ADP 2-0
INTELLIGENCE

JULY 2019

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes ADP 2-0, dated 4 September 2018.

HEADQUARTERS, DEPARTMENT OF THE ARMY

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

Foreword

The future for our Army is challenging. In order to prepare for an unknowable future, the Army must be ready to conduct the full range of military operations, with a focus on large-scale ground combat operations. The Army will operate across multiple domains with unified action partners. We must deploy and transition rapidly to large-scale ground combat operations, present multiple dilemmas to the enemy, operate dispersed while maintaining decisive effects, and consolidate gains.

Intelligence, especially warning intelligence and other aspects of setting the theater of operations, is integral to operations, as the theater army competes with peer threats below the level of armed conflict. Friendly forces attempt to maintain an enduring initiative during operations to shape and prevent. However, enemies are likely to initiate hostilities against friendly forces from initial positions of relative advantage.

Therefore, Army forces will conduct operations across multiple domains to gain freedom of action for other members of the joint force. Units must be prepared to fight for intelligence against a range of threats, enemy formations, and unknowns. These challenges include integrated air defense systems and long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, deception operations, and camouflage.

These complexities place a significant demand on intelligence professionals for real-time detailed intelligence to develop situational understanding and answer the commander's priority intelligence requirements. Intelligence enables command and control, facilitates initiative, and allows commanders and staffs to execute tailored solutions for complex problems in the fast-paced environments of the future. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for best effect. Ready access to the intelligence networks facilitates timely decision making and provides commanders the flexibility to successfully shape and execute operations.

ADP 2-0, Intelligence, provides a common construct for intelligence support in complex operational environments and a framework to support unified land operations across the range of military operations. This publication serves as the intelligence doctrinal foundation for our Army. Every Army professional must understand the doctrinal principles of Army intelligence.

ROBERT P. WALTERS, JR.
MAJOR GENERAL, UNITED STATES ARMY
COMMANDING

This page intentionally left blank.

*ADP 2-0

Army Doctrine Publication
No. 2-0

Headquarters
Department of the Army
Washington, D.C., 31 July 2019

Intelligence

Contents

*This publication supersedes ADP 2-0, dated 4 September 2018.

Figures

Tables

Preface

ADP 2-0 is the Army's most fundamental publication for Army intelligence. ADP 2-0 provides a common construct for intelligence doctrine from which Army forces adapt to conduct operations. ADP 2-0 augments and is nested with the capstone doctrine from both ADP 3-0 and FM 3-0.

The principal audience for ADP 2-0 is every Soldier and Department of the Army Civilian who interact with the intelligence warfighting function. This publication is the foundation for the intelligence warfighting function and subsequent doctrine development. It also serves as a reference for personnel who are developing doctrine, leader development, materiel and force structure, and institutional and unit training for intelligence.

Note. The Army does not have a specific military occupational specialty for open-source intelligence; it does not have base tables of organization and equipment for open-source intelligence units or staff elements.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See the Department of Defense [DOD] Law of War Manual, CJCSI 3121.01B, and FM 27-10.)

This publication contains copyrighted material.

ADP 2-0 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ADP 2-0 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ADP 2-0 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

ADP 2-0 applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated.

The proponent of ADP 2-0 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-DST-D (ADP 2-0), 550 Cibeque, Fort Huachuca, AZ, 85613-7017; by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Acknowledgement

The critical thinking material in paragraph 2-30 has been used with permission from the Foundation for Critical Thinking, www.criticalthinking.org, *The Thinker's Guide to Analytic Thinking*, 2017, and *The Miniature Guide to Critical Thinking: Concepts and Tools*, 2014, by Dr. Linda Elder and Dr. Richard Paul. The copyright owners have granted permission to reproduce material from their works. With their permission, some of the text has been paraphrased and adapted for military purposes.

This page intentionally left blank.

Introduction

KEY DOCTRINAL CONCEPTS

Operations and intelligence are closely linked. The intelligence process is continuous and directly drives and supports the operations process. This principle will remain true well into the future. Intelligence will continue to be a critical part of the conduct—planning, preparing, executing, and assessing—of operations. Future operations will be difficult. They will occur in complex operational environments against capable peer threats, who most likely will start from positions of relative advantage. U.S. forces will require effective intelligence to prevail during these operations.

Intelligence supports joint and Army operations across unified action, the Army's strategic roles, unified land operations, and decisive action at each echelon—from the geographic combatant command down to the battalion level. Specifically, intelligence supports commanders and staffs by facilitating situational understanding across all domains and the information environment. Commanders and staffs use situational understanding to identify and exploit multi-domain windows of opportunity and to achieve and exploit positions of relative advantage.

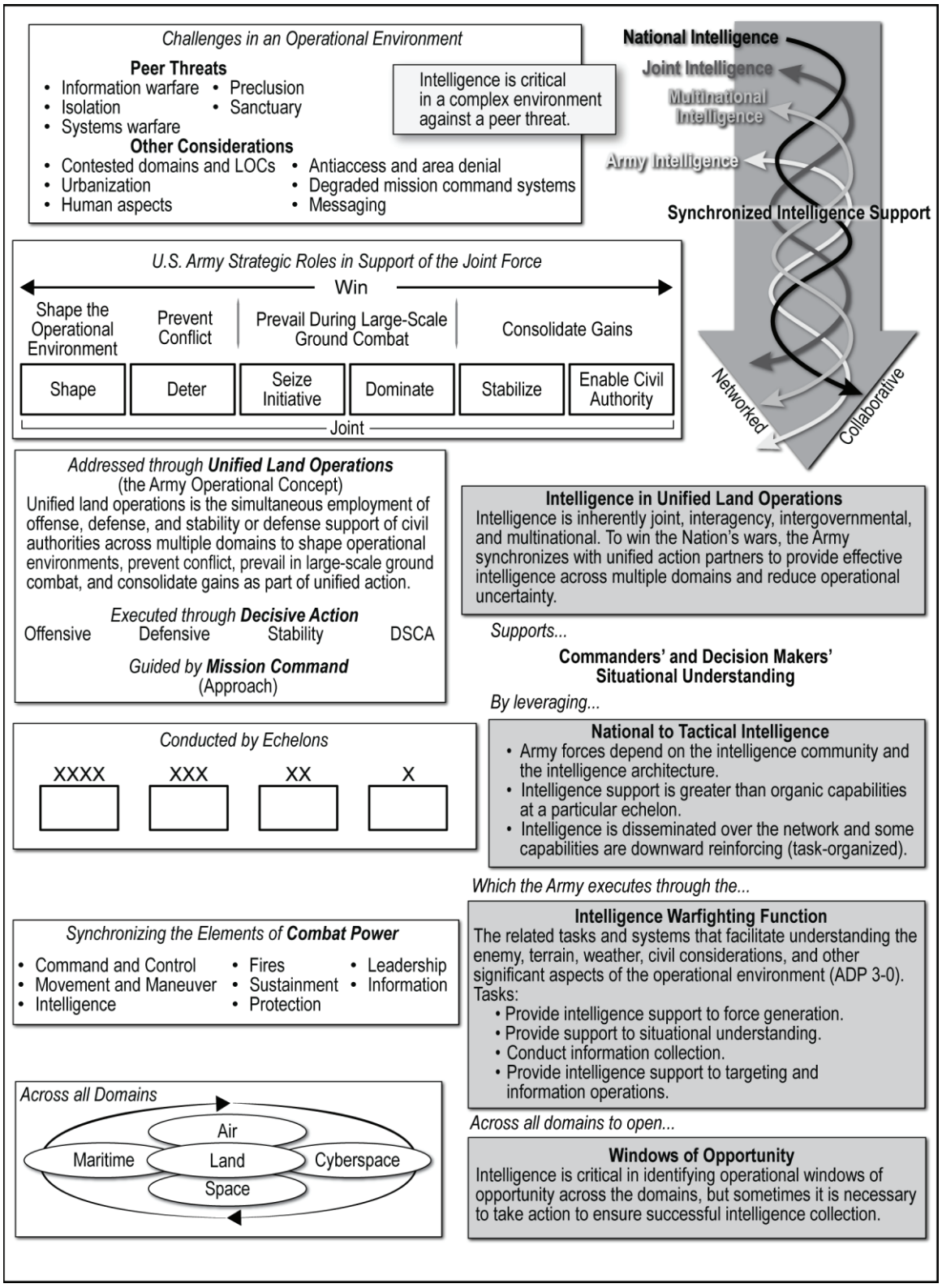
Intelligence is inherently joint, interagency, intergovernmental, and multinational. Every aspect of intelligence is synchronized, networked, and collaborative across all unified action partners. This synchronization occurs through national to tactical intelligence support. The Army both benefits from and contributes to national to tactical intelligence and focuses the Army intelligence effort through the intelligence warfighting function, which is larger than military intelligence. Critical participants within the function include commanders and staffs, decision makers, collection managers, and intelligence leaders.

Despite a thorough understanding of intelligence fundamentals and a proficient staff, an effective intelligence effort is not assured. Large-scale ground combat operations are characterized by complexity, chaos, fear, violence, fatigue, and uncertainty. The fluid and chaotic nature of large-scale ground combat operations causes the greatest degree of fog, friction, and stress on the intelligence warfighting function. Threat forces will attempt to counter friendly collection capabilities by using integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, camouflage and concealment, and deception.

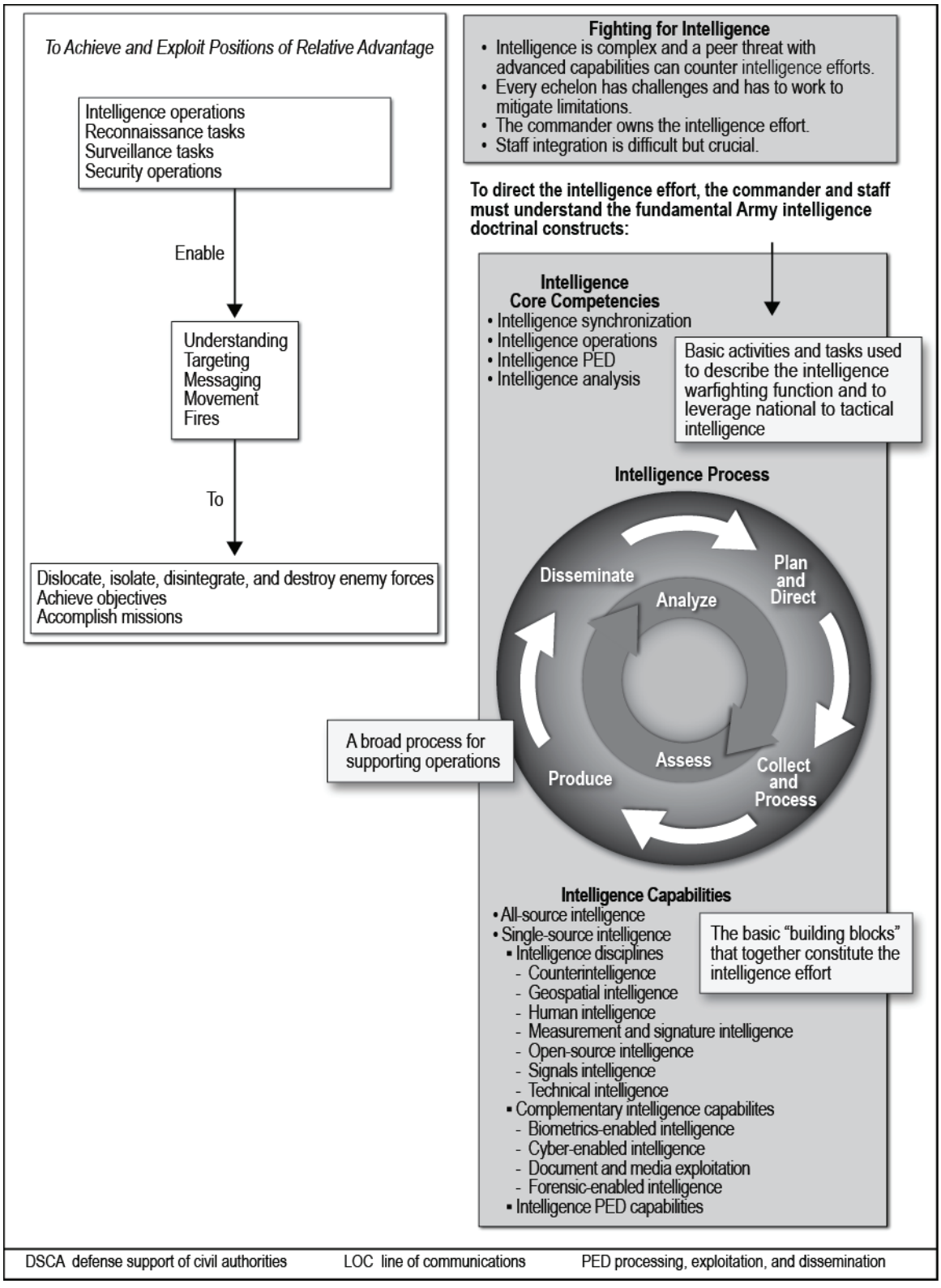
Ensuring an effective intelligence effort is a challenge described as fighting for intelligence. The following aspects of fighting for intelligence are critical:

- Effective intelligence requires developing an effective intelligence architecture well before large-scale combat operations.
- The commander must own the intelligence effort.
- The commander and staff—
  - Must forge an effective relationship and excel in staff integration.
  - Must understand intelligence limitations, especially collection gaps, at their echelon and overcome or mitigate those limitations through effective information collection.
  - At times, may have to conduct combat operations or find creative solutions to enable information collection.
- The unit must adjust the information collection plan, adapt to threat counter-collection measures, and maintain a layered and aggressive information collection effort.

