—assisted by their public affairs elements—need to implement effective programs that include the open, honest, accurate, complete, and timely released information their communities expect.

CORRECT MISINFORMATION AND COUNTER DISINFORMATION RELATED TO ARMY FORCES OR OPERATIONS

All Soldiers and leaders are authorized to correct misinformation about which they have personnel knowledge if the information is unclassified and releasable.

5-27. Threats use many methods in their attempts to attrit the U.S. domestic audience's trust and confidence in Army forces. Digital media platforms make it easy for threats to exploit information for effect, misinformation, and disinformation, but threats can use less technologically sophisticated methods as well. Intelligence, public affairs, and other staff members assist commanders in identifying misinformation and disinformation about the Army. Public affairs and leaders then correct the record as appropriate through official channels. All Army forces have a duty to be alert for information that erodes U.S. citizens' trust in Army forces and the Army as an institution.

5-28. When countering misinformation and disinformation, Army forces preemptively and proactively tell the Army's story by providing public information and conducting community engagements. Critical to preempting misinformation or disinformation is a quick and active response by Army forces as soon as something negative occurs that might impact Army operations or perceptions about the Army. Public affairs specialists at all echelons assist the chain of command to get facts and context to the public audience as soon as possible. Soldiers refer potential information for effect and disinformation concerning policy, classified matters, or anything outside their scope of knowledge to their public affairs officer or chain of command.

5-29. Whether informing U.S. domestic or international audiences, effectively correcting misinformation and countering disinformation requires unity of effort. This includes coordination among the DOD, the military departments, Department of State, multinational partners, combatant commands, and Army forces. Annex J (Public Affairs) to operation plans and orders at all echelons provides direction and guidance that facilitate this unity of effort. Public affairs guidance, to include clear information and imagery release authority by echelon, enables Army commanders to rapidly correct misinformation and to counter disinformation. (See FM 3-61 for more information on correcting misinformation and countering disinformation.)

INFORM INTERNATIONAL AUDIENCES

5-30. The presence of Army forces assures allies and partners while it deters threats. The presence of friendly forces reduces threats' perception of the benefit of aggression relative to restraint. The Army, as part of the joint force and whole of government, informs and assures allied and partner audiences about its activities and operations globally and within specific regions. The presence of Army forces provides the proof of a U.S. commitment that should be articulated by simple, clear, and synchronized messages conveyed from strategic to tactical levels.

5-31. Overseas, the chief of mission, usually an ambassador, is the highest U.S. authority in a foreign country and has a U.S. government communication strategy within which all military engagements are nested. Army commanders conducting missions within a country coordinate with American Embassy personnel to ensure their inform efforts are synchronized with the U.S. government's communication strategy for that country.

5-32. Commanders employ public affairs activities to communicate with foreign audiences just as they communicate with domestic audiences when in the United States. Army forces maintain a scrupulous level of honesty and integrity when communicating to international audiences and should assume that anything communicated locally overseas is being communicated globally. As commanders conduct operations, physical activities and visible signatures from these actions confirm, reinforce, or contradict the information that commanders communicate through public affairs and other means. Avoiding contradictions is critical to maintaining information advantage.

5-33. When communicating to international audiences, commanders and staffs develop messaging appropriate to their mission and authority that support strategic themes developed by the National Security Council staff and Department of State, DOD, and other U.S. Government departments and agencies. Commanders ensure that their international themes and messages align with messaging to U.S. domestic audiences.

CONDUCT COMMUNITY ENGAGEMENT OUTSIDE THE CONTINENTAL UNITED STATES

5-34. Community engagement is especially important for Army forces conducting operations overseas. These activities involve working collaboratively with, and through, groups of people affiliated by geographic proximity or special interests to enhance the understanding and support for Army forces and operations.

5-35. For Army forces conducting operations outside the United States, community engagement plays a critical role in enabling Army forces to achieve their objectives. In all operational contexts, Army forces themselves are the principal messaging tool that supports informing allies and partners. Commanders, advised by public affairs staff, include community engagement activities as a part of their operations, enhancing the inherent informational effect of Army operations and building the relationship between Army forces and the civilian communities near where they operate.

5-36. Since Army forces rely heavily on the support of civilian communities in the overseas regions in which they conduct operations to support strategic security objectives, community engagement is critical during competition. Community engagements build trust between Army forces and supporting communities. These engagements provide Army forces with a unique opportunity to understand concerns of the local population and to address and reduce concerns caused by Army operations. For both temporarily deployed forces and permanently forward-deployed forces, community engagement is critical to meet current or future operational requirements.

CONDUCT SOLDIER AND LEADER ENGAGEMENT

5-37. During operations in which Army forces are assigned an area of operations, commanders direct Soldier and leader engagements (SLEs) to inform audiences. *Soldier and leader engagement* is interpersonal interactions by Soldiers and leaders with audiences in an area of operations (ATP 3-13.5). Because Army forces conduct operations in and among populations, conducting SLEs effectively inform international audiences.

Note. For Army forces, key leader engagement is a type of SLE. Key leader engagements are meetings with an influential leader with the intent of building a relationship that facilitates communication and cooperation across a wider population. Commanders also use SLE to influence foreign relevant actors as discussed in Chapter 6.

5-38. An SLE can be planned or unplanned. Planned SLEs include deliberate interpersonal interactions to provide specific information. Unplanned SLEs benefit from spontaneous interactions that allow greater understanding of an operational environment (OE) and attitudes of local populations, to include specific audiences, and process this understanding into time-sensitive feedback to other forces.

5-39. Leaders prepare their Soldiers before and during Army operations to conduct SLEs. Soldiers are invaluable in helping to understand specific audiences and their attitudes toward Army forces. They may be the sensors who report indications that Army operations are viewed positively or negatively. Behavior such as fear, hostility, indifference, or support of various audiences toward Soldiers enhances understanding and helps commanders assess whether their operations and words align. Because Soldiers understand the commander's engagement guidance, they can immediately engage audiences to mitigate negative effects of misinformation and disinformation. Soldier and leader behavior among foreign audiences is the most powerful means of informing them. (See ATP 3-13.5 for more information on SLE.)

CONDUCT CIVIL AFFAIRS OPERATIONS

5-40. Army forces conduct civil affairs operations principally to engage the civil component of an OE. Because civil affairs forces focus much of their operations on understanding local populations and their institutions, these forces can enhance a commander's understanding of the human dimension and associated civil considerations. Because civil affairs missions depend on engaging and developing relationships with relevant audiences, civil affairs operations substantially contribute to informing during the normal course of their duties.

5-41. Civil affairs forces assist commanders in informing international audiences, to include unified action partners and indigenous populations and institutions. Civil-military integration, a core competency of civil affairs forces, is essential to informing international audiences. *Civil-military integration* is the actions taken to establish, maintain, influence, or leverage relations between military forces and indigenous populations and institutions to synchronize, coordinate, and enable interorganizational cooperation and to achieve unified action (FM 3-57). Civil-military integration is essential to effectively integrate operations with commanders and unified action partners to achieve unity of effort. The establishment of a civil-military operations center, or other mechanisms, enables civil information sharing and integration. (See FM 3-57 for more information on civil affairs operations.)

CORRECT MISINFORMATION AND COUNTER DISINFORMATION WITHIN INTERNATIONAL AUDIENCES

5-42. Threats use propaganda to attempt to gain a relative information advantage over the United States, its allies, and its partners. Propaganda is information that is biased or misleading and is designed to influence the opinions, emotions, attitudes, or behaviors of any group to benefit the sponsor. Threats use information for effect, misinformation, and disinformation as propaganda tools to influence international public opinions and to sow internal discord to fracture military alliances and partnerships.

Disinformation is incomplete, incorrect, or out of context information deliberately used to influence audiences. Threats often rely on publics to promulgate disinformation that members of the public unwittingly believe to be correct information.

5-43. Information for effect, misinformation, and disinformation reside in the same outlets as factual, truthful information. Knowing where to search and being able to identify the types and tactics of threat information is critical to counter a threat's malign narrative. The staff's understanding of informational considerations of an OE helps that staff identify threat means, methods, and capabilities for using propaganda.

5-44. Commanders and staffs consider several factors when deciding if, how, and when to correct misinformation and deciding whether to, how, and when to counter disinformation. Not all misinformation or disinformation needs to be actively addressed. First, they consider what makes the disinformation believable to a specific audience. Understanding what makes information about an event newsworthy to a specific audience helps understanding the factors that enable a threat to effectively use disinformation.

5-45. Second, commanders and staffs consider the unity of effort necessary to counter disinformation. When coordinating information activities, commanders ensure unity of effort in countering disinformation. Commanders consistently communicate in an integrated and coherent manner regarding the actions and intentions of Army forces and their leaders to counter disinformation.

5-46. Speed is a third consideration when countering misinformation and disinformation. The first side that presents the information often sets the context and frames the public debate. Staffs work quickly to get accurate information and imagery out first, without rushing to failure by inadvertently releasing inaccurate or incomplete information.

5-47. Some audiences will not respond positively to friendly attempts to correct misinformation and counter disinformation. These types of international audiences may automatically assume any information released by Army forces to be disinformation. Commanders and staffs examine the informational considerations of an OE and focus on correcting misinformation and defeating threat disinformation among audiences willing to consider public information released by Army forces. In some cases, Army commanders coordinate for an external source to correct misinformation or to counter disinformation.

INFORM CONSIDERATIONS

5-48. Several fundamentals guide commanders in planning for and executing inform information activity tasks, to include—

- Tell the truth.
- Timely release of information and OPSEC.
- Compliance with law and policy.

TELL THE TRUTH

5-49. The long-term success of a commander's communication strategy depends on maintaining the integrity and credibility of officially released information. Deceiving the public undermines trust in the Army. The accurate, balanced, and credible presentation of information leads to public confidence in the Army and the legitimacy of Army operations. Attempting to deny unfavorable information or failing to acknowledge its existence leads to media speculation, the perception of a cover-up, and the loss of public trust. Commanders and leaders, along with their public affairs officers, address issues openly and honestly as soon as possible.

TIMELY RELEASE OF INFORMATION AND OPERATIONS SECURITY

> *The First Amendment guarantees freedom of the press, but within the Department of Defense this right must be balanced against the military mission that requires operations security at all levels of command to protect the lives of US or multinational forces and the security of ongoing or future operations.*
>
> JP 3-61

5-50. Other sources will fill an information vacuum created by Army leaders not communicating effectively. Some sources may provide accurate information, other sources will provide misinformation, and threats will spread disinformation—false information intentionally designed to undermine Army credibility and operations. Timeliness matters, as perceptions and opinions begin to develop with the first information received, whether that information is accurate or not.

5-51. Informing relevant audiences by releasing information can have a powerful effect on friendly and threat perceptions and decision-making cycles. Army forces that release more timely and accurate relevant information to relevant audiences achieve an advantage by forcing opponents to react rather than act. The following are considerations for releasing timely and accurate information:

- Early release of information sets the pace and tone for solving a problem or creating a problem for the opponent.
- Early release of information presents facts accurately from the beginning rather than attempting to correct the record later.
- Uncontrolled release (or leaking) of information jeopardizes trust and credibility.
- Information released as early as possible from the most accurate source increases effectiveness.
- Information released prompts meaningful dialogue and public involvement.
- Information released corrects misinformation and counters disinformation.
- Information released builds public trust and confidence in the command.
- Information released prevents perceptions of scandal or cover-up.

5-52. Commanders and staffs must continuously assess the timing and content of changes to public affairs guidance, press releases, social media posts, and other activities to ensure that they do not provide OPSEC indicators that a threat could exploit. When OPSEC concerns preclude the complete release of information, commanders determine methods to control the timing and tempo of messaging to balance risk to the force with friendly credibility with designated relevant actors and audiences. Commanders release timely, factual, coordinated, and approved information and imagery as part of the inform information activity. Commanders release public information consistent with security restraints in DODI 5200.01 and the principles of information outlined in DODD 5122.05 listed in Figure 5-3.

5.1. It is the policy of the Department of Defense [DoD] to make available timely and accurate information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Requests for information from organizations and private citizens will be answered in a timely manner. In carrying out the policy, the following principles of information will apply:

a. Information will be made fully and readily available, consistent with the statutory requirements, unless its release is precluded by current and valid security classification. The provisions of Section 552 of Title 5, U.S.C., also known as the "Freedom of Information Act," will be supported in both letter and spirit.

b. A free flow of general and military information will be made available, without censorship or propaganda, to the Service members and their dependents.

c. Information will not be classified or otherwise withheld to protect the U.S. Government from criticism or embarrassment.

d. Information will be withheld only when disclosure would adversely affect national security, threaten the safety or privacy of Service members, or if otherwise authorized by statute or regulation.

e. The DoD's obligation to provide the public with information on its major programs may require detailed public affairs planning and coordination within the DoD and with other government agencies. The sole purpose of such activity is to expedite the flow of information to the public; propaganda has no place in DoD public affairs programs.

Figure 5-3. Department of Defense principles of information

COMPLIANCE WITH LAW AND POLICY

5-53. Leaders keep the inform information activity congruent and synchronized with the other four information activities. All information dissemination, regardless of the communicator or medium, is intended to either inform or influence. The intent of the communication guides the commander's decision to either inform or influence a particular audience. Lack of synchronized inform activities can damage the credibility of Army forces' actions and undermine OPSEC.

5-54. To help coordinate and de-conflict inform tasks and influence tasks, commanders and staffs maintain awareness of U.S. laws and statutes guiding the use of information throughout the competition continuum, whether in garrison or a forward position. The tasks associated with the inform activity do not try to force a particular point of view on audiences. Soldiers provide facts so various audiences can increase their understanding and then make their own decisions.

This page intentionally left blank.

Chapter 6
Influence

Fundamentally, all war is about changing human behavior. It is both a contest of wills and a contest of intellect between two or more sides in a conflict, with each trying to alter the behavior of the other side.