The introductory figure illustrates the nesting of intelligence with operations.



Introductory figure. ADP 2-0 logic chart



Introductory figure. ADP 2-0 logic chart (*continued*)

EXECUTIVE SUMMARY

This publication was deliberately changed to nest ADP 2-0 with FM 3-0 and to help focus the Army on the new challenges associated with joint large-scale combat operations and Army large-scale ground combat operations. Despite the change in focus, the intelligence fundamental concepts remain but with some modifications. This version of ADP 2-0 also incorporates terminology changes driven by updates to ADPs 3-0, 5-0, and 6-0.

This executive summary highlights the most important aspects of each chapter and the most significant changes from the last version. Additionally, each bullet includes the page number (in parenthesis) where that topic is discussed in this publication.

ADP 2-0 contains five chapters:

Chapter 1 discusses how intelligence nests with the most fundamental operational doctrinal concepts. In order to understand Army intelligence, it is important to understand intelligence within the larger context of FM 3-0. From national and DOD levels down to the Army battalion level, intelligence is an activity that is never at rest. Army forces are globally engaged, always executing operations and preparing for future operations as part of a joint team. This chapter—

- Provides an overview of—
  - *Large-scale combat operations*. (1-1)
  - *Unified action* and *joint operations*. (1-5)
  - The *Army's strategic roles*. (1-6)
  - *Unified land operations*. (1-7)
  - *Decisive action* with subordinate discussions on the offense, defense, stability, and defense support of civil authorities. (1-7)
- Updates discussion of the *operational environment*. (1-2)
- Updates the discussion of the *threat*. (1-4)
- Discusses intelligence support within *multi-domain operations*. (1-10)

Chapter 2 discusses the most fundamental intelligence doctrinal concepts. Intelligence support is critical to operations and occurs at each echelon, from theater army down to the battalion level. In order to drive intelligence, the commander and staff must understand the intelligence warfighting function, the intelligence core competencies, national to tactical intelligence, setting the theater, and establishing the intelligence architecture. This chapter—

- Discusses the *purpose of intelligence.* (2-1)
- Updates the discussion of the *intelligence warfighting function.* (2-2)
- Updates the description of the *intelligence core competencies* and introduces *intelligence processing, exploitation, and dissemination (PED)* as a fourth intelligence core competency. (2-5)
- Introduces PED as a term and updates the PED discussion to include intelligence PED. (2-6)
- Introduces *national to tactical intelligence*, which replaces the discussion of *intelligence enterprise*. (2-7)
- Introduces and discusses *regionally aligned forces* and *setting the theater* for intelligence in Army forces. (2-8)
- Introduces and discusses *establishing the intelligence architecture* as a capability. (2-9)

Chapter 3 discusses the most important intelligence doctrinal construct—the intelligence process. The intelligence process is a model that describes how the intelligence warfighting function facilitates situational understanding and supports decision making. This process provides a common framework for Army professionals to guide their thoughts, discussions, plans, and assessments. This chapter—

- Discusses how the *operations process* and *intelligence process* nest. (3-1)
- Discusses the *plan and direct* step. (3-3)
- Modifies the *collect* step to the *collect and process* step, and includes a new figure depicting the revision of the intelligence process. (3-5)
- Discusses the *produce* step. (3-6)
- Discusses the *disseminate* step. (3-6)

- Discusses the *analyze* continuing activity. (3-8)
- Discusses the *assess* continuing activity. (3-8)

Chapter 4 discusses the key capabilities by which the intelligence warfighting function facilitates situational understanding and supports decision making. The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. These key capabilities (building blocks) are all-source intelligence and single-source intelligence. Single-source intelligence comprises the intelligence disciplines, complementary intelligence capabilities, and PED capabilities. This chapter—

- Updates the discussion of *all-source intelligence* and introduces *identity activities* as an all-source effort. (4-1)
- Updates the discussion of the *intelligence disciplines.* (4-3)
- Updates the discussion of the *complementary intelligence capabilities.* (4-10)
- Replaces the discussion of *PED* with new material found in chapter 2. (2-6)
- Discusses *intelligence PED capabilities* that support information collection. (4-13)

Chapter 5 culminates this publication with an important discussion of fighting for intelligence. Intelligence is never perfect, information collection is never easy, and a single collection capability is never persistent and accurate enough to provide all of the answers. The fluid and chaotic nature of large-scale ground combat operations will cause the greatest degree of fog, friction, and stress on the intelligence warfighting function. Units must be prepared to fight for intelligence against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the operational environment. This chapter—

- Discusses *fighting for intelligence* during large-scale ground combat operations, with emphasis on the intelligence challenge. (5-1)
- Updates the description of the *commander's role in intelligence,* including *intelligence and the integrating processes.* (5-2)
- Discusses *planning considerations* and *information requirements* to support the defense and offense, reconnaissance, security operations, and deep operations. (5-5)
- Discusses unique aspects of *developing a flexible information collection plan* and *establishing an effective intelligence architecture.* (5-8)
- Updates the discussion on the *continuous nature of information collection*. (5-9)

NEW, RESCINDED, AND MODIFIED TERMS

ADP 2-0 becomes the proponent of one Army term, introduces two new Army terms, and modifies three Army terms. (See introductory table 1.)

Introductory table 1. New and modified Army terms

Term	*Remarks*
human intelligence	ADP 2-0 becomes the proponent.
intelligence enterprise	Replaced by national to tactical intelligence.
intelligence processing, exploitation, and dissemination	Modified description.
intelligence operations	Modified definition.
intelligence reach	Modified definition.
intelligence synchronization	Modified definition.
processing, exploitation, and dissemination	New term.

This publication uses the term *commander's critical information requirements and other requirements* when referring to information collection activities. When referring to the intelligence warfighting function or intelligence analysis, the more specific term, *priority intelligence requirements and other requirements* applies.

Acronyms are introduced at their first use in the front matter of this publication (preface and introduction), and again in the body of the publication (chapters 1 through 5).

ADP 2-0 introduces G-*X* and S-*X* (such as G-2 and S-2) acronyms at their first use without defining them as it hinders readability. Definitions for these acronyms can be found in the glossary of this publication.

Chapter 1

Operations and Intelligence

Throughout modern history, intelligence has been and remains an inherent part of military operations. From national and Department of Defense (DOD) levels down to the Army battalion level, intelligence is an activity that never stops. Army forces are globally engaged, always executing operations and preparing for future operations as part of a joint team. A key part of global engagement is the continuous use of intelligence, the collection and analysis of information, and the production of intelligence. This constant activity, referred to as intelligence, is never at rest. To understand Army intelligence, it is important to understand intelligence within the larger context of joint large-scale combat operations, including Army large-scale ground combat operations; the operational environment; unified action; the Army strategic roles; and unified land operations.

> ***Intelligence***
>
> Intelligence is (1) 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; (2) the activities that result in the product; and (3) the organizations engaged in such activities (JP 2-0).

LARGE-SCALE COMBAT OPERATIONS

1-1. Threats to United States (U.S.) interests worldwide are countered by the U.S. forces' ability to respond to a variety of challenges along a conflict continuum that spans from peace to war as shown in figure 1-1. U.S. forces conduct a range of military operations to respond to these challenges. The conflict continuum does not proceed smoothly from stable peace to general war and back.

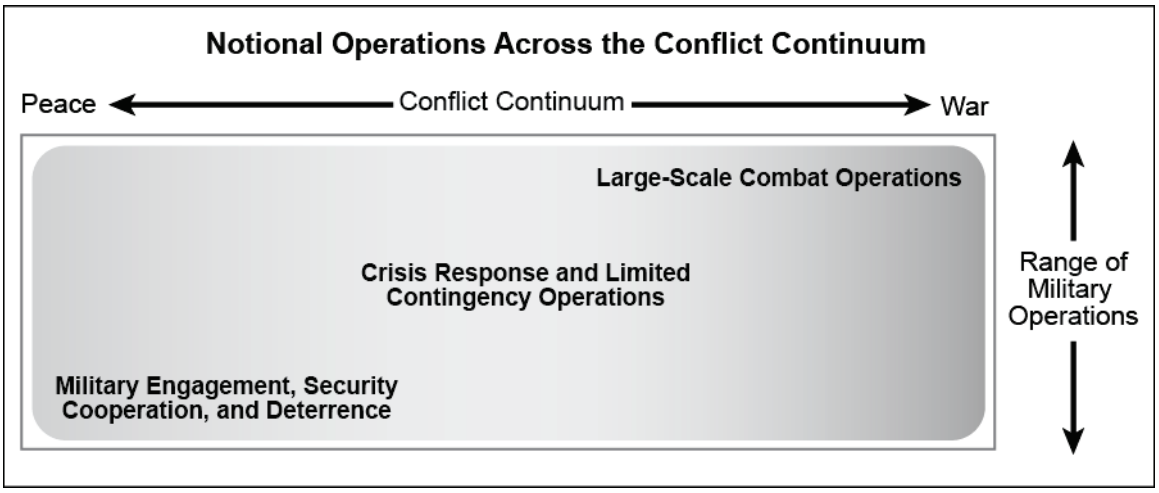


Figure 1-1. The conflict continuum and the range of military operations

1-2. The range of military operations is a fundamental construct that helps relate military activities and operations in scope and purpose within a backdrop of the conflict continuum. All operations along this range share a common fundamental purpose—to achieve or contribute to national objectives. Military engagement, security cooperation, and deterrence activities build networks and relationships with partners, shape regions, keep day-to-day tensions between nations or groups below the threshold of armed conflict, and maintain U.S. global influence. Typically, crisis response and limited contingency operations are focused in scope and scale and conducted to achieve a specific strategic- or operational-level objective in an operational area. *Large-scale combat operation*s 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). Large-scale combat operations are at the far right of the conflict continuum and associated with war. These operations occur in the form of major operations and campaigns aimed at defeating an enemy's armed forces and military capabilities to support national objectives. Large-scale combat operations are intense, lethal, and brutal. Their conditions include complexity, chaos, fear, violence, fatigue, and uncertainty.

1-3. While the Army must be manned, equipped, and trained to operate across the range of military operations, large-scale combat operations present the greatest challenge for Army forces. Army forces conduct large-scale ground combat operations with a focus on the defeat and destruction of enemy ground forces as part of the joint team. *Large-scale ground combat operations* are sustained combat operations involving multiple corps and divisions (ADP 3-0). Large-scale ground combat operations are not synonymous with total war and can occur below the nuclear threshold. However, large-scale ground combat operations entail significant operational risk, synchronization, capabilities convergence, and a high operational tempo. Army forces close with and destroy enemy forces in any terrain, exploit success, and break the opponent's will to resist. The ability to prevail in ground combat is a decisive factor in breaking an enemy's capability and will to continue a conflict. Conflict resolution requires the Army to conduct sustained operations with unified action partners as long as necessary to achieve national objectives.

1-4. Future battlefields will be complex. Enemies will employ a combination of conventional tactics, terrorism, criminal activity, and information warfare to complicate operations. Army forces will have to conduct urban and subterranean operations. Noncombatants will be crowded in and around large and densely populated cities. To an ever-increasing degree, ground operations are inseparable from activities in the information environment. These characteristics present a significant challenge for intelligence as a warfighting function. (See FM 3-0 for more information about large-scale ground combat operations.)

THE OPERATIONAL ENVIRONMENT

1-5. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Commanders at all levels have their own operational environment for their particular operation. An operational environment for a specific operation comprises more than the interacting variables that exist within a specific physical area. It also involves interconnected influences (for example, politics and economics)—globally or regionally—that impact the conditions and operations within that physical area. Thus, each commander's operational environment is part of a higher commander's operational environment.

1-6. An operational environment is complex and dynamic and consists of many relationships and interactions among interrelated variables. Today's information technology makes the information environment, which includes cyberspace and the electromagnetic spectrum (EMS), indispensable to military operations. The information environment is a key part of any operational environment and will remain congested and contested simultaneously during operations. All groups in the information environment—enemy, friendly, or neutral—remain vulnerable to attack by physical, psychological, cyber, or electronic means. Each complex aspect of the operational environment makes intelligence support that much more complex. (See FM 3-12 for more information on cyberspace operations and the EMS.)

OPERATIONAL AND MISSION VARIABLES

1-7. Analysis of the broad aspects of an operational environment in terms of the operational variables provides relevant information that senior commanders use to understand, visualize, and describe the operational environment. The operational variables are political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). Upon receipt of a warning order or mission,

Army leaders filter relevant information and narrow their focus to six mission variables—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). Extensive analysis of the operational and mission variables involves significant intelligence support as intelligence often provides the critical context and cultural understanding necessary to support staff planning and facilitate situational understanding.

Terrain

1-8. Terrain aspects and weather conditions are inseparable, directly influence each other, and impact military operations based on the mission variables (METT-TC). Terrain analysis, also referred to as geospatial analysis, involves the study and interpretation of an area's natural and man-made features, their effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process. The staff geospatial engineer normally analyzes the military aspects of terrain, which include the collection, analysis, evaluation, and interpretation of geospatial information on the terrain's natural and man-made features. Analysts combine other relevant factors with the terrain and weather to predict their effects on military operations. (For more information, see ATP 2-01.3.)

Weather

1-9. Weather analysis is more than just generating weather forecasts. Weather analysis focuses on detailed assessments of weather effects on friendly and threat operations and various systems. Analysts evaluate the effects of each military aspect of weather and focus on the aspects that have the most bearing on operations and decision making. The evaluation of each aspect should begin with operational climatology and current weather forecasts. Analysts fine-tune the evaluation to determine effects based on specific weather sensitivity thresholds for friendly and threat forces and systems. (For more information, see ATP 2-01.3.)

Civil Considerations

1-10. As part of generating intelligence knowledge before receipt of mission, the staff can database and describe civil considerations using the joint systems perspective (see JP 3-0), the operational variables (PMESII-PT), or the ASCOPE (areas, structures, capabilities, organizations, people, and events) characteristics. However, after the receipt of the mission, Army forces use ASCOPE characteristics as part of the mission variables (METT-TC) during intelligence preparation of the battlefield (IPB). The staff and intelligence analysts leverage information from many different sources, including publicly available information, to provide predictive, specific intelligence on ASCOPE characteristics that are significant to the mission. Lower echelon intelligence staffs may have to depend on higher echelon organizations, such as the Defense Intelligence Agency, to provide detailed information and analysis pertaining to civil considerations and sociocultural factors during some types of operations. (For more on ASCOPE and IPB, see ATP 2-01.3.)

Multi-Domain Extended Battlefield

1-11. The interrelationship of the air, land, maritime, space, and cyberspace domains, the information environment, and the EMS requires cross-domain situational understanding of the operational environment. Commanders and staffs must understand the friendly and enemy capabilities and vulnerabilities that reside in each domain. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for the best effects. Since many capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations. Intelligence plays an important role in facilitating situational understanding across all domains. This type of intelligence effort requires time, significant intelligence capabilities, and an analytical focus.

1-12. Since the Army conducts operations across all domains and the information environment, a multi-domain approach to operations is neither new to the Army nor to national to tactical intelligence. Rapid and continued advances in technologies and the military's use of new technologies within the space domain, the EMS, and the information environment (particularly cyberspace) will drive new requirements for special considerations for intelligence, planning, and converging effects from across all domains.

TRENDS

1-13. Several trends will continue to affect future operational environments. The competition for resources, water access, declining birthrates in traditionally allied nations, and disenfranchised groups in many nations contribute to the likelihood of future conflict. Populations will continue to migrate across borders and to urban areas in search of the employment and services urban areas offer. The adversarial use of media platforms to disperse misinformation and propaganda and malign narratives enables adversaries to shape operational environments to their advantage and ferment dissention, unrest, violence, or at the very least, uncertainty.

THREATS AND HAZARDS

1-14. Although threats are a fundamental part of an operational environment for any operation, they are discussed separately here for emphasis; hazard is an important related term that also affects operations:

- 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 (organized or not organized), paramilitary or military forces, nation-states, or national alliances. In general, a threat can be categorized as an enemy or an adversary.
- An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0).
- 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).
- A *hazard* is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation (JP 3-33).

1-15. While ADP 3-0 addresses various threats across the range of military operations, FM 3-0 focuses on peer threats in large-scale ground combat operations. A peer threat is an adversary or enemy with capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with U.S. forces. A peer threat may also have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary. Peer threats generate tactical, operational, and strategic challenges that are an order of magnitude more challenging militarily than those the Army has faced since the end of the Cold War.

1-16. Peer threats employ their resources across multiple domains to attack U.S. vulnerabilities. They use their capabilities to create lethal and nonlethal effects throughout an operational environment. During combat operations, threats seek to inflict significant damage across multiple domains in a short period of time. They seek to delay friendly forces long enough to achieve their goals and end hostilities before friendly forces reach culmination. Peer threats will use various methods to employ their national elements of power to render U.S. military power irrelevant. Five broad peer threat methods, often used in combination, are—

- **Information warfare:** The threat's orchestrated use of information activities (such as cyberspace operations, electronic warfare (EW), and psychological operations) to gain advantage in the information environment.
- **Preclusion:** The threat's use of a wide variety of capabilities to preclude a friendly force's ability to shape the operational environment and mass and sustain combat power. Antiaccess and area denial are two such activities.
- **Isolation:** The threat's containment of a friendly force so the friendly force cannot accomplish its mission. Peer threats will attempt to isolate U.S. forces in several ways. For example, the threat might prevent a friendly force from effectively communicating while also decisively fixing a friendly unit with long-range fires and close combat capabilities.
- **Sanctuary:** The threat's ability to put its forces beyond the reach of friendly forces. It is a form of protection derived by some combination of political, legal, and physical boundaries that restrict freedom of action by a friendly force commander.
- **Systems warfare:** The threat's analysis of the operational environment (including its forces and friendly forces) to identify specific friendly critical capabilities for disruption or destruction in order to cause failure of a larger friendly system.

1-17. Some peer threats have nuclear and chemical weapons capabilities and the ability to employ such weapons in certain situations. However, capability does not equal intent to use, and it is generally presumed that most would use restraint. Preparation and planning that consider nuclear and chemical weapons capabilities are of paramount importance in any confrontation with an adversary armed with them. Understanding threat nuclear and chemical weapons doctrine is important, particularly during large-scale ground combat operations.

1-18. The intelligence warfighting function analyzes nation-states, organizations, people, or groups to determine their ability to damage or destroy life, vital resources, and institutions, or to prevent mission accomplishment. Threats are sometimes categorized as traditional, irregular, disruptive, and catastrophic. While helpful in generally describing the nature of the threat, these categories do not precisely describe the threat's goals, organizations, and methods of operating.

1-19. Intelligence provides a deep understanding of the threat and how the threat can affect mission accomplishment, which is essential to conducting operations. Commanders and staffs must understand how current and potential threats organize, equip, train, employ, and control their forces. Therefore, the intelligence warfighting function must continually identify, monitor, and assess threats as they adapt and change over time. (For more information on threats and hazards see ADP 3-0 and FM 3-0.)

UNIFIED ACTION AND JOINT OPERATIONS

1-20. *Unified action* is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). *Unified action partners* are those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations (ADP 3-0). Army contributions to unified action are called unified land operations (see paragraph 1-28). (For more information, see ADP 3-0.)

1-21. Intelligence is inherently joint, interagency, intergovernmental, and multinational; it flows up and down through the echelons to provide the most complete, timely, accurate, and detailed intelligence possible. The Army provides adaptable intelligence capabilities that are dedicated to both joint and Army forces operating as a part of the joint team. This intelligence effort is synchronized, networked, and includes collaboration with unified action partners to achieve unity of effort and to meet the commander's intent. Intelligence unity of effort is critical to accomplish the mission. Multinational and interagency partners provide unique capabilities that reinforce and complement Army intelligence capabilities, as well as invaluable cultural awareness and different perspectives on the operational environment. Using the appropriate procedures, foreign disclosure guidance, and established policy, Army intelligence leaders provide information and intelligence support to multinational forces against an array of threats across multiple domains.

1-22. *Joint operations* are military actions conducted by joint forces and those Service forces employed in specific command relationships with each other, which of themselves, do not establish joint forces (JP 3-0). Traditionally, campaigns are the most extensive joint operations. In terms of joint large-scale combat operations, a campaign is a series of related major operations achieving strategic and operational objectives within a given time and space. A major operation is a series of tactical actions, such as battles, engagements, and strikes and it is the primary building block of a campaign. Army forces conduct supporting operations as part of a joint campaign.

1-23. Most joint operations share certain activities or actions in common. There are six general groups of military activities that typically occur in preparation for and during a joint large-scale combat operation. These six groups are shape, deter, seize initiative, dominate, stabilize, and enable civil authorities. These six general groups of activities provide a basis for thinking about a joint operation in notional phases. These phases often overlap, and they are not necessarily sequential.

1-24. As a part of joint operations, the Army is the dominant fighting force in the land domain. Across the globe, mission-tailored Army units build partnerships, deter adversaries, and overcome challenges to defeat enemies using simultaneous actions integrated in time, space, and purpose. Army forces both depend on and enable joint forces across all domains and the information environment. This mutual interdependence creates powerful synergies and reflects that all operations have multi-domain components. The Army depends on the

other Services for strategic and operational mobility, joint fires, and other key enabling capabilities like information collection in the deep area. The Army supports other Services, combatant commands, and unified action partners with ground-based indirect fires and ballistic missile defense, defensive cyberspace operations, electronic protection, communications, intelligence, rotary-wing aircraft, logistics, and engineering.

1-25. Joint and Army intelligence staffs, units, and organizations within the theater intelligence architecture operate as mutually supporting entities that ensure information and intelligence are shared across echelons to support commanders at all levels. Intelligence, surveillance, and reconnaissance is an important construct in both joint and Army intelligence. Consistent with joint doctrine, *intelligence, surveillance, and reconnaissance* is an integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations (JP 2-01). The Army continually executes intelligence, surveillance, and reconnaissance worldwide through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging intelligence at each echelon) and information collection.