ADP 1-01

Chapter 6 begins with an overview of the influence information activity. A description of the tasks that contribute to influencing threats and other foreign audiences follows. The chapter concludes with considerations for effectively influencing the behavior of foreign relevant actors.

INFLUENCE OVERVIEW

6-1. 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.

6-2. 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.

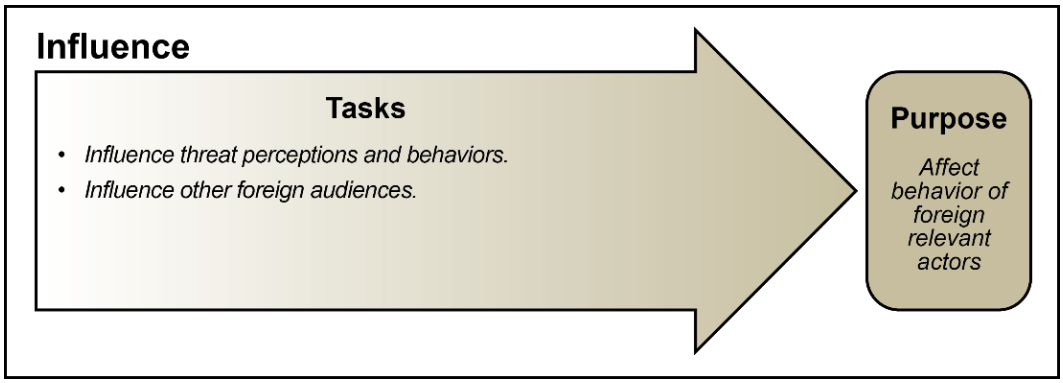


Figure 6-1. Tasks and purpose of the influence information activity

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

INFLUENCE THREAT PERCEPTION AND BEHAVIORS

6-3. 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.

6-4. 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—

- Conduct deception activities.
- Conduct military information support operations (MISO).

CONDUCT DECEPTION ACTIVITIES

> *If somebody's trailing you, make a circle, come back onto your own tracks, and ambush the folks that aim to ambush you.*
>
> *Standing Orders*, Rogers' Rangers

6-5. 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.

6-6. 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. The scope and scale of friendly deception activities are only limited by the resources available and the imagination of the commander and staff. All Army echelons should integrate deception into planning for operations. Well planned and executed deception achieves surprise.

A key deception principle for planners is Magruder's principle: it is far simpler to devise deception that closely aligns with a threat's existing beliefs than to change those beliefs.

6-7. Most leaders are familiar with the concept of deception. At very low tactical echelons, an infantry squad might use smoke to draw the attention of the enemy away for long enough to cross a street. At a slightly higher echelon, a platoon might conduct a feint to deceive the enemy about the location of the company commander's main attack for several minutes. Deception efforts at higher echelons require greater coordination because the number of actions required to successfully fool the threat increases. Friendly forces must provide enough indicators at the right time, in the right sequence, and at the right locations for the target of the deception to observe. This is because larger enemy forces have greater ability to discern the friendly deception effort because they have additional sensors and analysis capabilities in the same way friendly forces do. Army forces support or conduct three types of deception:

- Military deception (MILDEC).
- Tactical deception (TAC-D).
- Deception in support of operations security (DISO) (see Chapter 4 for more on DISO).

Support Military Deception

6-8. *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). Consisting of multiple actions executed over a span of time, most MILDEC is planned for and executed by the combatant command to create operational-level effects. Combatant command instructions add guidelines, policies, and processes that units must adhere to in their respective commands. MILDEC is a joint activity to which Army forces, as the primary land component, contribute to and support as directed. Army forces do not unilaterally conduct MILDEC. The Deception and the Invasion of the European Continent vignette provides an example of MILDEC at the theater level. (Refer to FM 3-13.4 for more information on Army support to MILDEC.)

Deception and the Invasion of the European Continent

Deception supported the success of OPERATION OVERLORD in the liberation of northwestern Europe in World War II. Deception troops created an entire fake Army group with an order of battle, cantonments, training sites, supply dumps, movements, embarkation points, shipping, and the corresponding electronic signal signatures. The fake army group's flamboyant commander, Lieutenant General George S. Patton, held press conferences, gave speeches, and conducted inspections that drew attention away from the location, disposition, and composition of the actual invasion force. Real German spies were captured and 'turned' into double agents, while dozens of fake ones volunteered their services—all controlled by the Allied deception team to feed the enemy's intelligence organization. This all-source intelligence picture confirmed the German high command's template that the Allies would stage in southwest England to assault the channel ports of northern France in the Pas de Calais. This was the reverse of the German plan to invade England earlier in the war.

The Allied air component supported the deception plan with a months-long interdiction campaign directly across the narrow channel from the fake army group—the most logical place to cross. The bombing was clearly meant to isolate the bulk of German forces positioned in the Pas de Calais region prior to the invasion. It also prevented counterattacking out against the real invasion in Normandy. Part of the air component also carefully mapped and measured German air and surface-search radars. In the weeks leading up to D-Day, many radars were destroyed in a calculated pattern that purposely left some intact in the Pas de Calais.

On the night of the invasion, the Allies began jamming some of the surviving German radars while leaving others to operate. Those German radar operators observed and reported a massive Allied invasion fleet approaching in the expected formation of minesweepers, landing craft, and gunfire support vessels. Shore observers also saw blinking signal lamps and heard the winches, chains, motors, and bullhorns of the amphibious fleet unloading in the darkness. Their reports corroborated the radar picture as did air defense units engaging aircraft dropping paratroopers inland from the beaches. What the Germans actually "saw" was an array of small Royal Navy patrol boats towing barges and blimps mounted with carefully sized radar reflectors and panels, equipped with programmed signal lamps, and fitted with loudspeakers playing the recorded sounds of earlier amphibious assaults and rehearsals. The paratroopers were dummies reinforced by a handful of heavily armed special operations teams carrying loudspeakers blaring drop-zone activities recorded on training jumps. These reports caused various German headquarters to begin positioning reserves and counterattack forces before the 'ghost fleet' retreated behind a smokescreen before dawn. Meanwhile, down the coast in Normandy, the actual airborne and amphibious landings gained several precious hours to secure and maintain a beachhead because of the delayed German reactions to them.

Conduct Tactical Deception

6-9. 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. The purpose of TAC-D is to—

- Gain the initiative.
- Mask vulnerabilities in friendly forces.
- Preserve combat power.

6-10. TAC-D by itself is not decisive, although it may be the main effort for a particular formation at some point during an operation. TAC-D effectively causes the enemy to squander time and resources on secondary activities long enough for friendly forces to achieve an exploitable advantage. Leaders conduct TAC-D at every echelon either with the resources they have or with assistance from their higher echelon. Integrating deception between echelons alters how the enemy views, analyzes, decides, and acts in response to friendly operations.

6-11. TAC-D includes the employment of both physical and technical *deception means*—methods, resources, and techniques that can be used to convey information to the deception target (JP 3-13.4). TAC-D means provide the signatures, associations, and profiles of friendly alleged activities to the enemy. Units employ as many deception means as possible within their capabilities to support TAC-D during all types of operations.

6-12. Physical deception means are resources, methods, and techniques used to convey information normally derived from direct observation or active sensors by the deception target. Most physical means also have technical signatures visible to sensors that collect scientifically or electronically. Planners typically evaluate physical deception means using characteristics such as shape, size, function, quantity, movement pattern, location, activity, and association with the surroundings. Examples might include—

- Movement of forces.
- Decoy equipment and devices.
- Security measures, such as camouflage and concealment.
- Tactical actions, such as feints and demonstrations.
- Reconnaissance, security, and surveillance activities.

6-13. Technical deception means may use equipment that manipulates electromagnetic, acoustic, or other forms of energy. They may be applied with corresponding physical means or alone to replicate something physical that is absent from visual contact. Planners integrate technical deception means with other technical activities that would occur during the operation. Higher headquarters may impose restrictions and limitations on the use of specific technical means for TAC-D. This is because they might interfere with an ongoing MILDEC or the effects of the technical means might extend into another friendly unit's assigned area. Examples of technical deception means might include—

- The establishment of communications networks and interactive transmissions that replicate a specific unit type, size, or activity.
- Organic capabilities that disrupt an enemy sensor or affect data transmission.

(Refer to FM 3-90 and FM 3-13.4 for more information on TAC-D.)

CONDUCT MILITARY INFORMATION SUPPORT OPERATIONS

6-14. *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.

6-15. 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.

6-16. Army PSYOP forces are trained and equipped to conduct MISO. MISO planners evaluate the psychological effects of military actions and advise commanders and staffs to maximize influence activities effectiveness and minimize adverse impact and unintended consequences. At the tactical level, Army PSYOP units provide support for Army corps and below. When directed, a tactical PSYOP group normally supports a corps. A tactical PSYOP battalion supports a division, with each of the PSYOP battalion's companies supporting selected brigades within the division. (Refer to FM 3-53 for more information on MISO.)

INFLUENCE OTHER FOREIGN AUDIENCES

> *Partnership develops trust, improves interoperability, and builds shared understanding as our Soldiers positively influence host-nation forces, leaders, populations, and other government agencies. This partnership produces enduring positive effects for regional stability and effective deterrence.*
>
> ADP 1

6-17. Within the framework of the combatant commander's campaign plan, Army forces seek to influence other foreign audiences. For one audience, efforts may be designed to increase mutual support and deepen existing relationships. For a different audience, influence efforts may focus on maintaining neutrality or changing from neutrality to supporting friendly positions.

6-18. During crises, Army forces seek to keep neutral audiences from inadvertently obstructing operations and allowing Army forces to focus their attention as much as possible on frustrating threat attempts to achieve goals and objectives. Should neutral audiences purposely interfere with operations, analysis can determine if the reasons are related to issues specific to the group's circumstances rather than a perceived alignment (and realignment) with a U.S. adversary. A calculated, appropriate U.S. response to ensure continued neutrality and reduction in interference helps avoid pushing a neutral audience to align with a threat. The continued neutrality of unaligned audiences is vital during fluid situations. Planners and advisors integrate the influence activities to ensure Army forces minimize mistakes and quickly mitigate the effects of any that occur. At the same time, it is vital to position Army units so they can rapidly and effectively exploit the effects of enemy actions and mistakes, such as collateral damage, civilian casualties, and human rights violations. In doing so, Army forces can increase the likelihood of swinging neutral audiences to the friendly position in dynamic environments.

6-19. When Army influence efforts maintain an audience's neutral stance, the audience is less likely to become an impediment to operations or become an adversary asset. If a neutral audience can be persuaded into becoming a friendly audience, then it becomes a potential impediment to an adversary and can increase the dilemmas it potentially faces. Primary tasks to influence other foreign audiences include—

- Conduct Soldier and leader engagement (SLE).
- Conduct MISO.
- Conduct civil affairs operations.

CONDUCT SOLDIER AND LEADER ENGAGEMENT

6-20. SLE is interpersonal interactions by Soldiers and leaders with populations in an area of operations. It can occur as an unplanned face-to-face encounter on the street or a scheduled meeting. Engagements can also occur via telephone calls, video teleconferences, or other audiovisual mediums. SLE supports both inform and influence activities.

6-21. Soldiers and leaders engage to provide information or to influence attitudes, perceptions, and behavior. Every interaction with local audiences, whether incidental to other activities or deliberately planned, has the potential to influence. Engagement provides a venue for building relationships, solving conflicts, conveying information, calming fears, and refuting rumors, lies, or incorrect information. Effectively integrating SLE into operations increases the potential for commanders to mitigate unintended consequences, counter adversary information activities, and increase local support for friendly forces and their collective mission. (Refer to ATP 3-13.5 for more information on SLE.)

CONDUCT MILITARY INFORMATION SUPPORT OPERATIONS

6-22. In addition to influencing threats, PSYOP units conduct MISO to influence other foreign audiences and populations. PSYOP units and staffs in Army headquarters help commanders align actions and messaging that influences these audiences to align them more closely with friendly goals and objectives. MISO help guide target audiences to make decisions that support the commander's objectives. In general, MISO focus on themes to influence foreign relevant actors that include—

- International legitimacy of U.S. and partner nation operations.
- Compliance with U.S. and partner nation operations that minimizes combatant and noncombatant casualties.
- Confidence in U.S. and partner nations' resolve.
- Commitment of the United States and partner nations to the security and stability of the region.
- Discrediting threat legitimacy and narrative.

(Refer to FM 3-53 for more information on MISO.)

CONDUCT CIVIL AFFAIRS OPERATIONS

6-23. Civil affairs operations are integrated with other influence activities to affect the behavior of foreign relevant actors. In this way, civil affairs operations act as the tangible connection for the commander to produce desired effects in the civil component of an operational environment (OE).

6-24. Assessment and analyses of civil engagement and civil reconnaissance provide commanders with situational understanding and feedback on the effectiveness of operations. When the influence effort of the commander requires offensive operations, civil affairs forces integrate mobilized civil networks into operations to increase civil security and civil control. This integration then impairs threat networks and degrades popular support for threat elements. In stabilization, civil affairs operations are most often synchronized with combat camera, MISO, public affairs operations, and foreign disclosure to align actions with messages and themes to create support for rule of law, local security forces, and legitimate authority.

6-25. Civil affairs forces assist commanders in influencing foreign audiences. Civil affairs units, from the company level through the Civil Affairs Command, establish civil-military operations centers, when required, to integrate, coordinate, and synchronize the efforts of Army forces with unified action partners, indigenous populations, and institutions. (Refer to FM 3-57 for more information on civil affairs operations.)

INFLUENCE CONSIDERATIONS

> *A force that uses information to deceive and confuse an opponent has an advantage. Using information to influence relevant actor behavior more effectively than an adversary or enemy is another information advantage.*
>
> FM 3-0

6-26. Influence activities align actions and messages with objectives to create desired, specific, and measurable changes in behavior that give commanders an advantage. Army leaders consider the following in planning and executing influence activities:

- Deliberate versus incidental influence.
- Language, regional, and cultural expertise.
- Authorities.

DELIBERATE VERSUS INCIDENTAL INFLUENCE

6-27. All warfighting functions contribute to the influence information activity because all military activities can influence threat behavior or the perceptions of a foreign audience. Regardless of the mission, Army forces consider the likely psychological impact of their operations and tasks on relevant actor perceptions, attitudes, and other drivers of behavior. The inherent informational aspects of operations produce cognitive effects on threats and other foreign relevant actors, including fear, anger, or confidence. These effects can erode, build, create, or negate other physical, human, and information advantages. Commanders and staffs prevent or

minimize the negative consequences of undesired or unplanned effects by considering how operations and actions affect an OE and influence the people in it. They then plan actions and communicate messages to elicit desired behaviors and support the national and operational narratives.

6-28. Planners and subject matter experts advise the commander about potential unplanned effects of operations and actions. Collateral damage, fratricide of allied or partner nation forces, or bad behavior by friendly forces all can have serious negative consequences that require commanders and staffs to have contingency plans and staff battle drills in place to mitigate. Plans and orders that include comprehensive risk assessments that address how things can go wrong, to include public affairs guidance, aid in mitigating any negative effects that operations may cause. Planning for influence activities early and anticipating foreign relevant actor actions and reactions helps shift influence efforts from reactive to proactive and keeps friendly forces on the offensive. Effectively anticipating actions and reactions by relevant actors requires a deliberate effort and dedicated staff to continuously monitor the environment.

LANGUAGE, REGIONAL, AND CULTURAL EXPERTISE

6-29. Leveraging information for the purpose of affecting behavior of relevant actors requires an understanding of the drivers of human behavior. These drivers include cultural aspects of the population, like language, arts, customs, and religion, as well as geographical considerations. Planners assess these aspects to understand threat and other foreign relevant actors and develop plans to influence them. Staffs identify and prioritize language, regional, and cultural capabilities required for their commanders to plan and execute missions effectively. Language, regional, and cultural subject matter experts enable operations when they provide a thorough understanding and appreciation of local populations, government officials, partners, and allies.

AUTHORITIES

6-30. Influence activities can be lethal or nonlethal, may be attributable or nonattributable, may require specific permissions and authorities, may be politically and time sensitive, and are governed by policies and statutes. In theaters where operations are transitioning from competition to crisis and armed conflict, commanders usually gain authorities to conduct influence tasks to reinforce the inherent informational aspects of operations by Army forces. For example, conducting a feint during large-scale combat operations is intended to influence threat decision making, but it requires no additional authorities beyond those articulated to the commander authorizing operations.

6-31. Influencing threats requires integration of influence considerations into the targeting process to ensure that staffs plan the most effective combination of lethal and nonlethal capabilities in context. Commanders and staffs employ as many legal and authorized potential means to influence their target audiences as required. Commanders and staffs must address authorities and approval in planning influence activities.

6-32. Authorities govern employment of joint and Army influence capabilities, to include civil affairs operations, MISO, MILDEC, cyberspace operations, and technical effects. U.S. and international law, DOD policies, status-of-forces agreements, treaty obligations, operation orders, and other binding documents may provide both authorities and limitations to conduct certain activities. (Commanders and staffs refer to GTA 33-01-004 as a starting point. For deception authorities and related references, refer to FM 3-13.4.)

This page intentionally left blank.

Chapter 7
Attack

Cyberspace and the [electromagnetic spectrum (EMS)] are critical for success in today's operational environment (OE). U.S. and adversary forces alike rely heavily on cyberspace and EMS-dependent technologies for command and control, information collection, situational understanding, and targeting.

FM 3-12

Chapter 7 begins with an overview of the attack information activity. A discussion of information attack methods follows. The chapter then describes the two attack tasks: degrade threat command and control (C2) and affect threat information warfare capabilities. The chapter concludes with attack considerations.

ATTACK OVERVIEW

7-1. 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.

7-2. 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.

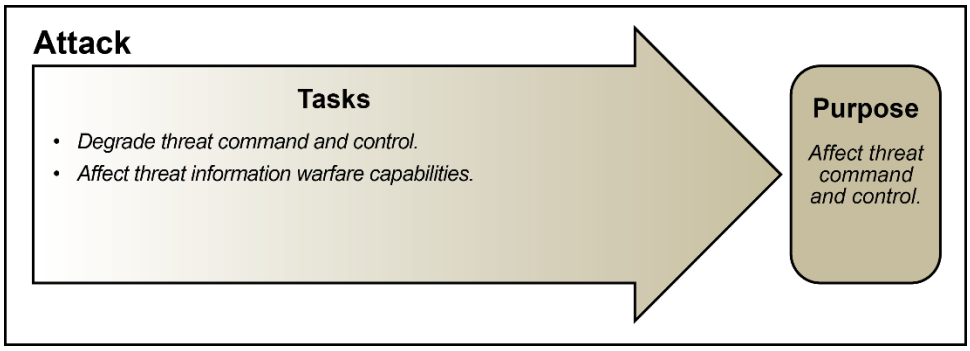


Figure 7-1. Task and purpose of the attack information activity

7-3. 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

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

7-4. 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.

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

7-5. 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.

7-6. 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.

7-7. 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. (Refer to ADP 3-19 for more information on fires. Refer to ADP 3-90 for offensive and defensive tactics of maneuver forces.)

ELECTROMAGNETIC ATTACK

7-8. 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.

7-9. *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.

7-10. Prior to conducting EA, Army commanders rely on organic and supporting intelligence and electromagnetic warfare (EW) forces to characterize threats in the EMS through electromagnetic reconnaissance and electromagnetic support activities. *Electromagnetic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-85). *Electromagnetic support* is the division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations (JP 3-85).

7-11. Army commanders conduct electromagnetic support within their areas of operations during operations across all the Army's strategic contexts. During competition below armed conflict, electromagnetic support can contribute substantially to the intelligence preparation of the operational environment (IPOE) and can help Army commanders form a baseline understanding of the EMS within their operational environments (OEs). During crisis and armed conflict, Army commanders leverage this baseline understanding of the EMS to conduct EA or request EA from higher echelons in support of operations. A significant percentage of EA support from higher echelons is likely to be joint, which requires understanding of the associated joint processes and timelines for employment. EA techniques can significantly reduce risk to forces and enable commanders to achieve episodic positions of relative advantage over threats by attacking or manipulating threat weapons, ISR systems, information systems, or networks.

7-12. Authorities for electromagnetic reconnaissance and electromagnetic support vary by situation and echelon and often intersect with intelligence collection authorities. As such, commanders and staffs ensure coordination among EW forces and assets and intelligence units and personnel. Authorities for EA are generally held at the combatant command level during competition below armed conflict and crisis. Combatant commanders may delegate EA control authority to subordinate joint force commanders. Army staffs coordinate for EA through the targeting process. (Refer to FM 3-12 for more information on EW.)

CYBERSPACE ATTACKS

7-13. *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. (Refer to FM 3-60 for more information on Army targeting.)

Cyberspace forces deliver cyberspace effects against threat networks, systems, and weapons. These effects enhance the Army's ability to conduct operations, reduce threat combat power, and project power across all domains.

7-14. 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.

7-15. 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.

7-16. Deny prevents access to, operation of, or availability of a target function by a specified level for a specified time. Cyberspace attacks deny the enemy's ability to access cyberspace by hindering hardware and software functionalities for a specific duration of time.

7-17. Disrupt completely but temporarily denies access to, or operation of, a target. Commanders can use cyberspace attacks that temporarily deny an enemy's ability to access cyberspace or communications links to disrupt decision making, the ability to organize formations, and the ability to conduct C2. Disruption effects in cyberspace are usually limited in duration.

7-18. Destroy completely and irreparably denies access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is rated according to the span of a conflict since threats can reconstitute many targets given enough time and resources. Commanders can use cyberspace attacks to destroy hardware and software beyond repair where replacement is required to restore system function. Destruction of enemy cyberspace capabilities can include irreversible corruption to system software causing loss of data and information. Destruction can also cause irreparable damage to hardware such as the computer processor, hard drive, or power supply on a system or systems on the enemy's network.

7-19. Manipulate, as an effect, is achieved by controlling or changing information, information systems, and networks in neutral or threat cyberspace to create physical denial effects. Manipulation uses deception, decoying, conditioning, spoofing, falsification, and other similar techniques. Manipulation changes data in a way that impacts enemy decision making. Manipulation can degrade a threat commander and staffs' effectiveness and decision making as they question the correctness of data coming from their systems. Friendly commanders can use cyberspace attacks to manipulate threat information or information systems in support of deception objectives.

7-20. During competition below armed conflict, cyberspace attack authorities are limited and require extensive national-level coordination and approvals. As situations progress into crisis and armed conflict, some authorities and approval levels may be delegated to combatant commanders or subordinate joint task force commanders. (Refer to FM 3-12 for more information on cyberspace attacks.)

SPACE OPERATIONS

7-21. 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. (See FM 3-14 for more information on space capabilities.)

7-22. 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. (See Chapter 4 for more information on defensive space operations.)

Offensive Space Operations

7-23. Offensive space operations are actions taken to negate attacks against U.S. and friendly space assets and threat freedom of action. The importance of space capabilities in military operations makes it crucial to be capable to negate enemy efforts interfering with or attacking U.S. and multinational space capabilities. Offensive space operations employ both reversible and nonreversible effects. 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—measures designed to mislead a threat by manipulation, distortion, or falsification of evidence or information into a system to induce the threat to react in a manner prejudicial to their interests.
- Disrupt—measures designed to temporarily impair threats use or access of a system, usually without physical damage to the affected system.

- Deny—measures designed to temporarily eliminate a threat's use, access, or operation of a system, usually without physical damage to the affected system.
- Degrade—measures designed to permanently impair (either partially or totally) the threat's use of a system, usually with some physical damage to the affected system.
- Destroy—measures designed to permanently eliminate the threat's use of a system, usually with physical damage to the affected system.

Navigation Warfare

7-24. 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. Navigation warfare may be implemented in a localized area or across all domains and mission areas. Navigation warfare is a consideration in all joint planning efforts. As it has strategic implications, it is incumbent upon the Army and joint forces to minimize unintended disruption to civil positioning, navigation, and timing services for noncombatants outside the area of operations.

7-25. The effects of navigation warfare on many systems are complex and may be limited in scope to a few miles or may cover an entire area of responsibility. Navigation warfare includes varying conditions from mild degradation to total Global Navigation Satellite System denial. It may even include Global Navigation Satellite System signal spoofing. The loss of this satellite signal may yield a significant decrease in the ability to conduct operations. The impact due to Global Navigation Satellite System interference—intentional or otherwise—goes far beyond handheld receiver devices. Loss of signal may impact C2, precision munitions, maneuver forces, aviation platforms, network timing protocol, and civil and commercial activities.

DEGRADE THREAT COMMAND AND CONTROL

> *Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals.*
>
> Sun Tzu

7-26. 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.

7-27. The protect information activity contributes to degrading threat C2 by denying the threat's access to friendly data and information as discussed in Chapter 4. The influence information activity contributes to degrading threat C2 by affecting threat perceptions as discussed in Chapter 6. The attack information activity degrades threat C2 by—

- Affecting the threat's understanding of an OE.
- Affecting threat networks and systems.

AFFECT THREAT UNDERSTANDING OF AN OPERATIONAL ENVIRONMENT

7-28. 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.

7-29. 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.

AFFECT THREAT NETWORKS AND SYSTEMS

As a defeat mechanism, *disintegrate* means to disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations (FM 3-0).

7-30. 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 within threat networks and systems (C2, ISR, and fires) for disruption, destruction, or manipulation.

7-31. When exploited for intelligence purposes, threat networks and systems can provide significant strategic insight as well as operational warnings. As commanders and staffs plan and execute actions to degrade these networks and systems, they weigh the relative operational value of degrading these systems against the potential loss of intelligence. For instance, if an Army force is collecting key warnings on enemy intent from a radio channel, a commander may forego jamming that radio channel during an operation even though such jamming might hinder enemy maneuver. Conversely, the commander may determine that such jamming will provide a great enough operational advantage to Army forces that it will offset the loss in intelligence insight into enemy intentions.

AFFECT THREAT INFORMATION WARFARE CAPABILITIES

7-32. Adversaries and enemies have active and effective information warfare capabilities. Many of the information activities discussed in previous chapters are intended to reduce the effectiveness of threat information warfare capabilities and the impact of threat information warfare on Army forces and operations. While it may be preferable for Army commanders to be able to prevent or mitigate the effects of these threat actions, it is by no means ensured that prevention or mitigation is possible in all instances. In cases where threat actors have decided to conduct information warfare attacks against Army and friendly forces and those attacks are imminent or ongoing, Army commanders may need to degrade or defeat threat information warfare capabilities directly.

7-33. To degrade or defeat threat information warfare capabilities, Army forces may employ the same types of capabilities and use methods like those used in other Army information activities. The type of threat information warfare capability, as well as the strategic context of the attack, may narrow or broaden the list of appropriate military capabilities employed in response. For instance, an appropriate response to a threat cyberspace attack on an Army logistics system during competition below armed conflict might be limited to a cyberspace security response coordinated through joint and whole of government channels. However, the

same type of cyberspace attack during crisis or armed conflict might warrant employment of Army cyberspace attack capabilities, EW capabilities, or a physical strike on threat cyberspace capabilities.

7-34. A technical or physical attack on threat information warfare capabilities might not always be required to functionally defeat the threat. For instance, friendly forces could diminish the impact of a threat disinformation campaign by blocking or removing the network nodes and communications systems used to promulgate it. Friendly forces could also achieve a similar effect by exposing the existence of the disinformation campaign and those who promulgate it. In this scenario, commanders would leverage the activities and capabilities associated with other information activities and tasks, such as public affairs and military information support operations (MISO). Exposing false threat narratives with truthful information, to include the authorized released of intelligence and imagery, directly attacks threat legitimacy. Coordinated at the strategic and operational levels, Army tactical commanders support these efforts as directed, to include providing intelligence, information, and imagery for release by higher authorities.