THE ARMY'S STRATEGIC ROLES

1-26. The Army's primary mission is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. The Army accomplishes its missions by supporting the joint force through the Army's four strategic roles: shape the operational environment, prevent conflict, prevail during large-scale ground combat, and consolidate gains. The strategic roles clarify the enduring reasons for which the Army is organized, trained, and equipped. Figure 1-2 shows the Army's strategic roles in a general relationship to the joint phasing model.

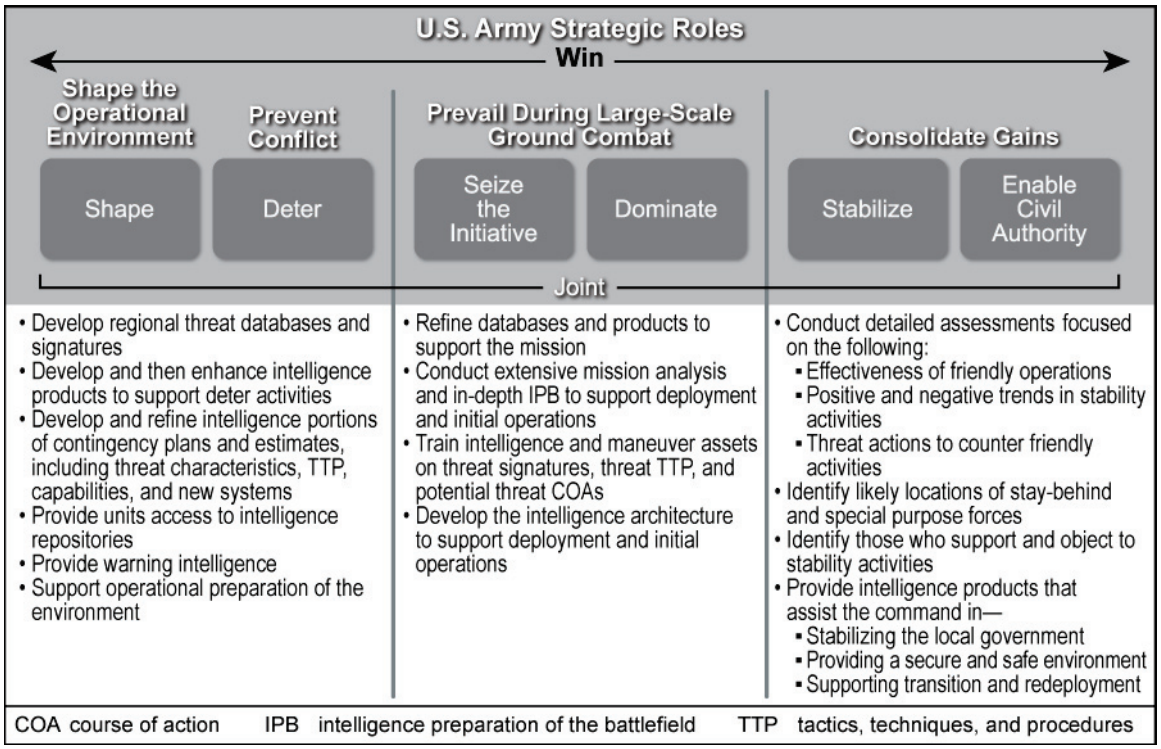


Figure 1-2. The Army's strategic roles and their relationship to the joint phases

1-27. There are requirements for intelligence during each strategic role. Some intelligence activities are specific to certain strategic roles, while others span multiple roles. (See figure 1-2 for some of the most important intelligence tasks for each strategic role.) Commanders and leaders ensure adequate planning for; collection; storage; processing, exploitation, and dissemination (PED); and analysis of information and intelligence during each strategic role. Ideally, regionally aligned forces build on and enhance existing threat data, information, and intelligence during the shaping activities. However, during the shape role, there may be instances in which

regionally aligned forces must develop and populate an authoritative database of threat signatures and associated contextual information, in conjunction with joint forces and the Defense Intelligence Agency. This allows units to access, maintain, populate, and continually update the database throughout all subsequent activities. Commands prepare to establish localized intelligence databases during all activities. It is critical for commands to update the intelligence database continually with actual and potential adversaries to maximize the value of intelligence products and reports.

UNIFIED LAND OPERATIONS

1-28. An *operation* is a sequence of tactical actions with a common purpose of unifying theme (JP 1). Army forces, as part of the joint and multinational force, contribute to the joint mission through the conduct of unified land operations. Unified land operations is the Army's operational concept and contribution to unified action; it is how the Army applies combat power. *Unified land operations* is the simultaneous execution of offense, defense, stability, and defense support of civil authorities across multiple domains to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action (ADP 3-0). The goal of unified land operations is to establish conditions that achieve the joint force commander's end state by applying landpower as part of a unified action to defeat the enemy. Military forces seek to prevent or deter threats through unified action, and, when necessary, execute operations to defeat aggression.

1-29. Land operations, particularly large-scale ground combat operations, focus on destroying or dislocating enemy forces or securing key land objectives that reduce the enemy's ability to conduct operations. Five characteristics distinguish land operations: scope, duration, terrain, permanence, and civilian presence. The characteristics of land operations contribute to the complexity and uncertainty of the environment in which Army forces conduct operations. Land operations against a peer threat (highly adaptive and technologically advanced) are especially challenging. At the beginning of a conflict, peer threats often occupy a position that greatly complicates Army forces' ability to conduct operations.

1-30. Peer threats are developing the capability to mass effects across multiple domains at a speed that will impact ongoing operations. They will most likely attempt to deny U.S. and multinational forces access to their territory. Once Army forces achieve access, the threat will attempt to deny them freedom of maneuver. Future adversaries are likely to use offensive cyberspace operations and counter-space measures to deny and degrade U.S. forces' maneuver, communications, intelligence collection, and targeting capabilities. Land-based threats will impede joint force freedom of movement and action across all domains and the information environment.

DECISIVE ACTION

1-31. Within unified land operations, Army forces conduct decisive action. *Decisive action* is the continuous, simultaneous combinations of offensive, defensive, and stability operations or defense support of civil authorities tasks (ADP 3-0). In unified land operations, commanders seek to seize, retain, and exploit the initiative while synchronizing their actions to achieve the best effects possible. Operations conducted outside the United States and its territories simultaneously combine three elements—offense, defense, and stability. Within the United States and its territories, decisive action combines the elements of defense support of civil authorities (DSCA) and, as required, offense and defense to support homeland defense. (See table 1-1 on page 1-8.)

1-32. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to visualize the operational environment and disrupt the threat simultaneously throughout the area of operations (AO) or perform the necessary stability tasks to consolidate gains. Collecting the intelligence required is often more complex and requires leveraging national to tactical intelligence capabilities. Commanders must be more involved in and knowledgeable of the intelligence warfighting function due to the complexity of operations. The following list provides some basic aspects of intelligence (discussed in more detail in subsequent chapters):

- The Army recognizes the function of intelligence as an element of combat power through the designation of the intelligence warfighting function.
- Intelligence is requirement-driven, and the commander drives intelligence primarily through clear, feasible, and focused requirements.

- The collection of information to support the production of intelligence is called information collection.
- There are many different intelligence analytical tasks such as generate intelligence knowledge, IPB, situation development, and intelligence support to targeting and information operations.
- The general intelligence capabilities employed by the commander and staff are: intelligence analysis elements, PED elements, and military intelligence (MI) units. These general capabilities consist of specific collectors or platforms with specific technical capabilities or sensors.

1-33. It is critical for the intelligence staff to support the commander's ability to visualize threats and relevant aspects of the operational environment during the conduct of decisive operations. However, information requirements, information collection tactics and techniques, the theater intelligence architecture, the nature of intelligence analysis, the employment of MI units, and specific tactics and techniques differ significantly depending on the specific decisive action task.

Table 1-1. Elements of decisive action

Offense	*Defense*
Types of offensive operations:	**Types of defensive operations**
• Movement to contact • Attack • Exploitation • Pursuit	• Mobile defense • Area defense • Retrograde
Purposes:	**Purposes:**
• Dislocate, isolate, disrupt, and destroy enemy forces • Seize key terrain • Deprive the enemy of resources • Refine intelligence • Deceive and divert the enemy • Provide a secure environment for stability tasks	• Deter or defeat enemy offense • Gain time • Achieve economy of force • Retain key terrain • Protect the population, critical assets, and infrastructure • Refine intelligence
Stability	***Defense support of civil authorities***
Stability operations tasks:	**Defense support of civil authorities tasks:**
• Establish civil security • Establish civil control • Restore essential services • Support to governance • Support to economic and infrastructure development • Conduct security cooperation	• Provide support to domestic disasters • Provide support for domestic, chemical, biological, radiological, and nuclear incidents • Provide support for domestic civilian law enforcement agencies • Provide other designated support
Purposes:	**Purposes:**
• Provide a secure environment • Secure land areas • Meet the critical needs of the population • Gain support for host-nation government • Shape the environment for interagency and host-nation success • Promote security, build partner capacity, and provide access • Refine intelligence	• Save lives • Restore essential services • Maintain or restore law and order • Protect infrastructure and property • Support maintenance or restoration of local government • Shape the environment for intergovernmental success

Offense

1-34. An *offensive operation* is an operation to defeat and destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). Offensive operations impose the commander's will on the enemy. The offense is the most direct means of seizing, retaining, and exploiting the initiative to gain a physical and psychological advantage. In the offense, the decisive operation is a sudden action directed toward enemy vulnerabilities and capitalizing on speed, surprise, and shock. If that operation fails to destroy the enemy, operations continue until enemy forces are defeated. Executing offensive operations compels the enemy to react, creating new or larger vulnerabilities the attacking force can exploit. (See ADP 3-90 for a detailed discussion of offensive operations.)

1-35. Offensive operations at all levels require effective intelligence to assist the commander in avoiding the threat's main strength and to deceive and surprise the threat. The entire staff, led by the intelligence staff, develops IPB products to assist the commander in identifying all aspects in the area of interest that can affect mission accomplishment within all domains. The IPB process is collaborative and requires information from all staff elements and some subordinate units that use IPB results and products for planning.

1-36. The intelligence staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat courses of action (COAs). These assets also collect information concerning the civil considerations within the AO. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements.

Defense

1-37. A *defensive operation* is an operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (ADP 3-0). Normally, the defense cannot achieve a decisive victory. However, it sets conditions for a counteroffensive or a counterattack that enables forces to regain the initiative. Defensive operations are a counter to an enemy offensive action. They defeat attacks, destroying as much of the attacking enemy as possible. They also preserve control over land, resources, and populations. The purpose of defensive operations is to retain key terrain, guard populations, protect lines of communications, and protect critical capabilities against enemy attacks. Commanders can conduct defensive operations to gain time and economize forces so offensive operations can be executed elsewhere. (See ADP 3-90 for a detailed discussion of defensive operations.)

1-38. The intelligence staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat COAs. Defending commanders can then decide where to arrange their forces in an economy-of-force role to defend and shape the battlefield. Intelligence analysis assists commanders in deciding on the precise time and place to counterattack. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements.

Stability

1-39. A *stability operation* is an operation conducted outside of the United States in coordination with other instruments of national power to establish or maintain a secure environment, provide essential government services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-0). These operations support governance by a host nation, an interim government, or a military government. Stability involves coercive and constructive actions. Stability assists in building relationships among unified action partners and promoting U.S. security interests. It can help establish political, legal, social, and economic institutions in an area while supporting transition of responsibility to a legitimate authority. Commanders are legally required to conduct minimal-essential stability tasks when controlling populated AOs. These tasks include providing security, food, water, shelter, and medical treatment.

1-40. For stability operations, commanders often require more detailed intelligence and IPB products to determine how best to conduct operations and influence the local populace to enhance stability. The identification and analysis of threats, terrain and weather, and civil considerations are critical in determining the most effective missions, tasks, and locations to conduct specific stability tasks. A lack of knowledge concerning insurgents, local politics, customs, culture, and how to differentiate between local combatants often leads to U.S. actions that can result in unintended and disadvantageous consequences. Consequences can include attacking unsuitable targets or offending or causing mistrust among the local population. This lack of knowledge could potentially threaten mission accomplishment. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements. (For more information on stability operations, see ADP 3-07.)