ATTACK CONSIDERATIONS

7-35. The tasks that compose the attack information activity target threat data and information, information systems, communications, and information warfare capabilities. To be successful, Army leaders consider the following in planning and executing attack tasks:

- Timelines for preparatory activities.
- Precision and scalability.

TIMELINES FOR PREPARATORY ACTIVITIES

7-36. Effective attacks require that commanders and staffs identify threat targets early during IPOE and continuously refine those targets throughout the operations process. In general, the more precise the required effect is, the more time it will take to analyze the target and prepare capabilities to create the effect. For example, coordinating for space and cyberspace capabilities often requires coordination and approval through the headquarters of several Army echelons, the combatant command headquarters, then to a supporting combatant command.

7-37. Effective units continuously conduct many preparatory activities during competition below armed conflict and through crisis and armed conflict. These activities include intelligence operations, cyberspace reconnaissance, electromagnetic reconnaissance, target audience analysis, and target development. During competition below armed conflict, units continuously conduct most of these preparatory activities at echelons above division. During crisis and armed conflict, units below corps may use organic assets and capabilities to continue these preparatory activities. However, units below corps will likely still rely on support from echelons above division to conduct cyberspace reconnaissance and augment division and below organic intelligence and EW capabilities. This reliance requires staffs to continuously coordinate requirements with higher echelon units throughout the operations process.

PRECISION AND SCALABILITY

7-38. Threat C2 systems present attractive targets. When friendly forces successfully attack, they render ineffective a large number of threat forces and weapon systems without directly attacking each individual system. When threat commanders cannot issue orders or direct their forces, it reduces the effectiveness of many or all that threat's capabilities. However, the fact that these C2 systems are so critical means that Army commanders must consider threat reactions and counteractions when attacking threat C2 systems.

7-39. To minimize the risk of unintended escalation during competition below armed conflict or in crisis, joint force commanders consider the precision and scalability of methods they select to attack threat C2 systems. Cyberspace attack, EW, space, and technical effects capabilities may vary widely in their ability to precisely affect a specific system or in their ability to scale effects on that system.

7-40. During armed conflict, Army commanders consider using lethal effects to degrade or destroy threat C2 systems. Delivering lethal effects through fires may be timelier than nonlethal technical effects, but it may also result in more collateral damage. Staffs develop and provide assessments of these tradeoffs to commanders during the targeting process.

This page intentionally left blank.

Chapter 8
Integration

Achieving information advantages is a commander-driven, combined arms activity that employs capabilities from every warfighting function.

FM 3-0

This chapter begins with an overview of joint and multinational information advantage. A discussion of the relationship of Army information activities and the information joint function follows. The chapter then describes the relationship, planning responsibilities, and integration of Army information activities during operations. The chapter concludes with training and educating the force on information advantage.

JOINT AND MULTINATIONAL INFORMATION ADVANTAGE

8-1. 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.)

INFORMATION JOINT FUNCTION

Joint force commanders use the information joint function to create and exploit information advantages to achieve objectives across the competition continuum.

8-2. 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 information joint function provides the intellectual organization of the tasks, subtasks, and outcomes used to create and exploit information advantages as shown in Figure 8-1 on page 8-2. The primary joint tasks are—

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

8-3. Outcomes of the understand task include identification of threats, vulnerabilities, and opportunities in the information environment and a better understanding of which relevant audience's drivers of behavior to affect to achieve objectives. Outcomes of the support task include facilitating shared understanding across the joint force; protecting friendly information, information networks, and information systems; and protecting joint force morale and will. Outcomes of the leverage task enable the joint force commander to inform audiences; influence foreign relevant actors; and attack and exploit information, information networks, and information systems. (Refer to JP 3-04 for a detailed discussion of the information joint function.)

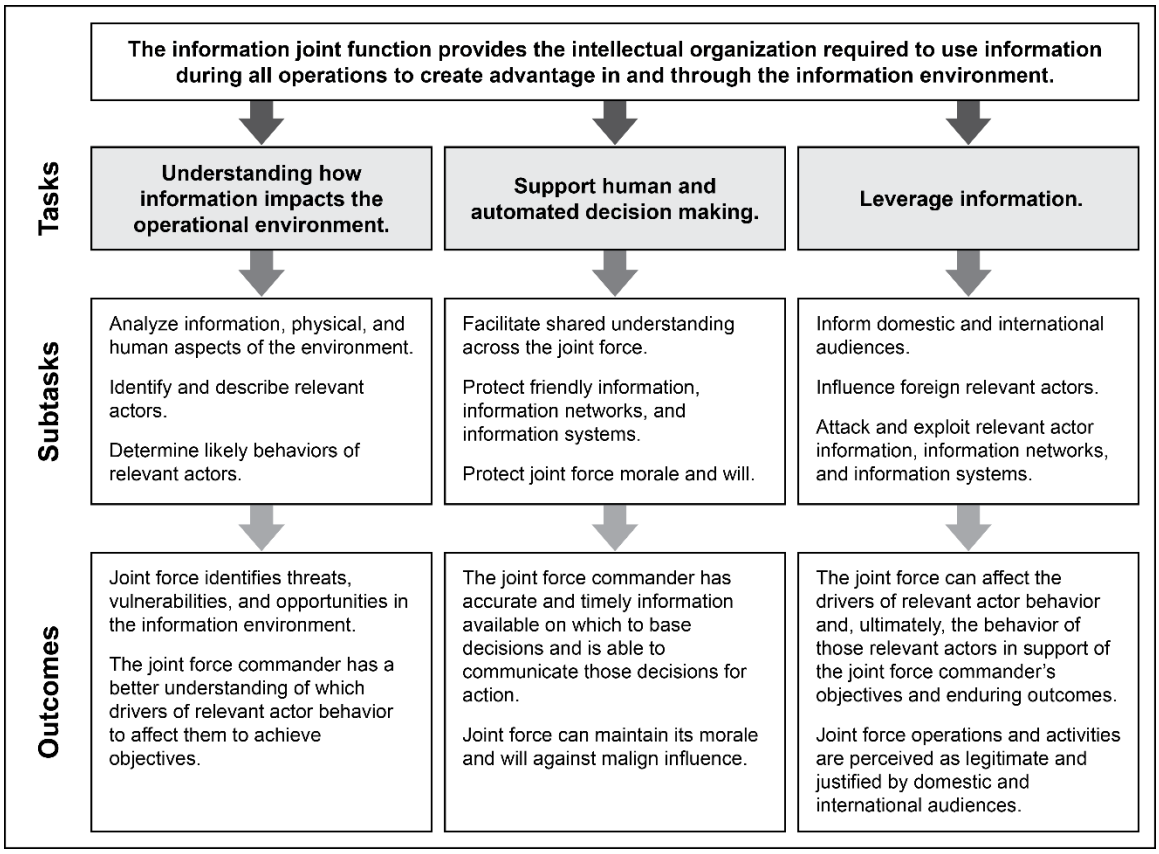


Figure 8-1. Tasks and outcomes of the information joint function

JOINT INFORMATION ADVANTAGE

8-4. 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

8-5. 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 them to act in ways to affect the joint force. Whether or not commanders consider this during planning, friendly activities do impact an OE and resonate in the operational area and potentially other operational areas.

8-6. Joint force commanders employ Army forces to achieve objectives while understanding the potential informational effects Army operations can have on an OE. Joint force commanders communicate to the senior Army headquarters how they intend to leverage these effects to accomplish various tasks, achieve joint information objectives, or support OIE. Army commanders nest the tasks and purpose they assign to

subordinates to support the joint force commander's intent throughout the operations process. (See paragraph 1-7 for a detailed discussion of inherent informational aspects of operations.)

Operations in the Information Environment

8-7. *Operations in the information environment* are military actions involving the integrated employment of multiple information forces to affect drivers of behavior (JP 3-04). OIE affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems.

8-8. The combatant commander has responsibility for establishing processes and procedures to deconflict and synchronize OIE to achieve unified action. Combatant commanders apply strategic guidance related to OIE during planning, through preparation, and throughout execution. The joint force commander may establish various teams and cells, to include the information cross-functional team, media operations center, key leader engagement cell, information management cell, or others as required. The joint staff typically coordinates and deconflicts military activities such as electromagnetic attack (EA), cyberspace attack, offensive space operations, and military information support operations (MISO) within the joint targeting process.

8-9. Joint force commanders may choose to create a task force for the integrated employment of specialized capabilities required to conduct OIE. Joint doctrine refers to this type of task force as an OIE unit. OIE units are composed of a headquarters and information forces—those Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the information environment. Information forces include psychological operations (PSYOP), civil affairs, electromagnetic warfare (EW), cyberspace, public affairs, information operations, and space forces. Information forces are provided by the Services and made available to the joint force through the request for forces process.

Note. Although JP 3-04 rescinded joint information operations as defined and practiced, the Department of the Army retains the term *information operations* to refer to select units, such as 1st Information Operations Command and personnel assigned to Functional Area 30 (Information Operations). NATO's AJP-10.1 retains the term and practice of information operations.

MULTINATIONAL CONSIDERATIONS

> *The behaviour-centric approach is the primary doctrinal tenet that focuses planning and execution of activity to appropriately inform and influence the attitudes and behaviour of audiences to attain the end state.*
>
> AJP-10.1

8-10. Army forces integrate their information activities with multinational partners. *Multinational operations* is a collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance (JP 3-16). Multinational partners may contribute different or additional information forces to an operation. Each nation's force has unique capabilities and often operates with different authorities to employ key information capabilities in the various domains of an OE. Army forces anticipate and plan for most operations being multinational.

8-11. Multinational operations can present unique integration challenges. The differences between the various nations can affect how successfully a multinational force enables, protects, informs, influences, or attacks threat information capabilities to achieve objectives. Situational understanding affects how various commanders employ their assigned forces in support of achieving objectives. For example, if a multinational commander cannot anticipate and adjust for the various legal and regulatory restrictions for sharing classified information with allies and partners, subordinate commanders will probably understand the situation differently. Multinational national challenges include—

- National caveats on the use of respective forces.
- Doctrinal differences.

- Cultural and language barriers.
- Communications and procedural interoperability.
- Sharing of information and intelligence.
- Equipment interoperability limitations.
- Rules of engagement.

8-12. To help overcome these challenges, multinational commanders develop procedures to speed the exchange of relevant information to other nations, develop a standard lexicon that supports situational understanding of information and information capabilities, and ensure the staff is trained not to overclassify information. Participating in theater security cooperation activities helps Army forces appreciate partner capabilities and improves interoperability prior to conflict. (Refer to NATO's AJP-10.1 for allied joint doctrine on information operations. Refer to FM 3-13 for more information on multinational operations.)

ARMY FORCES AND THE INFORMATION JOINT FUNCTION

8-13. Although the Army's information framework differs from the joint information function, they both have the same goal: to create relative advantages that commanders can use to achieve objectives. To help understand the relationship between the Army's information framework and the information joint function, Figure 8-2 illustrates how Army information activities align with the joint information subtasks. (Refer to JP 3-04 for details on joint information subtasks.)

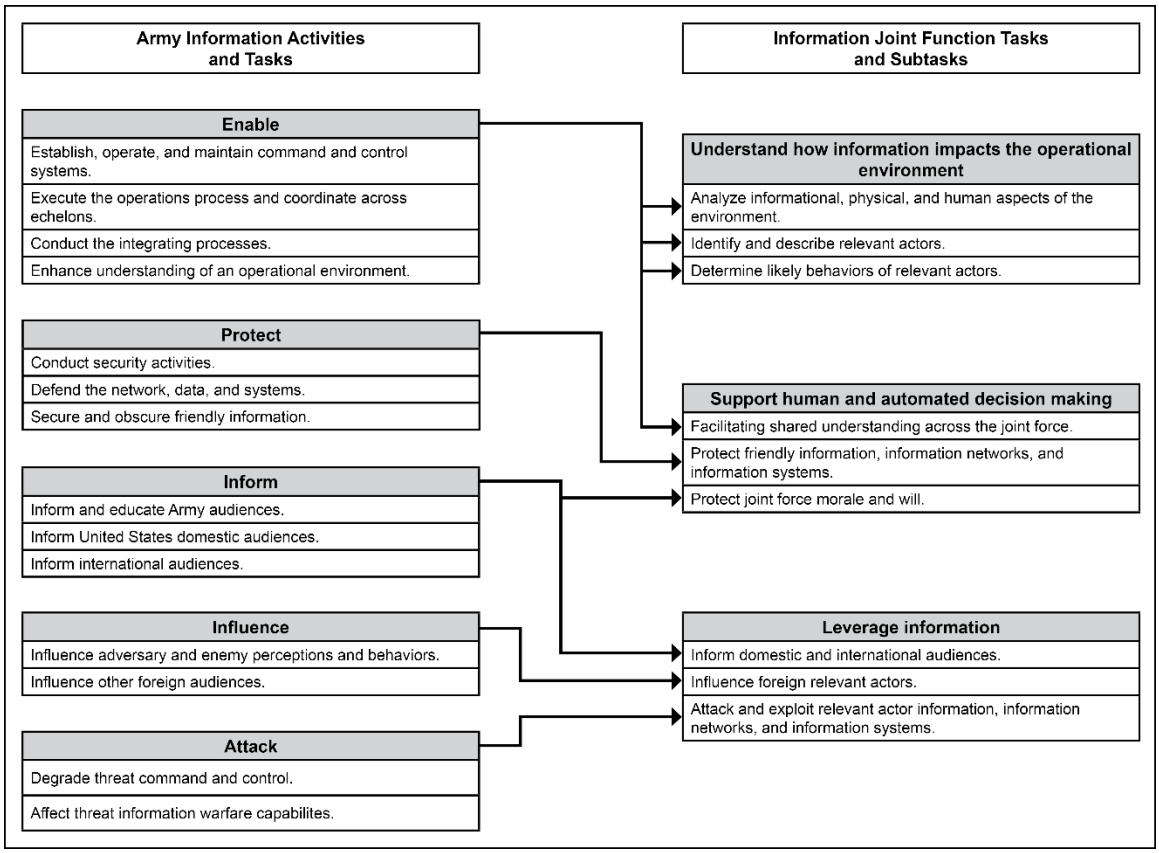


Figure 8-2. Army information activities relationship to joint subtasks

8-14. Army forces use joint information doctrine when interacting with the higher joint headquarters but communicate with subordinate Army forces using Army doctrinal terms. Army information activities and tasks provide specificity while remaining aligned with the broader joint information tasks. The following echelons and types of units require a detailed understanding of both Army and joint information doctrine:

- Headquarters likely to be designated a joint task force.
- Theater armies.
- Headquarters likely to be designated as a land component command.
- Headquarters likely to be designated as a joint force land component command.
- Civil affairs units.
- Cyber units.
- EW units.
- Information operations units.
- Intelligence units.
- PSYOP units.
- Public affairs units.
- Space operations units.
- Special forces units.
- Security force assistance units.
- Digital liaison detachments.

ARMY INFORMATION ACTIVITIES DURING OPERATIONS

8-15. Army commanders, supported by their staffs, integrate information activities into their concept of operations to create and exploit information advantages. Integration is the arrangement of military forces and their actions to create a force that operates by engaging as a whole. Subordinate commanders ensure they integrate their information activities with the higher commander's intent and concept of operations. Integration occurs at all echelons, with lower echelons relying on both the analytic capabilities, information capabilities, and experience of higher headquarters commanders and staffs to anticipate information requirements and synchronize the execution of tasks.

INFORMATION ACTIVITIES AND THE OPERATIONS PROCESS

8-16. To gain information advantages, the commander, supported by the staff, integrates information activities throughout the operations process. The operations process (plan, prepare, execute, and assess) is the major C2 activity performed during operations. Because nearly all military capabilities and actions can contribute to gaining or exploiting information advantages, the entire staff assists the commander in integrating information tasks during planning, preparation, execution, and assessment. The staff accomplishes this in the integrating cells (current operations, future operations, and plans); in working groups and boards; and through the integrating processes.

Planning

8-17. 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. (Refer to FM 5-0 for a detailed description of the military decision-making process and other planning processes used by Army staffs.) As part of planning, the staff should at a minimum—

- Consider how the informational considerations affect the warfighting functions' ability to contribute to mission accomplishment.
- Analyze the interaction of factors within the physical and human dimensions with those of the information dimension of an OE in the specific context of the operation being conducted.
- Identify unique employment considerations for information capabilities executing specific information tasks, such as MISO, offensive cyberspace operations, space operations, and EA.
- Anticipate and assess both the risk to the mission resulting from impacts and the signature resulting from unintentional inherent informational aspects of Army operations.
- Identify information tasks directed by higher headquarters required to accomplish the mission.

- Identify and consider ongoing or planned unified action partner information activities within an OE.
- Consider gaps in language, regional, cultural, or technical expertise required to understand an OE.
- Recognize potential undesirable information effects of friendly activities.
- Develop an assessment plan to monitor effects of information activities, including effects of other units, to enable adjustments as required.
- Identify required capabilities not organic to assigned forces and secure them from higher headquarters via contract or other means.
- Identify existing and required authorities needed to conduct information activities.

Preparing

8-18. *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.

8-19. Preparation helps the force transition from planning to execution. Army forces typically begin to prepare during planning and continue preparation until execution. 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.

8-20. 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.

8-21. 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.

Executing

8-22. *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.

8-23. The current operations integrating cell assesses the effects and performance of information activities during execution. Current operations integrating cell members compare the current situation to the plan as an operation progresses. These members modify information tasks as necessary to accomplish the mission. Common staff tasks related to executing information tasks include the following:

- Monitor information tasks and tasks intended to have effects in the information dimension.
- Nominate targets for attack.
- Update running estimates.
- Monitor networks and electromagnetic emissions.
- Deconflict information activities.
- Synchronize information tasks across warfighting functions with lower, higher, and adjacent headquarters, and with outside agencies when appropriate.

Assessing

8-24. 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.

8-25. Assessing information activities is an integral part of knowing if friendly forces have achieved various information advantages. Assessing information activities requires—

- Developing the assessment approach (planning).
- Developing and publishing the assessment plan (planning).
- Collecting information and intelligence (planning, preparation, and execution).
- Analyzing information and intelligence (planning, preparation, and execution).
- Communicating feedback and recommendations (planning, preparation, and execution).
- Adapting plans or operations (planning, preparation, and execution).

8-26. Commanders typically use two types of indicators to assess. One type of indicator is referred to as a measure of performance. Units use a measure of performance to measure a friendly action tied to task accomplishment. It answers the question: Was the task accomplished? The echelon executing the information task is typically best able to assess whether it executed a specific task successfully. Another type of indicator is referred to as a measure of effectiveness. Units use measures of effectiveness to measure change in a system or in target behavior over time to assess if a force is achieving objectives or attaining the end state. Measures of effectiveness help to answer: Are the information activities and tasks Army forces execute contributing to achieving an objective or the end state? Because achieving objectives typically requires different units executing a variety of tasks, the echelon assigning the tasks can typically best measure effectiveness. (Refer to ATP 5-0.3 for further discussions on each step of the assessment process. Refer to JP 3-04 for more detail on assessing information advantage.)

RESPONSIBILITIES

8-27. Commanders and staffs at all echelons integrate information activities and tasks into all operations. Creating information advantages requires a cross-functional approach synchronized and coordinated in functional and integrating cells using the operations process, the subordinate integrating processes, and working groups and boards. Commanders, staffs, and Soldiers at all levels have a responsibility to achieve and preserve information advantages.

Commander Responsibilities

8-28. Commanders are responsible for creating and exploiting information advantages throughout the operation. They do this by providing their staff and subordinate leaders with direction and guidance for planning, preparing, and executing information activities and tasks. They understand the relationship among human, information, and physical advantages in the context of their mission and assigned area of operations. Based on their situational understanding and assessment, commanders adjust information tasks as required to achieve objectives and accomplish the mission.

8-29. Commanders, supported by their staffs, integrate information activities internally, vertically, horizontally, and externally. Commanders integrate information activities internally within their command posts (CPs) to enhance their understanding of an OE, to include how to leverage the inherent informational aspects of their units to support mission accomplishment. Internal integration informs the commander on how successful vertical, horizontal, and external integration of the information activities can contribute to the mission.

8-30. Commanders integrate vertically when they nest their operations in the operational narrative, support higher headquarters information objectives, and fulfill information requirements. They accomplish this by receiving, analyzing, and understanding the objectives assigned by the higher headquarters and then by providing the required authorities and capabilities to subordinate commanders to perform specific information tasks.

8-31. Commanders integrate horizontally by maintaining situational awareness of operations that adjacent units plan and execute. If a commander anticipates that certain information activities will affect an adjacent unit's operations, that commander coordinates with the adjacent commander to deconflict or ensure the effects are complementary. Commanders likewise anticipate the information effects an adjacent unit's activities will have on their operations and coordinate accordingly. Commanders direct subordinate units to coordinate with adjacent units when creating an information effect requires actions by more than one unit.

8-32. Commanders integrate externally when appropriate and may be granted direct liaison authority by their higher headquarters. Integrating information activities with allies, partners, interagency organizations, and various audiences can enhance the effectiveness of a unit's operations while also mitigating negative or hostile information effects. Commanders always take operations security (OPSEC) and unified action partner caveats into consideration when conducting external integration. The exchange of liaisons is a best practice for coordination and is particularly important when adjacent units do not share a parent unit.

8-33. Commanders use commander's critical information requirements (CCIRs) to help drive decisions critical to creating information advantages. They use priority intelligence requirements (PIRs) and friendly force information requirements for collecting pertinent information needed to make those decisions.

8-34. Commanders emphasize the significance of the timeliness of data and information because the speed with which commanders make decisions is vital to creating information advantages. Commanders and staffs use decision tools such as synchronization matrixes, decision support matrixes, and decision support templates to coordinate decisions in time and space. (Refer to FM 5-0 for more information on decision support tools.) Ultimately, commanders establish and communicate their priorities to ensure they have the right data at the right time to support timely decision making.

Common Staff Responsibilities

8-35. The staff has common responsibilities for supporting information advantage. Staff members have specific duties and responsibilities associated with their areas of expertise, and they must be ready to advise the commander and other senior leaders regarding information pertaining to those areas of expertise.

Regardless of their career field or specialty, all staffs share a common set of information advantage responsibilities:

- Managing information.
- Protecting information.
- Developing running estimates.
- Updating running estimates.
- Completing research and analysis.
- Participating in the integrating processes.
- Developing and submitting information requirements.
- Responding to requests for information.

Soldier Responsibilities

8-36. Every Soldier has information advantage responsibilities. Information tasks are not just conducted by information units or specialists. All Soldiers collect, protect, and create information during operations. Each Soldier's approach to information must reflect this reality every day, at every level, in all things.

8-37. The fight for information is continuous. Whether in garrison or deployed for large-scale combat, Soldiers must be cognizant of the information the threat can collect on them, the information the threat is likely collecting, and the information which they must protect. Soldiers establish and maintain information advantages or run the risk of ceding the advantage to the threat. Effective Soldiers understand their responsibilities related to information advantage and the ways that fulfilling their responsibilities correlate to having human and physical advantages. Some responsibilities common to all Soldiers:

- Generate relevant information through accurate reporting.
- Understand the larger intent of the operation.
- Carry the U.S. message into the operational area.
- Maintain OPSEC.
- Be aware of threat information manipulation methods.
- Obscure friendly actions and protect sensitive capabilities of interest from threat collection.
- Be aware of the message their actions convey on and off duty.

Information Activity Lead Responsibilities

8-38. Various staff members have key responsibilities to synchronize and integrate information activities. Information activity leads are the primary members of the staff responsible to the commander for integrating the five information activities. Information activity leads coordinate with other staff members responsible for various tasks and subtasks Army forces enable each information activity. Typically, the following staff members lead the information activities:

- Chief of staff (enable information activity).
- Chief of protection (protect information activity).
- Public affairs officer (inform information activity).
- Assistant chief of staff, operations (influence and attack information activity).
- Chief of fires or deputy fire support coordinator (attack information activity).

Note. Headquarters at brigade and below are not manned with all the staff officers discussed in paragraphs 8-39 through 8-87. The subordinate headquarters relies on the initial analysis conducted by the higher headquarters staff, refines that analysis based upon their mission, and submits request for information to mitigate information gaps. The executive officer recommends to the commander which staff officer to assign responsibility for coordinating specific information activities when required.

Chief of Staff

8-39. The chief of staff is the commander's principal staff officer. Commanders normally delegate executive management authority to the chief of staff. The chief of staff is normally empowered to make certain decisions to retain agility in decision making, to include coordinating the staff and directing staff information advantage efforts. When authorized, the chief of staff can represent the commander and coordinate liaison exchanges with higher echelon, lower and adjacent units, and other organizations.

8-40. Experience and delegated authority uniquely position the chief of staff to best integrate the various tasks and subtasks associated with the enable information activities. The chief of staff develops and leads the staff. The chief of staff establishes and monitors the headquarters battle rhythm and nests it with higher echelon and subordinate headquarters battle rhythms for effective planning support, decision making, and other critical functions. By establishing and managing staff processes and procedures, understanding staff capacity, setting priorities, and managing knowledge and information, the chief of staff integrates and synchronizes staff tasks associated with enable information activities.

Assistant Chief of Staff, Operations

8-41. The assistant chief of staff, operations, ensures warfighting function integration and synchronization across the planning horizons in current operations, future operations, and plans integrating cells. This includes ensuring that staffs integrate all information activities and associated tasks into the concept of operations. Additionally, the G-3 is the lead for integrating the influence and the attack information activities into operations. Assisted by the G-39 and chief of fires, the G-3 integrates the influence and attack tasks in the current operations, future operations, and plans cells.

8-42. Army forces influence in two ways: through the inherent informational effects of Army operations and through employment of specific capabilities to execute information tasks to support operations. During the operations process, the G-3 ensures that subordinate forces conduct operations to maximize their inherent informational effects. The G-3 also ensures that specific units and staff sections execute information tasks that enhance mission accomplishment.

Chief of Protection

8-43. The chief of protection is the principal staff officer responsible for the protection warfighting function for divisions, corps, and theater armies. At echelons below division, the S-3 typically coordinates the protection function. The protection warfighting function includes tasks to protect friendly information. The chief of protection integrates tasks required to minimize physical signatures, security activity tasks, and tasks required to protect networks, data, and information systems.

8-44. The chief of protection leads the protection working group. The protection working group includes members from across the staff. This cross-functional group integrates and synchronizes capabilities and resources to preserve combat power, including information, from threats and hazards. The protection working group contributes to all aspects of the operations process and integrating processes. (Refer to ADP 3-37 and FM 6-0 for more information on protection doctrine and the protection working group.)

Public Affairs Officer

8-45. The public affairs officer (PAO) is the primary staff member responsible to the commander for coordinating and synchronizing the various tasks associated with the inform information activity. The PAO contributes communication expertise in aspects of informing and publicly communicating with a variety of audiences. The PAO provides recommendations to the commander on developing messaging that reinforces higher echelons informing activities and other messaging that supports the commander's assigned mission.

8-46. PAOs have specialized training that enables them to analyze specific informational considerations of an OE and assist the commander and staff in understanding what inform activity tasks best support the mission. The PAO is a continuous participant during the entire operations process, playing an active role in several working groups that support planning, preparation, and execution. PAOs continually assess the impact of activities related to informing various audiences and recommend adjustments to planned inform tasks to better support the mission. Headquarters at brigade and below are not assigned a PAO. Commanders at brigade and below appoint a unit public affairs representative to perform some PAO duties.