Defense Support of Civil Authorities

1-41. *Defense support of civil authorities* is support provided by United States Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events (DODD 3025.18).

1-42. DSCA is a task executed in the homeland and U.S. territories. It is conducted to support another primary agency, lead federal agency, or local authority. When DCSA is authorized, it consists of four tasks (see table 1-1 on page 1-8). (See DODD 3025.18 for the full name and discussion of each task.) National Guard forces—Title 32 or state active forces under the command and control of the governor and adjutant general—are usually the first forces to respond on behalf of state authorities. When Federal military forces are employed for DCSA activities, they remain under Federal military command and control at all times. (See JP 3-28 and ADP 3-28 for detailed DSCA discussions.)

1-43. The concepts and basic processes used to produce intelligence to support decision making for DSCA are no different from those used during offensive, defensive, and stability operations. However, the operational environment is significantly different, and all commanders must ensure intelligence support in DSCA remains within the guidelines of U.S. law and applicable policies.

1-44. Following DODM 5240.01, for procedures 1 through 10; DOD 5240.1-R, procedures 11 through 15; and AR 381-10 procedures ensures adherence to regulations, statutes, and laws concerning intelligence activities. In particular, intelligence operations must adhere to regulations and directives that implement restrictions in compliance with intelligence oversight requirements. Further, any use of intelligence capabilities for purposes other than those designated in the Chairman, Joint Chiefs of Staff Standing DSCA Execute Order must be expressly approved by the Secretary of Defense. Information collection conducted to support the commander focuses on saving lives and reducing risk to Army forces. Commanders and intelligence professionals consult with staff judge advocates concerning any unclear areas of intelligence activities.

1-45. The intelligence process, some information collection units and systems, and intelligence analysis may assist in supporting the four DSCA core tasks. Army National Guard activities in Title 32, United States Code (USC), status and Regular Army and Army Reserve intelligence activities in Title 10, USC, status can perform intelligence tasks that support DSCA. (See ATP 2-91.7 for more information.)

Intelligence Support Within Multi-Domain Operations

1-46. Army operations and battles will invariably involve challenges across multiple domains. All Army operations are multi-domain operations and all battles are multi-domain battles. Examples of Army multi-domain operations and activities include airborne and air assault operations, air and missile defense, fires, aviation, cyberspace electromagnetic activities, information operations, space operations, military deception, and information collection. Key considerations for operating in multiple domains are—

- Command and control.
- Reconnaissance in depth.
- Mobility.
- Cross-domain fires.
- Tempo and convergence of effects.
- Protection.
- Sustainment.
- Information operations.
- Cyberspace electromagnetic activities.

1-47. Army forces may be required to conduct operations across multiple domains to gain freedom of action for other members of the joint force. This is similar to other members of the joint force operating across multiple domains to assist in providing land forces with positions of relative advantage. Examples of these operations include neutralizing enemy integrated air defenses, destroying long-range surface-to-surface fires systems, denying enemy access to an AO, disrupting enemy command and control, protecting friendly networks, conducting tactical deception, or disrupting an enemy's ability to conduct information warfare.

1-48. Every echelon is affected by the multi-domain extended battlefield; each should consider time, geography, decision making, the EMS, and the other domains differently. However, not every echelon is able to effectively conduct operations across multiple domains. Brigade combat teams (BCTs) and lower echelons focused on fighting in the close area generally lack the time and ability to effectively plan and employ multi-domain capabilities other than those already under their control. These echelons focus on fundamental operational aspects such as mobility, lethality, and protection. The division is the first echelon able to effectively plan and coordinate for the employment of all multi-domain capabilities across the operational framework (including the considerations—physical, temporal, virtual, cognitive). Theater army and corps echelons have a broader perspective, better focus, and far more capabilities to orchestrate and converge multi-domain activities and operations in time and space. Through these activities and operations, intelligence is critical in assisting friendly forces to effectively identify and exploit windows of opportunity across the domains to create and exploit temporary windows of superiority. (See FM 3-0 for more information on the multi-domain extended battlefield and operational framework.)

1-49. These operations require a significant amount of detailed intelligence to facilitate the commander's visualization of the threat, threat capabilities, and relevant aspects of the operational environment in time and space. This intelligence support assists commanders and staffs in deciding when and where to concentrate sufficient combat power to defeat the threat while mitigating risk.

This page intentionally left blank.

Chapter 2

Intelligence Support

Army intelligence as a function supports operations by accomplishing various intelligence tasks and activities for commanders and staffs. To provide this support, the intelligence staff, augmented with an analysis element and capabilities, performs intelligence analysis to support the commander and command and control, including the staff integrating processes. MI units collect information from across the operational environment and in each domain and the information environment. The results from this information collection effort provide information for analysis and production into intelligence. This intelligence support occurs at each echelon, from theater army down to the battalion level, within an overarching national to tactical intelligence architecture. Together with the commander, staff, and all units, this functional system is known as the Army intelligence warfighting function.

THE PURPOSE OF INTELLIGENCE

2-1. Intelligence is a product, a process, and a function that enables the Army to conduct operations by supporting the commander and command and control (which is accomplished by supporting the rest of the staff). Commanders and staffs rely on many different types of intelligence products. The intelligence process is continuous and directly supports the operations process by developing information requirements, collecting on those requirements, processing data into information, analyzing information and intelligence from all sources, producing intelligence, and when necessary, developing the situation through operations. Intelligence is also a complex function.

2-2. Intelligence supports commanders (and in some cases other decision makers) and staffs by providing situational understanding of the threat, terrain and weather, civil considerations, and other aspects of the operational environment. Intelligence supports the commander and staff with analysis and production of effective timely, relevant, accurate, and predictive assessments and products tailored to the commander's and staff's specific needs.

2-3. Intelligence drives operations and operations enable intelligence; this relationship is continuous. Intelligence supports the planning, preparing, execution, and assessment of operations by supporting command and control. The command and control warfighting function integrates the elements of combat power across the warfighting functions. To ensure effective intelligence support, commanders and staffs must understand the interrelationship of command and control, the intelligence warfighting function, and fundamental intelligence doctrine. (See figure 2-1.) (See ADP 6-0.)

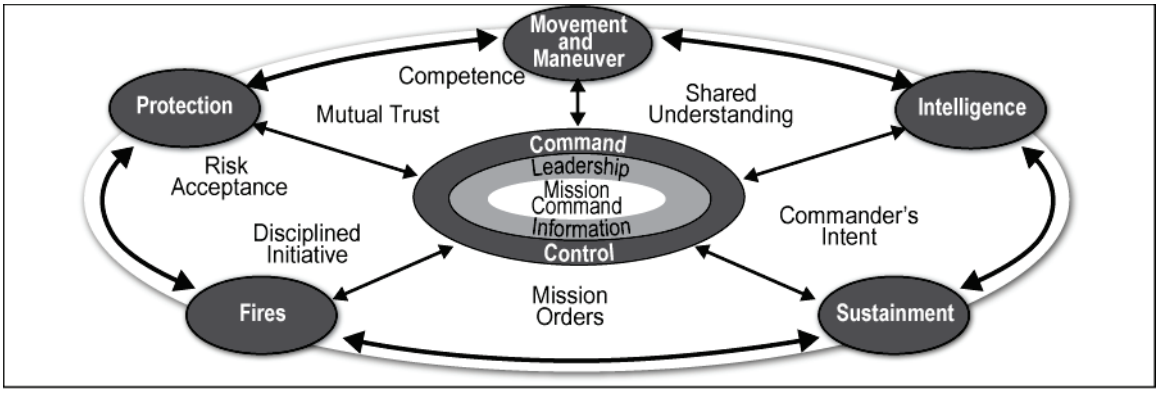


Figure 2-1. Interrelationship of command and control and the warfighting functions

2-4. Commanders require intelligence about the threat and other aspects of the operational environment before and during operations to effectively accomplish their missions. Intelligence assists commanders in visualizing the operational environment, organizing their forces, and controlling operations to achieve their objectives by answering specific requirements focused in time and space. These intelligence products enable commanders to make decisions based on all available information, identify and assess potential COAs, plan operations, properly direct their forces, and employ ethical, effective, and efficient tactics and techniques. Additionally, intelligence supports protection by alerting commanders to threats and assisting in preserving and protecting the force.

2-5. Supporting command and control and the staff integrating functions is complex. Operations, targeting, intelligence, and communications are inextricably linked. Therefore, the commander must drive the operations process partially by enabling the intelligence warfighting function. Commanders use their staff to synchronize intelligence with the other warfighting functions to visualize the operations and disrupt the threat simultaneously throughout an AO. Successful intelligence is the result of carefully developed requirements, staff integration and synchronization, continuous information collection, and, when necessary, the willingness to fight for intelligence.

2-6. Intelligence leaders (both in the intelligence staff and in MI units) ensure that the intelligence warfighting function operates effectively and efficiently. They are the commander's primary advisors on information requirements, intelligence analysis, employing information collection assets, and fighting for intelligence. Intelligence analysis is a thorough and deliberate process. Intelligence leaders provide the commander with predictive assessments that consider all aspects of the threat, terrain and weather, and civil considerations, and should provide the commander with an estimate about the degree of confidence the intelligence leader places on each analytic assessment.

THE INTELLIGENCE WARFIGHTING FUNCTION

2-7. The intelligence warfighting function is the Army's contribution to the joint intelligence effort. 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 operational environment (ADP 3-0). Specifically, other significant aspects of the operational environment include threats, adversaries, the operational variables, and can include other aspects depending on the nature of operations.

2-8. The intelligence warfighting function encompasses more than the MI branch:

- The commander drives the operations process and focuses the intelligence effort that supports it.
- Intelligence is commander-centric. The commander performs the central role within intelligence and enables the intelligence warfighting function.
- The entire staff is important to the intelligence warfighting function and each staff member contributes to intelligence in a different way.
- During combat operations, the G-2/S-2, G-3/S-3, G-6/S-6, and fire support coordinator form the staff core that is essential to synchronize and integrate intelligence.
- Every Soldier contributes to information collection.

INTELLIGENCE WARFIGHTING FUNCTION TASKS

2-9. The intelligence warfighting function facilitates support to the commander and staff through a broad range of supporting Army Universal Task List (AUTL) tasks. (See ADRP 1-03.) These tasks are interrelated, require the participation of the commander and staff, and are often conducted simultaneously. The intelligence warfighting function tasks facilitate the commander's visualization and understanding of the threat and other relevant aspects of the operational environment. Army units at the Army Service component command (ASCC) level or formed as a joint task force use the Universal Joint Task List (also called UJTL). The intelligence warfighting function includes the following tasks:

- **Provide intelligence support to force generation**—the task of generating intelligence knowledge concerning an operational environment, facilitating future intelligence operations, and tailoring the force.
- **Provide support to situational understanding**—the task of providing information and intelligence to commanders to assist them in achieving a clear understanding of the force's current state with relation to the threat and other relevant aspects of the operational environment.
- **Conduct information collection**—the task that synchronizes and integrates the planning and employment of sensors and assets as well as the PED systems in direct support of current and future operations.
- **Provide intelligence support to targeting and information operations**—the task of providing the commander information and intelligence support for targeting to achieve lethal and nonlethal effects.

2-10. Table 2-1 illustrates how the intelligence warfighting function tasks support the commander. (See ADRP 1-03 for the complete list of tasks and their measures of performance.)