INTEGRATION OF THE INFORMATION ACTIVITIES

8-47. 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. (Refer to ATP 6-0.5 for additional information on functional and integrating cells.)

Table 8-1. Information activity and task leads

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		

8-48. 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 to support cross-functional staff integration. (Refer to FM 6-0 for additional information about boards, working groups, and planning teams.)

8-49. 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. If the staff judge advocate determines the commander lacks the required authorities, then the staff judge advocate recommends the specific authorities to request to allow execution of the required information tasks.

8-50. 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. The information task leads use the working groups to synchronize contributions from multiple CP cells and provide analysis, coordination, and recommendations on how the unit can leverage information activities to gain information advantages.

Enable Information Activity

8-51. The chief of staff is the lead for enable information activities. The enable activity has four corresponding information tasks that support decision making and the conduct of operations. The G-6 and knowledge management officer (KMO) lead the first information task: establish, operate, and maintain C2 systems. The G-3 leads the second information task: execute the operations process and coordinate across echelons. The third information task—conduct integrating processes—is led by the integrating process leads: G-2, G-3, chiefs of fires, chief of protection, and KMO. The G-2 leads the fourth task: enhance understanding of an OE.

Establish, Operate, and Maintain Command and Control Systems

8-52. The chief of staff, supported by the staff, establishes the CP, network, and processes that, together with the staff, compose the C2 system. The KMO is the principal task lead who advises the commander on how to maximize the flow of information and knowledge generation via the C2 system. The entire staff supports this task with the G-6 offering critical expertise concerning the network and communications. The KMO ensures that the staff and subordinate units understand knowledge management processes and procedures. Units often establish standard operating procedures that direct how the C2 system manages knowledge.

8-53. The signal staff supports the knowledge management process by configuring the network to best support the C2 system given the informational considerations of an OE. Most units establish standard operating procedures that describe the procedures for organizing their C2 network. During the planning process, the signal staff makes recommendations to adjust network procedures as required to support operations in an area of operations. The signal staff participates in the knowledge management working group and proposes adjustments to the network based on changing information requirements and threat actions.

Execute the Operations Process and Coordinate Across Echelons

8-54. The G-3 is the commander's principal staff officer for coordinating and synchronizing operations in their entirety. The G-3 ensures that all actions, to include information tasks, are integrated and synchronized operations through the operations process. The G-3 accomplishes this by—

- Ensuring warfighting function integration and synchronization across the planning horizons in current operations, future operations, and plans integrating cells.
- Authenticating all plans and orders for the commander to ensure units synchronize all functions in time, space, and purpose in accordance with the commander's intent and planning guidance.
- Understanding adjacent unit assigned objectives and coordinating with adjacent units to ensure operations complement accomplishing higher echelons objectives.

Conduct the Integrating Processes

8-55. Successfully executing the operations process requires Army forces to conduct a variety of processes designed to enhance situational understanding, make better decisions, and synchronize activities. Every process must occur in concert with other processes to satisfy a specific information or knowledge requirement. Several staff officers lead a specific integrating process, to include:

- Intelligence preparations of the OE (G-2).
- Information collection (G-3).
- Targeting (chief of fires).

- Risk management (chief of protection).
- KMO.

8-56. The chief of staff ensures the integrating processes generate the required understanding for the commander and staff to successfully execute the operations process. The KMO is coordinated by the chief of staff and is the staff member responsible to the commander for synchronizing the integrating processes into the operations process. During the operations process, the KMO participates in planning. The KMO then subsequently makes recommendations to the chief of staff during preparation and execution to adjust knowledge management procedures, including changes to the battle rhythm. The knowledge management working group, led by the KMO and chaired by the chief of staff, is the primary venue to account for changes to the informational and knowledge requirements of the headquarters and subordinate units. This working group recommends appropriate adjustments to C2 processes to maintain efficient information flow throughout the C2 system. When appropriately synchronized, people, processes, and tools of the C2 system work together to achieve shared understanding.

Enhance Understanding of an Operational Environment

8-57. The G-2, assisted by the staff, leads this activity. Enhancing understanding of an OE begins during planning and then occurs throughout the operations process. Commanders and staffs seek to build and maintain situational understanding throughout the operations process. Several tasks assist commanders and staffs in understanding how information and information capabilities impact operations, to include—

- Analyzing the operational and mission variables.
- Identifying and describing relevant actors.
- Identifying likely behavior of relevant actors.

8-58. Intelligence preparation of the operational environment (IPOE) is the integrating process led by the intelligence staff that allows commanders and staffs to take a holistic approach to analyzing an OE. The staff's contribution to IPOE is a critical component to enhance understanding of an OE. Understanding the impact of informational considerations on OEs is inherent in IPOE and assists the staff understand how various aspects of the human, information, and physical dimensions will affect Army operations. Because the effects of Army operations on the dimensions are dynamic, the staff must continually conduct IPOE and adjust running estimates accordingly. IPOE is critical in developing friendly courses of action, developing decision points for the commander, and planning information collection and targeting operations. (Refer to ATP 2-01.3 for more information on IPOE.)

Protect Information Activity

8-59. The chief of protection, assisted by the OPSEC officer, G-3, and G-6, is the lead for protect information activities. The protect activity has three corresponding information tasks. The first information task, secure and obscure friendly information, is led by the OPSEC officer. The second information task, conduct security activities, is led by the G-3. The third information task, defend the network, data, and systems, is led by the G-6.

Secure and Obscure Friendly Information

8-60. The OPSEC officer, assisted by the entire staff, leads this activity. The main process that integrates this activity is the OPSEC process. The OPSEC process is designed to develop measures and countermeasures that balance risk with the highest possible protection while protecting essential elements of friendly information (EEFIs).

8-61. Beginning during planning, the OPSEC process occurs throughout the operations process. During planning, the staff assists the OPSEC planner in identifying the EEFIs, measures and countermeasures, and tasks for subordinate units to execute, to include deception activities that support OPSEC. The OPSEC planner subsequently specifies approved EEFIs, measures, countermeasures, coordinating instructions, and tasks to subordinate units in the unit's operation order.

Note. Joint doctrine uses the term *critical information* rather than *essential elements of friendly information*. Critical information refers to information that answers key questions likely to be asked by adversaries about specific friendly intentions, capabilities, and activities.

8-62. The protection working group chaired by the operations officer and led by the chief of protection integrates the capabilities and resources that preserve combat power from threats as well as the OPSEC process. The OPSEC officer uses the protection working group to help assess unit measures and countermeasures throughout preparation and execution of the mission, as well as to identify and recommend adjustments to measures and countermeasures. (Refer to ATP 3-13.3 for more detailed information on integrating OPSEC.)

Note. At echelons below division, the OPSEC officer is typically assigned as an additional duty by the commander.

Conduct Security Activities

8-63. The operations officer leads this activity with assistance from the chief of protection, intelligence officer, and signal officer. The operations officer integrates security activities during the planning process. Based on the staff's running estimates, the operations officer develops security operations that counter threat reconnaissance, counter unmanned aircraft systems, and provide local security. Many threats have the capability to employ reconnaissance of the EMS, space, or both that may dictate specific countermeasures by Army forces.

8-64. The operations officer monitors security operations throughout the operation and recommends changes to security activities during the operation. During planning, the chief of protection identifies various physical security recommendations to safeguard friendly personnel and information. During the protection working group, the chief of protection identifies recommended changes to procedures. The intelligence officer develops the counterintelligence (CI) plan to detect and identify foreign intelligence entities' intelligence collection activities targeting Army forces. The intelligence officer identifies required changes to CI activities throughout the intelligence process. The intelligence officer is also responsible for the physical security program, personal security program, intelligence oversight training for those with clearances, conduct of Threat Awareness and Reporting Program training for unit members, and other duties outlined for the command inspection program and AR 350-1. The signal officer is responsible for the communications security program and ensuring units meet annual training requirements for use of automated systems.

Defend the Network, Data, and Systems

8-65. The signal staff officer leads this activity, assisted by the cyber electromagnetic warfare officer (known as CEWO) and space operations officer. The signal officer integrates defending the network, data, and systems initially during the planning process as part of IPOE and subsequently during preparation and execution of the operation. The IPOE process, supported by running estimates from the G-6, cyber electromagnetic warfare officer, and space operations officer, allows the planners to derive specific actions required to manage Army forces' use of the EMS and integrate defense of the network, data, and systems. These actions are regularly assessed during internal signal staff officer processes and the protection working group. Because some network defensive actions may reduce the functionality of some network and data systems, the signal staff officer ensures that the commander and staff understand the potential implications to operations.

Note. Echelons below division do not have assigned space operations officers. Echelons below brigade do not have cyber electromagnetic warfare officers assigned. These echelons rely on analysis and support from higher echelons or augmentation from an Active or Reserve Component.

Inform Information Activities

8-66. The PAO is the primary staff member responsible to the commander for integrating and synchronizing the various tasks associated with the inform information activity. During operations, the PAO is assisted by the G-9 and G-39. The inform activity communicates relevant information to various audiences. This activity has three corresponding information tasks. Army leaders, supported by the PAO, are responsible for the first activity: inform and educate Army audiences. The PAO leads the integration of the other two activities: inform U.S. domestic audiences and inform international audiences. The PAO continually monitors information that might be of concern to the unit and provides recommendations to the commander in accordance with PAO guidance received from higher headquarters.

Inform and Educate Army Audiences

8-67. When Army leaders inform and educate Army audiences, they communicate information to various internal audiences. In public affairs, internal audiences are specific audiences within the Department of Defense (DOD). Internal audiences range from a Soldier's or Civilian's immediate family members to each individual Soldier and Civilian. Integrating tasks associated with informing and educating Army audiences is both an Army leader and PAO responsibility.

8-68. Informing and educating Army audiences is a continuous process, the content of which changes based upon the situation. At home station, leaders focus on reducing vulnerabilities to Soldiers, Civilian professionals, and their Families. Upon receipt of mission, the focus and priorities may shift to specific threats, relevant actors, conditions, and vulnerabilities associated with the mission both while deployed and at home station.

8-69. The PAO integrates informing and educating Army audiences into operations by developing the commander's communication strategy, which includes command information, and by providing specific media education. PAOs assist the commander and subordinate leaders by implementing higher-level communication guidance and helping to identify pertinent information of interest, including misinformation and disinformation, applicable to various audiences within the commander's span of control. The PAO also recommends specific training and resources to help educate Soldiers, Civilian professionals, and their Families on various topics. This education covers conducting media engagements, training unit public affairs representatives, replicating media engagements during unit training, teaching basic media and military interactions, and having media awareness.

8-70. When a unit receives a mission, the PAO analyzes higher-level communication guidance and the informational considerations of an OE in coordination with the commander, G-2, G-3, G-39, PSYOP officer, and OPSEC officer. The PAO also develops specific information to communicate to various internal audiences. In some cases, the PAO generates the media to communicate specific information; in other cases, the PAO recommends communications approaches the commander and unit leaders can use to inform Army audiences. Assisted by intelligence and operations staff, the PAO identifies the information warfare approaches that the threat might employ against other internal audiences, such as civilian professionals and family members. As part of planning, the PAO proposes specific education requirements to the commander to prepare Soldiers to resist potential threat information warfare methods.

8-71. During operations, the PAO recommends adjustments to the commander's communication strategy as an output of participating in the current operations, future operations, and plans integrating cells, as well as various working groups associated with the integrating processes. The PAO also engages unit leaders to maintain situational understanding of the information requirements of various internal audiences and to identify specific information trends that require additional focus.

Inform United States Domestic and International Audiences

8-72. When Army leaders inform U.S. and international audiences, they are communicating information to various external audiences. External audiences are specific audiences outside the DOD. The PAO identifies relevant external audiences during all Army strategic contexts. Ideally, the PAO identifies external audiences during competition, and then subsequently identifies relevant audiences during crisis and conflict. In this way, the PAO helps the commander understand the information needs of various external audiences to

support the commander's objectives and assigned mission. The PAO integrates informing U.S. and international audiences via the commander's communication strategy.

8-73. Communicating with and keeping the domestic audience informed is a commander's obligation. By maintaining awareness of higher headquarters' PAO guidance and analyzing various local domestic audiences, the unit's PAO can develop community engagement opportunities and integrate them with unit activities.

8-74. When Army forces are assigned or deploy in support of a combatant commander, the PAO's analysis expands, to include various audiences from allies, partners, and host nations. The PAO identifies various local foreign audiences and, keeping the higher commander's PAO guidance in mind, identifies specific audiences to engage. The PAO considers specific cultural sensitivities, higher echelons communication objectives, and OPSEC considerations when recommending informing activities to the commander.

8-75. During operations, the PAO participates in all aspects of the operations process and consults with the G-9, G-39, and staff judge advocate during planning on the informational considerations relevant to informing various audiences. The PAO advises the planners on operational activities that various audiences might misinterpret or misunderstand, potentially undermining operations. This advice includes articulating ways the threat might use information to attack the credibility of Army operations and sow disinformation among target audiences, including various Army audiences. As part of articulating the likely threat disinformation strategy, the PAO describes methods for friendly forces to defeat threat disinformation strategies.

8-76. This analysis and planning ensures that the commander's communication strategy integrates tasks, actions, themes, and messages that complement, reinforce, and are de-conflicted with each other. The staff judge advocate provides a legal review of this analysis and planning. The G-9 provides input regarding civil impacts garnered through the civil knowledge integration process to inform the commander and staff on resulting actions, themes, and messages as they impact an OE.

8-77. The PAO monitors the situation throughout preparation and execution. Then the PAO assesses the effectiveness of the communication strategy while coordinating with the G-9, G-39, operations officer, intelligence officer, and OPSEC officer. Together they identify changes in the threat's information warfare approach and prevent disclosure of sources, methods, and information categorized as controlled or classified. When required, the PAO recommends changes for dissemination via a fragmentary order.

Note. Commanders at echelons below brigade appoint a unit public affairs representative to facilitate the inform activity. PAOs assigned to higher echelons train unit public affairs representatives on writing public affairs plans and policies, employing embedded media, engaging with local media, and conducting media opportunities.

Influence Information Activity

8-78. The G-3, assisted by the G-39, leads the influence information activity. The G-39 leads the integration of the two associated information tasks: influence threat perceptions and behaviors and influence other foreign audiences. The G-39 ensures the staff accounts for and exploits the inherent informational effects of Army operations as well as the deception activities, Soldier and leader engagements (SLEs), and MISO required to support the commander's mission and supporting objectives.

8-79. In echelons at brigade and below, the chief of staff or executive officer designates a staff member to lead the influence information tasks. The designated staff member coordinates with the higher echelon's G-39 to obtain the G-39's running estimate and subsequently relies on the higher echelon's analysis throughout the operations process. Since some influence activity subtasks, like MISO, require specifically trained and certified Soldiers to execute them, units requiring specific support request augmentation from their higher headquarters. If augmentation is not available, lower echelons return to their higher headquarters to adjust the tasks they are assigned but not capable of executing.

8-80. Several staff members provide specialized support to the influence information activity and related tasks. These include the staff judge advocate, intelligence officer, military deception (MILDEC) officer,

cyber electromagnetic warfare officer, deputy fire support coordinator, PAO, PSYOP officer or noncommissioned officer, and G-9. Both influence information activity tasks integrate into operations using similar mechanisms.

8-81. The G-39 leads the influence information activity tasks throughout the operations process. During planning, the G-39 supports the G-3 in accounting for the inherent informational effects of Army operations on relevant audiences and analyzing how differing approaches support or detract from the ability of Army forces to achieve objectives and accomplish the mission. The G-39 also advises the G-3 on how best to incorporate various specialized Army information capabilities to amplify the effects of Army operations to influence relevant audiences and complement the various courses of action developed during planning.

8-82. Several working groups facilitate the cross-functional integration of influence activity tasks. These include the civil-military operations working group, cyberspace electromagnetic activities working group, targeting working group, and assessment working group. These groups support the G-39's ability to conduct the analysis required to provide informed recommendations to the commander throughout the operations process. Additionally, these working groups support the G-39's ability to provide the mechanism by which a unit submits requests for support when required capabilities exceed the unit's capacity. Normally, established working groups are sufficient to coordinate information activities. As necessary, the commander establishes additional information-focused working groups when additional understanding or coordination of influence activities is required to facilitate integration into Army operations.

Note. Commanders at echelons below division do not have a G-39 staff section, PSYOP officer, MILDEC officer, or G-9 assigned to their headquarters. These echelons rely on analysis and support from higher echelons or augmentation from Active or Reserve Component information forces. The chief of staff or executive officer designates a member of the staff to coordinate with the higher echelon's PSYOP staff, MILDEC officer, or G-9 as required.

Attack Information Activity

8-83. The G-3, assisted by the chief of fires or deputy fire support coordinator, is responsible for integrating the attack information activity. The attack activity has two corresponding tasks: degrade threat C2 and affect threat information warfare capabilities. Each of these activities is led by the chief of fires. The chief of fires is assisted by the G-2, targeting officer, cyber electromagnetic warfare officer, G-39, PSYOP staff member, MILDEC officer, and space operations officer.

8-84. The chief of fires integrates these tasks into operations as part of the targeting process via the targeting working group. The IPOE process works concurrently with the targeting process to develop situational understanding of the threat's C2 system, sensors, and networks and threat information warfare capabilities.

8-85. The staff identifies gaps in knowledge about the threat's C2 and information warfare systems during IPOE, identifies the required information, and passes these information requirements to the intelligence section's collection manager for consideration by the information collection working group. Based on the commander's targeting guidance, the information collection working group prioritizes the information requirements, identifies available collection assets to collect the required information, and if required submits information requirements to higher headquarters for action.

8-86. As part of the targeting process, the staff selects and prioritizes targets and matches the appropriate capabilities to them, considering the capabilities available and the commander's desired effect. A consideration when recommending targets for engagement is the potential for intelligence loss. For example, destroying enemy communications infrastructure may result in a decrease in the enemy commander's ability to control friendly forces, but it may also eliminate Army forces' ability to collect signals intelligence. In this case, Army commanders carefully time the attack, maximizing both the amount of information collected and disruption to enemy C2. If additional attack capabilities are required, the chief of fires requests additional capabilities or requests that a higher headquarters consider the target for execution.

8-87. During conflict, Army forces typically aim to achieve the maximum effect possible against the threat's information capabilities. Commanders achieve the greatest advantage by affecting a variety of informational considerations that enemy commanders need to achieve their missions. The staff recommends the appropriate

balance of physical destruction and available nonlethal capabilities to employ against the enemy's most important decision-making, communications, and information warfare capabilities. Commanders typically designate targets that significantly contribute to gaining an information advantage as high-payoff targets. It is important to identify enemy controlled systems and infrastructure that will be required for friendly force use during or post conflict.

8-88. The targeting process is continuous. Targeting occurs prior to and throughout the operations process. The targeting working group meets throughout the operations process to identify targets supporting the inform, influence, and attack information activity and makes recommendations to change targeting priorities as the situation changes.

Note. Commanders at echelons below brigade typically do not have information operations, PSYOP, or civil affairs staff members assigned to their headquarters. These echelons rely on analysis and support from higher echelons. The chief of staff or executive officer designates a member of the staff to coordinate with the higher echelons' psychological warfare staff member or G-9 as required.

INFORMATION TRAINING AND EDUCATION

8-89. The Army uses training and education to equip Soldiers and leaders with the knowledge and skills they need to compete and fight with information. All Soldiers receive informational training and education appropriate to their assigned specialty and when executing operations training aligned with a specific OE. This includes digital readiness and data literacy training as described in paragraphs 3-64 through 3-69.

8-90. Informational training and education help Soldiers develop skills they apply both at home station and while deployed. The training includes basic skills that every Soldier must know and apply to protect information and information systems, to understand and support narratives, and to recognize and become resilient when facing information disruption and malign behavior. The Army further provides Soldiers with specific technical training and education to create or exploit information advantages.

COMMON TRAINING AND EDUCATION

8-91. Army training and education provides Soldiers and leaders with an individual understanding of the information contest occurring during all three strategic contexts. Soldiers gain a better understanding of ways adversaries use information and technical means to undermine the United States on societal and global scales. Army forces are most resilient and effective when Soldiers and Civilian professionals can identify friendly information vulnerabilities and methods a threat seeks to exploit for advantage.

8-92. Training varies depending on the situation and a Soldier's experience. Beginning in basic training, Soldiers learn the importance of fieldcraft, for example, to include camouflage, concealment, and minimizing signatures. Soldiers are also steeped in the Army core values, instilling in them the endurance required to maintain their morale and will even in the face of threat disinformation and misinformation. During advanced individual training, Soldiers learn how to operate and troubleshoot various information systems that enable them to perform specific tasks associated with their specific profession. When Soldiers arrive at their unit, they receive additional information training related to unit essential tasks, and possibly regional considerations. Finally, all Soldiers receive annual information training including information security, information awareness, cyber awareness, OPSEC, and threat awareness and reporting. Examples of informational training common to all Soldiers include—

- Resiliency to information for effect, misinformation, and disinformation.
- Understanding of operational and strategic narratives.
- SLE.
- Ability to protect friendly information and information systems.
- Ability to use information systems and access classified information.
- Ability to conceal visual signatures and patterns of life.
- Ability to limit personal electromagnetic signatures.

TECHNICAL TRAINING AND EDUCATION

8-93. Technology and the threat's use of technology to collect information, protect information, manipulate information, shape attitudes and beliefs, mobilize mass actions, and hinder the commander's exercise of C2 continuously threaten Army forces. Adversaries armed with long-range precision weapons—and with the ability to integrate them with technical information capabilities for direct and indirect confrontation—pose operational challenges. To counter these challenges, 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.
- CI.
- Cyberspace operations.
- EW.
- Information management.
- Intelligence and the various intelligence disciplines including human intelligence, open-source intelligence, and signal intelligence.
- Knowledge management.
- MILDEC.
- MISO.
- Network operations
- Public affairs operations.
- Space operations.
- Operational law.

This page intentionally left blank.

Source Notes

This division lists sources by page number.

vii "All warfare is based…" Sun Tzu quoted in Lionel Giles, trans., *The Art of War* (London: Luzac & Co, 1910), 6.

1-1 "To guess at …" Napoleon, quoted in J.F.C. Fuller, *Memoirs of an Unconventional Soldier* (London: Ivor Nicholson and Watson Limited, 1936), 272.

1-4 "The essence of…" JP 3-04, *Information in Joint Operations* (Washington DC: Government Publishing Office, 14 September 2022), ix.

1-6 **Fighting for and With Information** vignette. Adapted from "Ambiguous Environment: Fighting for Information," Army University Press staff, unpublished text, 2017.

1-7 **The Three Warfares Strategy in the South China Sea** vignette. Adapted from "China's 'Three Warfares' in Theory and Practice in the South China Sea," Doug Livermore, *Georgetown Security Studies Review*, accessed 20 September 2023, https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

1-12 "The [People's Liberation Army] …" ATP 7-100.3, *Chinese Tactics* (Washington DC: Government Publishing Office, 09 August 2021), 5-4.

1-13 **Russian Activities in Ukraine 2014** vignette. Adapted from JP 3-04, *Information in Joint Operations* (Washington DC: Government Publishing Office, 14 September 2022), I-3, I-4.

2-1 "As our present …," J.F.C. Fuller, *Memoirs of an Unconventional Soldier* (London: Ivor Nicholson and Watson Limited, 1936), 326.

2-11 **Information Advantage during Large-Scale Combat** vignette. Adapted from FM 100-6 (obsolete), *Information Operations* (Washington DC: Government Publishing Office, 27 August 1996), 3-1.

2-14 "A principle is …" ADP 1-01, *Doctrine Primer* (Washington DC: Government Publishing Office, 31 July 2019), 2-1.

3-1 "If you know …" Sun Tzu quoted in Lionel Giles, trans., *The Art of War* (London: Luzac & Co, 1910), 24–25.

3-9 "See yourself, see …" FM 3-0, *Operations* (Washington DC: Government Publishing Office, 01 October 2022), 3-8.

3-11 "When I took …" T.E. Lawrence, *The Letters of T.E. Lawrence*, David Garnett, ed. (Toronto: Jonathan Cape Ltd., 1938), 769.

3-13 "In war obscurity …" *Infantry in Battle* (Washington DC: The Infantry Journal - Incorporated, 1939), 16. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/infantry-in-battle.pdf.

4-1 "Leaders must assume…" FM 3-0, *Operations* (Washington DC: Government Publishing Office, 01 October 2022), 3-10.

4-2 "Operations Security (OPSEC) as …" *PURPLE DRAGON: The Origin and Development of the United States OPSEC Program monograph*, Center for Cryptologic History, Series VI, Vol 2, National Security Agency, 1993 (redacted version: 08-22-2007, FOIA Case #8481), accessed 18 July 2023. https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/purple_dragon.pdf.

4-4 "To design and …" ATP 3-37.34, *Survivability Operations* (Washington DC: Government Publishing Office, 16 April 2018), 6-5.

4-7 "Threat cyberspace and …" ATP 6-02.12, *Department of Defense Information Network-Army Planning Techniques* (Washington DC: Government Publishing Office, 17 November 2021), 1-2.

4-11 **Personal Electronic Devices** vignette. Combined Arms Doctrine Doctorate staff, unpublished text, 2022 based on "Fitness App Strava Lights up Staff at Military Bases." BBC News, BBC, 29 Jan. 2018, www.bbc.com/news/technology-42853072; Garamone, Jim. New Policy Prohibits GPS Tracking in Deployed Settings, U.S. Department of Defense, 6 Aug. 2018, www.defense.gov/News/News-Stories/Article/Article/1594486/new-policy-prohibits-gps-tracking-in-deployed-settings/; Hsu, Jeremy. "The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data." Wired, Conde Nast, 30 Jan. 2018, www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

5-1 "When what we do …" JDN 2-13. *Commander's Communication Synchronization* (Washington DC: Government Publishing Office, 16 December 2013), vi.

5-4 Figure 5-2. Eisenhower's order of the day (6 June 1944). https://www.archives.gov/milestone-documents/general-eisenhowers-order-of-the-day. Citation: D-day statement to soldiers, sailors, and airmen of the Allied Expeditionary Force, 6/44, Collection DDE-EPRE: Eisenhower, Dwight D: Papers, Pre-Presidential, 1916-1952; Dwight D. Eisenhower Library; National Archives and Records Administration.

5-10 "The First Amendment …" JP 3-61, *Public Affairs* (Washington DC: Government Publishing Office, 17 November 2015), vii.

5-11 Figure 5-3. Principles of Information. DODD 5122.05, *Assistant to The Secretary of Defense for Public Affairs (ATSD(PA))* (Washington DC: Government Publishing Office, 07 August 2017), 11.

6-1 "Fundamentally, all war …" ADP 1-01, *Doctrine Primer* (Washington DC: Government Publishing Office, 31 July 2019), 3-1.

6-2 "If somebody's trailing …" *Standing Orders*, Rogers' Rangers as written in TC 3-21.76, *Ranger Handbook* (Washington DC: Government Publishing Office, 26 April 2017), xx.

6-3 **Deception and the Invasion of the European Continent** vignette. Adapted from FM 100-6 (obsolete), *Information Operations* (Washington DC: Government Publishing Office, 27 August 1996), 3-4.

6-5 "Partnership develops trust, …" ADP 1, *The Army* (Washington DC: Government Publishing Office, 31 July 2019), 2-1.

6-6 "A force that …" FM 3-0, *Operations* (Washington DC: Government Publishing Office, 01 October 2022), 1-22.

7-1 "Cyberspace and the …" FM 3-12, *Cyberspace Operations and Electromagnetic Warfare* (Washington DC: Government Publishing Office, 24 August 2021), 1-1.