Table 2-1. Overview of intelligence warfighting function tasks

Intelligence tasks ►	*Commander's focus ►*	*Commander's decisions*
Provide intelligence support to force generation: • Provide intelligence readiness. • Establish an intelligence architecture. • Provide intelligence overwatch. • Generate intelligence knowledge. • Tailor the intelligence force.	Orient on contingencies.	• Should the unit's level of readiness be increased? • Should the operation plan be implemented?
Provide support to situational understanding: • Perform IPB. • Perform situation development. • ~~Provide intelligence support to protection.~~ • Provide tactical intelligence overwatch. • Conduct police intelligence operations. • Provide intelligence support to civil affairs operations.	• Plan an operation. • Prepare. • Execute. • Assess. • Secure the force. • Determine 2d and 3d order effects on operations and the populace.	• Which COA will be implemented? • Which enemy actions are expected? • What mitigation strategies should be developed and implemented to reduce the potential impact of operations on the population?
Conduct information collection: • Collection management. • Direct information collection. • Execute collection. • Conduct intelligence-related missions and operations.	• Plan information collection for an operation, including PED requirements. • Prepare. • Execute. • Assess.	• Which DPs, HPTs, and HVTs are linked to the threat's actions? • Are the assets available and in position to collect on the DPs, HPTs, and HVTs? • Have the assets been repositioned for branches or sequels?
Provide intelligence support to targeting and information operations: • Provide intelligence support to targeting. • Provide intelligence support to information operations. • Provide intelligence support to combat assessment.	• Create lethal or nonlethal effects against targets. • Destroy, suppress, disrupt, or neutralize targets. • Reposition intelligence or attack assets.	• Are the unit's lethal and nonlethal actions and maneuver effective? • Which targets should be re-engaged? • Are the unit's information operations effective?

COA	course of action	HVT	high-value target
DP	decision point	IPB	intelligence preparation of the battlefield
HPT	high-payoff target	PED	processing, exploitation, and dissemination

2-11. There are intelligence-related AUTL tasks beyond the four most significant intelligence warfighting tasks in table 2-1. Soldiers, systems, and units from all branches conduct intelligence-related AUTL tasks. Every Soldier, as a part of a small unit, is a potential information collector. Soldiers develop a special awareness simply due to exposure to events occurring in the AO, and they can collect and report information based on their observations and interactions with the local population. The increased awareness that Soldiers develop through personal contact and observation is a critical element of the unit's ability to understand the operational environment more fully.

2-12. Therefore, the Army established the *every Soldier is a sensor* (known as ES2) program, which is accomplished through information collection operations among populations. The AUTL task to establish a mission intelligence briefing and debriefing program is designed to assist units in collecting useful information in their AO more effectively. This task is critical because units often operate in an AO characterized by violence, uncertainty, and complex threats. (See ATP 3-55.4.)

2-13. Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See the DOD Law of War Manual and CJCSI 3121.01B [classified].) In some cases, there are certain sensitivities, ethical considerations, and limitations to personnel conducting information collection—for example, civil affairs and medical Soldiers. Medical personnel cannot be assigned information collection tasks due to their Geneva Convention category status. If medical personnel do gain information through casual observation of activities in plain sight while conducting their duties, they will report the information to their chain of command. In all cases, Army professionals base their decisions and actions on the moral principles of the Army Ethic, ensuring the protection of the inalienable rights of all people.

INTELLIGENCE CORE COMPETENCIES

2-14. The intelligence core competencies are the most basic activities and tasks the Army uses to describe and drive the intelligence warfighting function and leverage national to tactical intelligence. At the most basic level, the intelligence warfighting function makes observations about the threat and relevant aspects of the operational environment through **collection** resulting in data that it **processes and exploits** into useable information for **analysis and production**. This results in intelligence. Because of the complexity of this undertaking, the entire effort must be **synchronized** carefully. The four aspects (in bold) capture the intelligence core competencies. Commanders and staffs must thoroughly understand the core competencies to apply the intelligence process and leverage national to tactical intelligence. The intelligence core competencies are—

- Intelligence synchronization (**synchronized**).
- Intelligence operations (**collection**).
- Intelligence PED (**processes and exploits**).
- Intelligence analysis (**analysis and production**).

2-15. The intelligence core competencies also serve as those areas that all MI units and Soldiers must continuously train on to maintain a high degree of proficiency. Intelligence professionals have unique technical training, intelligence oversight, and other oversight requirements in order to operate as part of the DOD intelligence effort. MI Soldiers must continuously and rigorously train to thoroughly understand unique authorities and guidelines, terms, and technical channel procedures.

Intelligence Synchronization

2-16. ***Intelligence synchronization*** **is the art of integrating information collection; intelligence processing, exploitation, and dissemination; and intelligence analysis with operations to effectively and efficiently fight for intelligence in support of decision making.** This core competency ensures the intelligence warfighting function supports command and control. Intelligence synchronization balances time with collection, production, required accuracy, and specificity to meet the commander's intent and other requirements.

2-17. Intelligence synchronization requires an effective relationship with the commander, focused information collection, effective dissemination of predictive assessments, and adaptability to changing situations. Some critical aspects of effective intelligence synchronization include—

- Early and continuous teamwork with the commander and across the staff.
- Expertise and proficiency in information collection, PED, and leveraging national to tactical intelligence.
- Mastery of the intelligence process.
- A collaborative environment for flexible, creative analysts to solve complex problems.

Intelligence Operations

2-18. Intelligence operations is one of the four primary means for information collection. The other three are reconnaissance, surveillance, and security operations. ***Intelligence operations*** **are the tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements.** These requirements are normally specified in the information collection plan. Intelligence operations collect information about the intent, activities, and capabilities of threats and relevant aspects of the operational environment to support commanders' decision making.

2-19. Intelligence operations, like reconnaissance, surveillance, and security operations, are shaping operations used by the commander for decisive action. MI units use the operations process to conduct intelligence operations. Intelligence operations are conducted using mission orders and standard command and support relationships. Flexibility and adaptability to changing situations are critical for conducting effective intelligence operations. To plan and then remain flexible and adaptable, MI units and the intelligence staff must carefully deconflict and coordinate intelligence operations.

2-20. Deconfliction and coordination require a series of related activities that facilitate operations in another unit's AO. These activities facilitate successful intelligence operations and fratricide avoidance. At a minimum, MI units coordinate for and report their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission. When possible, MI units and the intelligence staff should conduct a thorough face-to-face coordination.

2-21. MI units must also coordinate with the appropriate staff elements to establish fire support coordination measures around information collection assets, airspace control measures, and the appropriate weapons control status (in reference to aerial information collection assets). Failure to conduct proper deconfliction and coordination may result in mission failure or unnecessary risk to personnel. MI units' leadership also coordinates with the supported unit's intelligence section for debriefings of returning members, convoy leaders, and others.

2-22. Intelligence coordination is also conducted by the intelligence staff to facilitate active collaboration, laterally and vertically. It includes establishing and maintaining technical channels to direct, refine, and focus intelligence operations. (See paragraphs 4-11 through 4-13 and FM 2-0 for more on technical channels.)

Intelligence Processing, Exploitation, and Dissemination

2-23. Army doctrine has long recognized the functions of processing, initial analysis, and reporting, and the requirement for providing combat information. Joint and Army doctrine currently recognizes these functions under the concept of PED and the core capability of intelligence PED. In joint doctrine, PED is an intelligence concept that facilitates the allocation of assets to support intelligence operations. Under the joint PED concept, planners examine all collection assets and determine if allocation of additional personnel and resources is required to exploit the collected information.

2-24. Beyond doctrine, PED plays an important role in the development of DOD intelligence capabilities. PED began as processing and intelligence exploitation support for unique systems and capabilities—for example, full motion video from unmanned aircraft systems. Unlike previous geospatial intelligence (GEOINT) collection capabilities, full motion video did not have an automated capability to process raw data into a useable format and supporting personnel to perform initial exploitation. Therefore, a separate PED capability was required. Since 2006, PED requirements across multiple disciplines have grown significantly, and DOD has created many different PED capabilities across various echelons.

2-25. ***Processing, exploitation, and dissemination*** **is the execution of the related functions that converts and refines collected data into usable information, distributes the information for further analysis, and, when appropriate, provides combat information to commanders and staffs**. PED is not exclusive to MI organizations; other branches employ sensor collection capabilities. Therefore, PED conducted by intelligence personnel or units is called *intelligence PED*. Intelligence PED facilitates efficient use and distribution of information following collection. In essence, intelligence PED is the way the intelligence warfighting function processes collected data and information, performs an initial analysis (exploitation), and provides information in a useable form for further analysis. During intelligence PED, some information will be identified as combat information. In those cases, the combat information will be disseminated to commanders and staffs.

2-26. An important part of intelligence PED is ensuring information is distributed with adequate context and formatted to facilitate understanding or make subsequent analysis easier. Another important aspect of PED is providing feedback on the effectiveness of collection relative to the information collection plan and expected results. All PED methods are related closely to planning, information collection, control via technical channels, and intelligence analysis and production requirements. Receiving feedback gives leaders and staffs the information needed to maintain synchronization of intelligence operations with the overall operation. This synchronization may include retasking MI collection assets or cueing other MI collection capabilities.

2-27. The current approach to intelligence PED reflects a deliberate solution to the increased complexity of intelligence operations and the explosion of available data and information resulting from information collection. This approach is part of meeting the enduring challenge to get the right information to the right place at the right time. The amount of available data and information will continue to grow exponentially. In response, the Army is emphasizing PED resourcing, planning, and execution, and maintaining a continuous assessment of its usefulness. This approach is resourced with and executed by a variety of intelligence PED capabilities leveraged throughout the Army and intelligence community.

Intelligence Analysis

2-28. Analysis is the basis for planning and staff activities. Analysis facilitates commanders' and other decision makers' ability to visualize the operational environment, organize their forces, and control operations in order to achieve their objectives.

2-29. Intelligence analysis is specific to the intelligence warfighting function and results in the production of timely, accurate, relevant, and predictive intelligence. ***Intelligence analysis*** **is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production**. The purpose of intelligence analysis is to describe the current—and attempt to proactively assess—threats, terrain and weather, and civil considerations. Intelligence analysis sets the stage for the development of information collection requirements, which result in information collection and then more intelligence analysis; this relationship is continuous. (See ATP 2-33.4 for more on intelligence analysis.)

2-30. Intelligence analysis is continuous, complements intelligence synchronization, and enables operations. Some aspects that enable effective staff support and intelligence analysis include—

- **Critical thinking.** Critical thinking is essential to analysis. Using critical thinking, which is disciplined and self-reflective, provides more holistic, logical, ethical, and unbiased analysis and conclusions. Applying critical thinking ensures analysts fully account for the elements of thought, the standards of thought, and the traits of a critical thinker.
- **Embracing ambiguity.** Well-trained analysts are critical due to the nature of changing threats and operational environments. They must embrace ambiguity, and recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn during analysis.
- **Collaboration.** Commanders, intelligence and other staffs, and intelligence analysts collaborate. They actively share and question information, perceptions, and ideas to better understand situations and produce intelligence. Collaboration is essential to analysis; it ensures analysts work together to effectively and efficiently achieve a common goal. Often analytical collaboration is enabled by DOD intelligence capabilities.

NATIONAL TO TACTICAL INTELLIGENCE

2-31. National to tactical intelligence comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. While there are many aspects to national to tactical intelligence, the most important element of the intelligence effort is the people that make it work. The intelligence warfighting function is the Army's contribution to national intelligence.

2-32. The value of the national to tactical intelligence effort is the ability it provides to leverage information from all unified action partners, including access to national capabilities, as well as nonintelligence information, larger volumes of information and intelligence, and specialized analysis by unified action partners. Collaboration is the central principle of conducting analysis. Army units provide accurate and detailed intelligence on the threats and relevant aspects of the operational environment (especially those related to Army activities), while other portions of the DOD intelligence effort provide expertise and access not readily available to the Army. Additionally, DOD agencies provide governance over certain intelligence methods and activities. Cooperation benefits everyone.

2-33. Analysts leverage higher-level intelligence organizations to create a more comprehensive and detailed assessment of threats and relevant aspects of the operational environment (such as the multi-domain extended battlefield, civil considerations, and sociocultural factors) to facilitate situational understanding and visualization of the AO. An example of achieving greater efficiency between the intelligence and command and control warfighting functions is the creation of fusion centers. Fusion centers are ad hoc cells designed to enable targeting, facilitate current or future operations, and inform decision making. (See FM 2-0 for more information on fusion centers.)

2-34. The effectiveness of the intelligence warfighting function hinges directly on collaboration and unity of effort within the intelligence community. Numerous DOD and non-DOD agencies and organizations in the intelligence community support Army operations by providing specific intelligence products and services. The intelligence community has become increasingly important as new technologies facilitate collaborative analysis and production. DOD members include the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and Army, Navy, Air Force, and Marine Corps Intelligence. Non-DOD members include the Central Intelligence Agency, Department of State, Department of Energy, Federal Bureau of Investigation, Department of the Treasury, U.S. Coast Guard Intelligence, Department of Homeland Security, the Drug Enforcement Administration, and the Office of Director of National Intelligence. Intelligence community members establish standards in their respective specialties. Effective intelligence staffs are familiar with these organizations and the methods of obtaining information from them as necessary. (See JP 2-0.)

Note. *Intelligence community* is all departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role (JP 2-0).

NATIONAL AND JOINT INTELLIGENCE

2-35. National intelligence organizations employ specialized resources and dedicated personnel to collect intelligence worldwide about trends, threats and threat capabilities, events and activities, and other national intelligence requirements. National intelligence organizations primarily support national decision makers, while also routinely providing support to the joint force commander. However, depending on the situation, the focus of this national-level intelligence collection and production may meet some Army service needs.

2-36. The United States Army Intelligence and Security Command (INSCOM) is a direct reporting unit to the Army Deputy Chief of Staff for Intelligence, who conducts and synchronizes worldwide intelligence collection across all disciplines and all-source analysis activities. The Army, in response to validated requirements, may provide the theater and joint force with intelligence capabilities resident within INSCOM. INSCOM also delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, unified action partners, and the U.S. intelligence community.

2-37. There are two types of units assigned to INSCOM: military intelligence brigades-theater (MIB-Ts) and functional commands. There are seven MIB-Ts, each one tailored for the combatant command it supports. These brigades provide collection, processing, analysis, and dissemination support to the ASCCs, combatant commanders, and the intelligence community. INSCOM MIB-Ts are assigned through the appropriate joint documentation process to geographic combatant commands (GCCs). GCCs routinely provide these brigades in an operational control relationship to the supporting ASCCs.

2-38. INSCOM's functional brigades and groups may provide general support, general support reinforcing, or direct support to theaters of operations through intelligence reach, or they may be force tailored for deployment to support the joint force. These brigades and groups, while not regionally aligned, work in coordination with INSCOM's MIB-Ts to effectively create a seamlessly integrated tactical to national intelligence architecture. Functional commands within INSCOM have missions and capabilities focused on a single discipline or operational function. Examples of this type of command include the—

- 902d MI Group (counterintelligence [CI]).
- Army GEOINT Battalion.
- Army Operations Group (human intelligence [HUMINT]) operating in direct support of Army requirements.
- 704th MI Brigade providing signals intelligence (SIGINT) functional capabilities to support national and Army requirements.
- 116th Aerial Intelligence Brigade (aerial intelligence, surveillance, and reconnaissance and associated PED) to support combatant command and Army requirements.
- National Ground Intelligence Center (NGIC), which is the Army's service intelligence production center in response to national and Army requirements.
- Army Field Support Center.

REGIONALLY ALIGNED FORCES AND SETTING THE THEATER

2-39. *Regionally aligned forces* are those forces that provide a combatant commander at up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions (FM 3-22). Regionally aligned forces also include capabilities that are Service-retained but aligned with a combatant command. Regional missions include theater security cooperation and other shaping efforts. A large portion of joint and Army intelligence is regionally aligned.

2-40. Regionally aligned forces and other specified Army units require ready access to and seamless interaction with their associated combatant command's intelligence architecture. When an Army headquarters enters a GCC theater as a joint force command, joint task force, or combined joint task force, it primarily receives intelligence support through the joint intelligence architecture. Specifically, the GCC joint intelligence center/joint intelligence operations center (also called JIC/JIOC) provides all-source intelligence support unless another support relationship is established. Other Army units within the GCC depend on the combatant command's MIB-T for situational awareness throughout the area of responsibility. This relationship allows units to tailor mission planning and training, establish an effective intelligence architecture, and leverage DOD intelligence effectively. This concept refers to the MIB-T as the anchor point within that specific theater.

2-41. The intelligence warfighting function must constantly set the theater for all Army forces across all echelons of a deployed force in theater. Intelligence staffs and MI units must carefully transition intelligence capabilities and activities to support all engagements and operations as the Army moves from shape to prevent to prevail in large-scale ground combat and to consolidate gains. There are three core tasks involved in setting the theater:

- The intelligence staff plans, builds, and evolves an intelligence architecture based on the information collection, PED, and analysis capabilities allocated or requested to support operations.
- The intelligence staff builds the knowledge needed to understand the operational environment through coordination and collaboration with regionally aligned forces, using the MIB-T as the anchor point. This task includes connecting the intelligence architecture to and incorporating reports and products into the command and control systems.
- The intelligence staff supports theater security cooperation and engagements that develop context and build relationships with unified action partners through the successful conduct of intelligence operations, intelligence analysis, and intelligence PED.

ESTABLISHING THE INTELLIGENCE ARCHITECTURE

2-42. The intelligence architecture is the compilation and interrelationship of all relevant intelligence and communications capabilities, data centers, organizations, supporting capabilities, concepts of operations, and personnel necessary to ensure the successful execution of the intelligence process. It connects the units, capabilities, PED activities, and analysts whose products and assessments inform decision makers. The architecture consists of more than a unit's organic intelligence capabilities, systems, and personnel. It includes all elements of the intelligence network and associated communications architectures required to enable intelligence operations to support mission requirements. (See FM 2-0 for more on intelligence units, general capabilities, collectors and platforms, and specific technical capabilities and sensors.)

2-43. Planning the intelligence architecture is inseparable from long-range planning for future intelligence operations. It is tied directly to the types and methods of support the commander directs. It is roughly equivalent to developing a blueprint for a house and gathering the materials to build the house. The unit cannot count on support from intelligence capabilities unless they are included in the intelligence architecture and supported by interoperable communications.

2-44. The intelligence staff portrays the intelligence architecture in a series of planning products that map the operational and technical aspects of the interoperability between the many components of the architecture. The architecture includes but is more encompassing than the different intelligence, communications, and technical networks. (Technical networks are those information management and information system connections that allow sharing of resources and information.) Intelligence architecture products capture not only networks and their technical specifications but also how the elements of the architecture relate and interoperate with each other. These products should address mission tasks, technical control, tipping and cueing, maintenance, security measures, medical evacuation, and force protection, among other considerations. General intelligence collection capabilities are captured in detail, including specific collectors or platforms and their specific technical sensors or capabilities, to avoid gaps in collection capabilities.

2-45. Planning and coordinating the intelligence architecture is critical during all types of operations. When developing the intelligence architecture, the intelligence staff considers all personnel, organizations, systems, and procedures necessary for developing intelligence, including those needed for intelligence operations. The architecture must address bandwidth requirements, preparing for operations, collecting the required information and analyzing it, producing the required products, disseminating the resulting intelligence, and assessing both the intelligence produced and the process that produced it. It is critical for the intelligence staff to work with the commander and the staff as early as possible and throughout planning to ensure the intelligence architecture is addressed adequately. The G-2/S-2 also ensures the unit or organization and its subordinates are adequately integrated into their intelligence architecture to enable effective information collection, PED, and analysis to support mission requirements. This ensures the intelligence architecture supports the necessary operational and technical connections between collection assets, control elements, PED nodes, analytical cells, and headquarters to enable an effective and efficient information flow of intelligence to decision makers and the rest of DOD.

2-46. Effective communications connectivity, automation, and interoperability are essential components of the intelligence architecture. These components are especially difficult to establish during large-scale combat operations when tactical forces will not have fixed sites and a robust communications infrastructure is not in place or are severely impacted by an adversary. Establishing the communications network involves many complex technical issues. The intelligence staff collaborates closely with the signal staff to arrange the required communications links. The intelligence staff requires classified and unclassified network connectivity for its equipment. If elements of the intelligence staff will be working outside the range of the unit's communications systems, intelligence architecture planning must include coordination for global or extended-range capabilities.

INTELLIGENCE ACROSS ARMY ECHELONS

2-47. Army intelligence supports decisive action at all echelons. Specifically, the intelligence warfighting function supports operations from the theater army down to the battalion level. The commander and staff need accurate, relevant, and predictive intelligence to understand threat centers of gravity, goals and objectives, and COAs. The commander and staff must also have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations. Precise intelligence is critical to target threat capabilities at the right time and place and to open windows of opportunity to achieve positions of relative advantage.

2-48. The basic intelligence support provided by the G-2/S-2 and intelligence staff at each echelon is the same. What differs is the size, composition, and number of supporting capabilities for the intelligence staff; access to higher-level information and intelligence; number and complexity of the requirements; and time available to answer those requirements. In general, the higher the echelon, the greater the volume, depth, and complexity (for example, detailed intelligence products about threat cyberspace activities) of analysis and intelligence production the intelligence staff can perform. Lower-echelon G-2/S-2s and intelligence staffs often must depend on the higher echelon for certain intelligence products and support. Therefore, the commander and staff must understand the intricacies or specifics of the intelligence warfighting function across each echelon.

2-49. MI unit structures and capabilities differ significantly across theaters and echelons. For example—

- Each theater army MIB-T is structured differently and has different capabilities and capacities.
- The corps expeditionary-military intelligence brigade (E-MIB) is the lowest level with organic CI teams and HUMINT units specifically designated for detainee facility interrogations.
- The theater army, corps, and BCT have organic MI units—the MIB-T, E-MIB, and MI company respectively—but the division and battalion do not have an organic MI unit. ***Note.*** Some of the corps E-MIBs can be task-organized to support the division or even some BCTs.

2-50. These aspects of the intelligence warfighting function matter to the success of operations. Figure 2-2 provides a quick summary of the operations, intelligence staffs, and organic MI units at each level. (For more information on the Army echelons, see FM 3-0; for more on intelligence units and capabilities from theater army to the battalion level, see FM 2-0.)