7-5 "Fighting with a …" Sun Tzu quoted in Lionel Giles, trans., *The Art of War* (London: Luzac & Co, 1910), 3.

8-1 "Achieving information advantages …" FM 3-0, *Operations* (Washington DC: Government Publishing Office, 01 October 2022), 5-4.

8-3 "The behaviour-centric …" AJP-10.1, *Allied Joint Doctrine for Information Operations* (Washington DC: NATO Standardization Office, 26 January 2023), 7.

Glossary

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

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
AJP	allied joint publication
AR	Army regulation
ATP	Army techniques publication
C2	command and control
CCIR	commander's critical information requirement
CCS	commander's communication synchronization
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CI	counterintelligence
COP	common operational picture
CP	command post
DA	Department of the Army
DISO	deception in support of operations security
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
EA	electromagnetic attack
EEFI	essential element of friendly information
EMS	electromagnetic spectrum
EW	electromagnetic warfare
FIE	foreign intelligence entity
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
G-39	assistant chief of staff, information plans and operations
GTA	graphic training aide
i.e.	id est, Latin for "that is"
IPOE	intelligence preparation of the operational environment
ISR	intelligence, surveillance, and reconnaissance

JDN	Joint doctrine note
JP	joint publication
KMO	knowledge management officer
METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations
MILDEC	military deception
MISO	military information support operations
NATO	North Atlantic Treaty Organization
OE	operational environment
OIE	operations in the information environment
OPSEC	operations security
PAO	public affairs officer
PIR	priority intelligence requirement
PSYOP	psychological operations
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SLE	Soldier and leader engagement
TAC-D	tactical deception
TC	training circular
U.S.	United States
U.S.C.	United States Code

SECTION II – TERMS

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

audience

In public affairs, a broadly-defined group that contains stakeholders and/or publics relevant to military operations. (JP 3-61)

battle rhythm

(Army) A deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations. (FM 6-0)

board

(Army) A grouping of predetermined staff representatives with delegated decision authority for a particular purpose or function. (FM 6-0)

civil-military integration

The actions taken to establish, maintain, influence, or leverage relations between military forces and indigenous populations and institutions to synchronize, coordinate, and enable interorganizational cooperation and to achieve unified action. (FM 3-57)

combat power

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)

combined arms

The synchronized and simultaneous application of arms to achieve an effect greater than if each element was used separately or sequentially. (ADP 3-0)

command and control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. (JP 1, Volume 2)

command and control system

(Army) The arrangement of people, processes, networks, and command posts that enable commanders to conduct operations. (ADP 6-0)

command post

A headquarters, or a portion there of, organized for the exercise of command and control. (FM 6-0)

commander's communication synchronization

A process to coordinate and synchronize narratives, themes, messages, images, operations, and actions to ensure their integrity and consistency to the lowest tactical level across all relevant communication activities. (JP 3-61)

commander's critical information requirement

Specific information identified by the commander as being essential to facilitate timely decision making. (JP 3-0)

command information

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)

common operational picture

(Army) A display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADP 6-0)

communications security

Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 6-0)

counterintelligence

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)

crisis

An emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives. (JP 3-0)

critical information

Specific facts about friendly intentions, capabilities, and activities needed by an enemy or adversary for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 2-0)

cyberspace attack

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)

cyberspace defense

Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures. (JP 3-12)

cyberspace security

Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers and networks, including platform information technology. (JP 3-12)

deception means

Methods, resources, and techniques that can be used to convey information to the deception target. (JP 3-13.4)

defensive cyberspace operations

Missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity. (JP 3-12)

depth

The extension of operations in time, space, or purpose to achieve definitive results. (ADP 3-0)

***disinformation**

Incomplete, incorrect, or out of context information deliberately used to influence audiences.

disintegrate

To disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations. (FM 3-0)

electromagnetic attack

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)

electromagnetic compatibility

The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (JP 3-85)

electromagnetic hardening

Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (JP 3-85)

electromagnetic masking

The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

electromagnetic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 3-85)

electromagnetic support

Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 3-85)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan. (JP 3-85)

enemy

A party identified as hostile against which the use of force is authorized. (ADP 3-0)

essential element of friendly information

A critical aspect of a friendly operation that, if known by a threat would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADP 6-0)

execution

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)

external audience

In public affairs, all people who are not United States military members, Department of Defense civilian employees, and their immediate families. (JP 3-61)

friendly force information requirement

Information the commander and staff need to understand the status of friendly force and supporting capabilities. (JP 3-0)

human dimension

Encompasses people and the interaction between individuals and groups, how they understand information and events, make decisions, generate will, and act within an operational environment. (FM 3-0)

indicator

In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities. (JP 3-13.3)

***information activity**

A collection of tasks linked by purpose to affect how humans and automated systems derive meaning from, use, and act upon, or are influenced by, information.

***information advantage**

A condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior.

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

information dimension

The content and data that individuals, groups, and information systems communicate and exchange, as well as the analytics and technical processes used to exchange information within an operational environment. (FM 3-0)

information environment

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)

***information for effect**

The use, publication, or broadcast of factual information to negatively affect perceptions and/or damage credibility and capability of the targeted group.

information management

(Army) The science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products. (ADP 6-0)

informational considerations

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)

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)

internal audience

In public affairs, United States military members and Department of Defense civilian employees and their immediate families. (JP 3-61)

knowledge management

(Army) The process of enabling knowledge flow to enhance shared understanding, learning, and decision making. (ADP 6-0)

large-scale combat operations

Extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives. (ADP 3-0)

liaison

That contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action. (FM 6-0)

message

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

military deception

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)

military information support operations

Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives. (JP 3-13.2)

***misinformation**

Unintentional incorrect information from any source.

mission command

(Army) The Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation. (ADP 6-0)

multinational operations

A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 3-16)

operation

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

operational environment

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

operational reach

The distance and duration across which a force can successfully employ military capabilities. (JP 3-0)

operations in the information environment

Military actions involving the integrated employment of multiple information forces to affect drivers of behavior. (JP 3-04)

operations process

The major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. (ADP 5-0)

physical dimension

The material characteristics and capabilities, both natural and manufactured, within an operational environment. (FM 3-0)

planning horizon

A point in time commanders use to focus the organization's planning efforts to shape future events. (ADP 5-0)

preparation

Those activities performed by units and Soldiers to improve their ability to execute an operation. (ADP 5-0)

priority intelligence requirement

An intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support. (JP 2-0)

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)

public

In public affairs, a segment of the population with common attributes to which a military force can tailor its communication. (JP 3-61)

public affairs

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

relevant actor

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. (JP 3-04)

relevant information

All information of importance to the commander and staff in the exercise of command and control. (ADP 6-0)

risk management

The process to identify, assess, and mitigate risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

running estimate

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

security operations

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)

Soldier and leader engagement

Interpersonal interactions by Soldiers and leaders with audiences in an area of operations. (ATP 3-13.5)

tactical deception

A friendly activity that causes enemy commanders to take action or cause inaction detrimental to their objectives. (FM 3-90)

target

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

target audience

An individual or group selected for influence. (JP 3-04)

targeting

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

***technical effects**

One or more capabilities, activities, or programs planned, coordinated, or executed that utilize classified means to accomplish an objective or enable military operations.

tempo

The relative speed and rhythm of military operations over time with respect to the enemy. (ADP 3-0)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

unified action

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

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)

warfighting function

A group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives. (ADP 3-0)

working group

(Army) A grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. (FM 6-0)

References

All URLs accessed on 30 October 2023.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. 15 September 2023.

FM 1-02.1. *Operational Terms*. 09 March 2021.

RELATED PUBLICATIONS

These cited documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint doctrinal and administrative publications are available online at https://www.jcs.mil/Doctrine/. Most Department of Defense publications are available at https://www.esd.whs.mil/dd/.

CJCSI 3211.01F. (U) *Joint Policy for Military Deception* (S/NF). 15 May 2015. This publication is classified and requires a common access card to access.

DODD 5122.05. *Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))*. 07 August 2017.

DODI 5200.01. *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)*. 21 April 2016.

DODI 5400.17. *Official Use of Social Media for Public Affairs Purposes*. 12 August 2022.

JP 1, Volume 1. *Joint Warfighting*. 27 August 2023.

JP 1, Volume 2. *The Joint Force*. 19 June 2020.

JP 2-0. *Joint Intelligence*. 26 May 2022.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-04. *Information in Joint Operations*. 14 September 2022.

JP 3-12. *Joint Cyberspace Operations*. 19 December 2022.

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

JP 3-13.3. *Operations Security*. 06 January 2016.

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

JP 3-16. *Multinational Operations*. 01 March 2019.

JP 3-60. *Joint Targeting*. 28 September 2018.

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

JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.

JP 6-0. *Joint Communications System*. 10 June 2015.

ARMY PUBLICATIONS

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

ADP 1. *The Army*. 31 July 2019.

ADP 2-0. *Intelligence*. 31 July 2019.

ADP 3-0. *Operations*. 31 July 2019.

ADP 3-19. *Fires*. 31 July 2019.

ADP 3-37. *Protection*. 31 July 2019.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 4-0. *Sustainment*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

AR 350-1. *Army Training and Leader Development*. 10 December 2017.

AR 360-1. *The Army Public Affairs Program*. 08 October 2020.

AR 380-67. *Personnel Security Program*. 24 January 2014.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 01 March 2019.

ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities*. 11 December 2015.

ATP 3-11.50. *Battlefield Obscuration*. 15 May 2014.

ATP 3-12.3. *Electromagnetic Warfare Techniques*. 30 January 2023.

ATP 3-13.3. *Army Operations Security for Division and Below*. 16 July 2019.

ATP 3-13.5. *Soldier and Leader Engagement*. 21 December 2021.

ATP 3-37.34/MCTP 3-34C. *Survivability Operations*. 16 April 2018.

ATP 3-39.32. *Physical Security*. 08 March 2022.

ATP 5-0.3/MCRP 5-10.1/NTTP 5-01.3/AFTTP 3-2.87. *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment*. 07 February 2020.

ATP 5-19. *Risk Management*. 09 November 2021.

ATP 6-0.5. *Command Post Organization and Operations*. 01 March 2017.

ATP 6-01.1. *Techniques for Effective Knowledge Management*. 06 March 2015.

ATP 7-100.3. *Chinese Tactics*. 09 August 2021.

FM 2-0. *Intelligence*. 01 October 2023.

FM 3-0. *Operations*. 01 October 2022.

FM 3-12. *Cyberspace Operations and Electromagnetic Warfare*. 24 August 2021.

FM 3-13. *Information Operations*. 06 December 2016.

FM 3-13.4. *Army Support to Military Deception*. 26 February 2019.

FM 3-14. *Army Space Operations*. 30 October 2019.

FM 3-53. *Military Information Support Operations*. 04 January 2013.

FM 3-55. *Information Collection*. 03 May 2013.

FM 3-57. *Civil Affairs Operations*. 28 July 2021.

FM 3-60. *Army Targeting*. 11 August 2023.

FM 3-61. *Communication Strategy and Public Affairs Operations*. 25 February 2022.

FM 3-90. *Tactics*. 01 May 2023.

FM 5-0. *Planning and Orders Production*. 16 May 2022.

FM 6-0. *Commander and Staff Organization and Operations*. 16 May 2022.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.

GTA 33-01-004. *Military Information Support Operations Authoritative References*. 01 November 2017.

TC 7-100.2. *Opposing Force Tactics*. 09 December 2011.

OTHER REFERENCES

AJP-10.1. *Allied Joint Doctrine for Information Operations*. 26 January 2023. https://nso.nato.int/nso/.

Army Values. https://www.army.mil/values/index.html.

Soldier's Creed. https://www.army.mil/values/soldiers.html.

National Military Strategy of the United States. 2015. https://jdeis.js.mil/jdeis/jel/jel/other_pubs/nms_2015.pdf.

National Security Strategy of the United States. 2017. https://jdeis.js.mil/jdeis/jel/jel/other_pubs/nss2017.pdf.

Title 5, U.S.C. "Freedom of Information Act." https://www.loc.gov/.

Warrior Ethos. https://www.army.mil/values/warrior.html.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

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

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

SOURCES USED

ADP 1-01. *Doctrine Primer*. 31 July 2019.

Army University Press staff (2017). "Ambiguous Environment: Fighting for Information." Unpublished text.

ATP 6-02.12. *Department of Defense Information Network-Army Planning Techniques*. 17 November 2021.

Combined Arms Doctrine Doctorate staff (2022). "Personal Electronic Devices." Unpublished text.

FM 100-6 (obsolete). *Information Operations*. 27 August 1996.

Fuller, J.F.C. *Memoirs of an Unconventional Soldier*. London: Ivor Nicholson and Watson Limited, 1936.

"General Dwight D. Eisenhower's Order of the Day (1944)." *National Archives and Records Administration*. National Archives and Records Administration. www.archives.gov/milestone-documents/general-eisenhowers-order-of-the-day. Accessed 18 July 2023.

Giles, Lionel, trans. *The Art of War*. London: Luzac & Co, 1910.

Infantry in Battle. Washington DC: The Infantry Journal - Incorporated, 1939.

JDN 2-13. *Commander's Communication Synchronization*. 16 December 2013.

Lawrence, T.E. *The Letters of T.E. Lawrence*. David Garnett, ed. Toronto: Jonathan Cape Ltd., 1938.

Livermore, Doug. "China's 'Three Warfares' in Theory and Practice in the South China Sea." *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/. Accessed 20 September 2023.

PURPLE DRAGON: The Origin and Development of the United States OPSEC Program. https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/purple_dragon.pdf. Accessed 18 July 2023.

TC 3-21.76. *Ranger Handbook*. 26 April 2017.

This page intentionally left blank.

Index

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

This page intentionally left blank.

ADP 3-13

27 November 2023

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2331813

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve. To be distributed in accordance with the initial distribution number (IDN) 116195, requirements for ADP 3-13.

This page intentionally left blank.

PIN: 216559-000