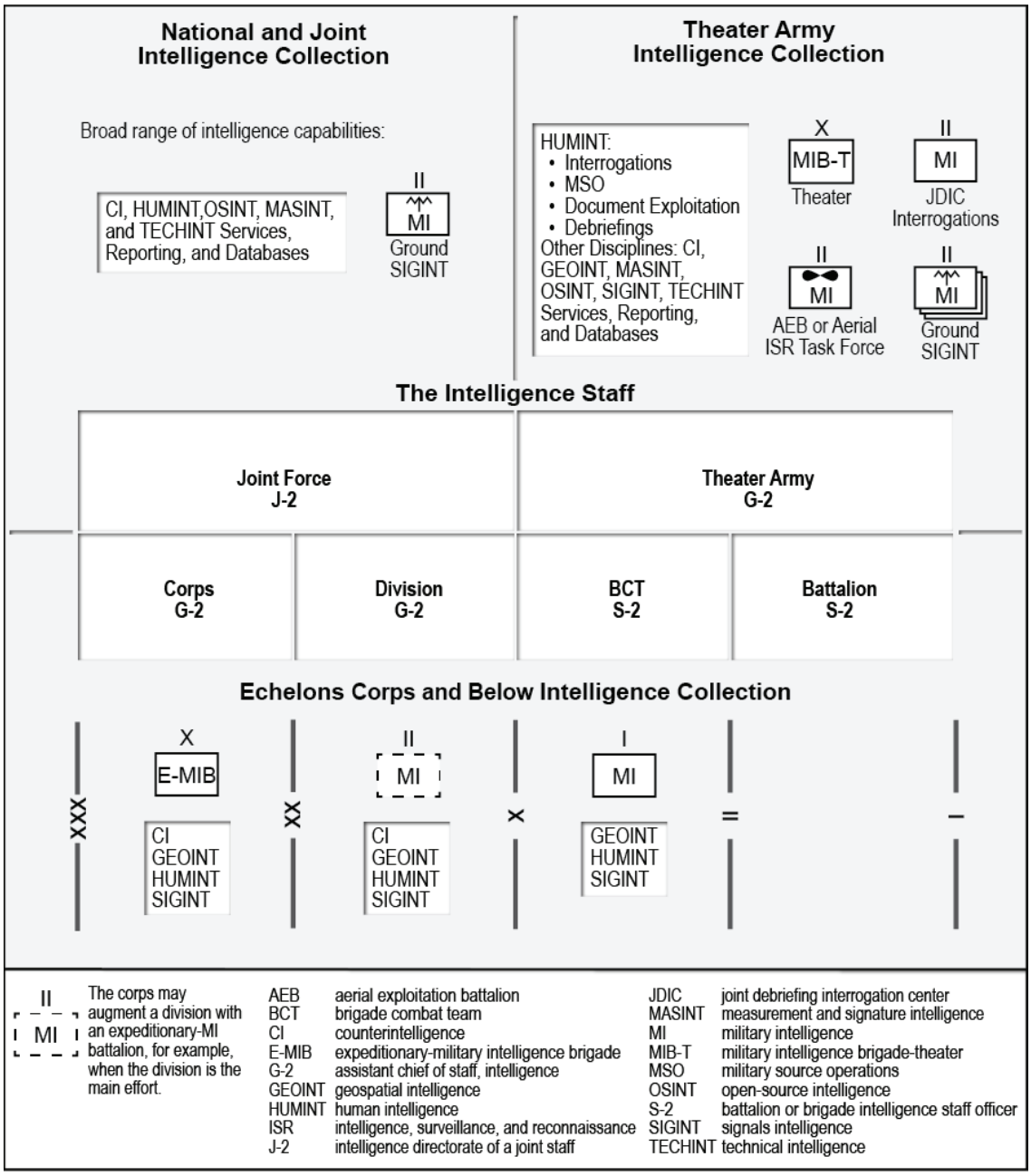


Figure 2-2. Intelligence across the echelons

This page intentionally left blank.

Chapter 3

The Intelligence Process

The Army views the intelligence process as a model that describes how the intelligence warfighting function facilitates situational understanding and supports decision making. This process provides a common framework for Army professionals to guide their thoughts, discussions, plans, and assessments. Effective execution of the intelligence process depends on commander and staff involvement and effective information collection.

THE OPERATIONS PROCESS AND THE INTELLIGENCE PROCESS

3-1. Commanders use the operations process to drive the planning necessary to understand, visualize, and describe their operational environment; make and articulate decisions; and direct, lead, and assess military operations. Commanders successfully drive the operations process by using information and intelligence. The design and structure of the intelligence process support commanders by providing intelligence needed to support command and control and the commander's situational understanding. The commander provides guidance and focus by defining operational priorities and establishing decision points and commander's critical information requirements (CCIRs).

3-2. The joint intelligence process provides the basis for common intelligence terminology and procedures. (See JP 2-0.) It consists of six interrelated categories of intelligence operations:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

3-3. Due to the unique characteristics of Army operations, the Army intelligence process differs from the joint process in a few subtle ways while accounting for each category of the joint intelligence process. The Army intelligence process consists of four steps (plan and direct, collect and process, produce, and disseminate) and two continuing activities (analyze and assess).

3-4. The commander's guidance drives the intelligence process. This process generates information, products, and knowledge about threats, terrain and weather, and civil considerations for the commander and staff. The intelligence process supports all of the activities of the operations process (plan, prepare, execute, and assess). Although the intelligence process includes unique aspects and activities, it is designed similarly to the operations process:

- The *plan and direct* step of the intelligence process closely corresponds with the *plan* activity of the operations process.
- The *collect and process*, *produce*, and *disseminate* steps of the intelligence process together correspond to the *execute* activity of the operations process.
- *Assess* and *analyze* are continuous. These activities form part of the overall *assessment* activity of the operations process.

3-5. Intelligence support to operations requires leveraging national to tactical intelligence. This support is coordinated through the intelligence staff at each echelon by using the intelligence process. Figure 3-1 illustrates the intelligence process.

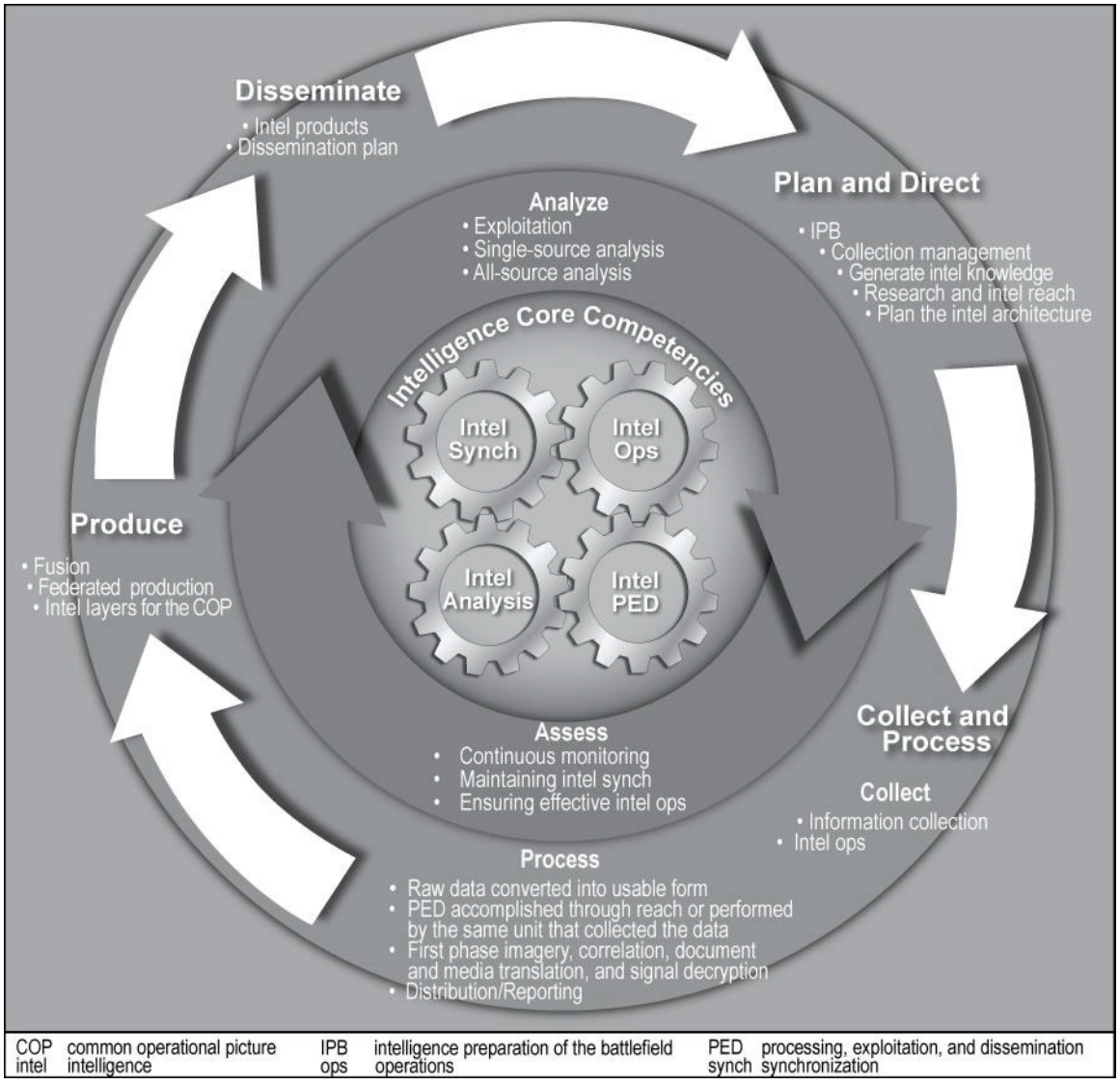


Figure 3-1. The intelligence process

3-6. The G-2/S-2 produces intelligence for the commander as part of a collaborative process. The commander drives the G-2/S-2's intelligence production effort by establishing intelligence and information requirements with clearly defined goals and criteria. Differing unit missions and operational environments dictate numerous and varied production requirements to the G-2/S-2 and staff.

3-7. The G-2/S-2 and staff provide intelligence products that enable the commander to—

- Plan operations and employ maneuver forces effectively.
- Recognize potential COAs.
- Conduct mission preparation.
- Employ effective tactics, techniques, and procedures.
- Take appropriate security measures.
- Focus information collection.
- Conduct effective targeting.

COMMANDER'S GUIDANCE

3-8. Commanders drive the intelligence process by providing commander's guidance and approving priority intelligence requirements (PIRs). While it is not part of the intelligence process, commander's guidance is one of the primary mechanisms used to focus the intelligence process. When approving their PIRs, commanders should limit the number of PIRs so the staff can focus its efforts and allocate sufficient resources. Each commander dictates which intelligence products are required, when they are required, and in what format.

INTELLIGENCE PROCESS STEPS

3-9. The intelligence process leverages all sources of information and expertise, including the intelligence community and nonintelligence entities, to provide situational awareness to the commander and staff. The intelligence warfighting function uses the intelligence process as a management tool to ensure the right information gets to the right users at the right time in a useable format without inundating users. Just as the activities of the operations process overlap and recur as the mission demands, so do the steps of the intelligence process.

3-10. Intelligence activities are enabled by and subject to laws, regulations, and policies to ensure the proper conduct of intelligence operations. While there are too many to list, legal authorities include the USCs, executive orders (EOs), National Security Council and DOD directives, Army regulations, U.S. SIGINT directives, status-of-forces agreements (also called SOFAs), rules of engagement, and other relevant international laws. Commanders will request assistance from their servicing judge advocate to interpret or deconflict these legal authorities.

PLAN AND DIRECT

3-11. Each staff element must conduct analysis before operational planning can begin. Planning consists of two separate but closely related components—conceptual and detailed planning. Conceptual planning involves understanding the operational environment and the problem, determining the operation's end state, and visualizing an operational approach. Detailed planning translates the broad operational approach into a complete and practical plan. (For more information on conceptual and detailed planning, see ADP 5-0.)

3-12. The initial generation of intelligence knowledge about the operational environment occurs far in advance of detailed planning and orders production. This intelligence assists in focusing information collection once a mission is received or in anticipation of a mission. Commanders and staffs often begin planning in the absence of a complete and approved higher headquarters' operation plan or operation order. In these instances, the headquarters begins a new planning effort based on a warning order and other directives, such as a planning order or an alert order from their higher headquarters.

3-13. Intelligence planning is also an inherent part of the Army design methodology and the military decision-making process. Intelligence analysts must prepare detailed planning products for the commander and staff for orders production and the conduct of operations. Through thorough and accurate planning, the staff allows the commander to focus the unit's combat power to achieve mission success.

3-14. The plan and direct step also includes activities that identify key information requirements and develops the means for satisfying those requirements. The intelligence staff collaborates with the operations and signal staffs to plan the intelligence architecture. Collaboration facilitates parallel planning and enhances all aspects of the intelligence process by enriching analysis, incorporating different points of view, and broadening situational understanding. The staffs produce a synchronized and integrated information collection plan focused on answering PIRs and other requirements. PIRs and other requirements drive the information collection effort.

3-15. Commanders must employ organic collection assets as well as plan, coordinate, and articulate requirements to leverage DOD intelligence capabilities. Commanders and staffs cannot expect higher echelons to automatically provide all of the information and intelligence they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from developing specific and detailed requirements. Commanders and staffs must focus requests for intelligence support by clearly articulating requirements.

3-16. The staff focuses information collection plans on answering CCIRs and other requirements and enables the quick retasking of units and assets as the situation changes. Collection management includes continually identifying intelligence gaps. This ensures the developing threat situation and civil considerations—not only the operation order—drive information collection. Specifically, G-2/S-2s—

- Evaluate information collection assets for suitability (availability, capability, vulnerability, and performance history) to execute information collection tasks and make appropriate recommendations on asset tasking to the primary operations staff officers.
- Assess information collection against CCIRs and other requirements to determine the effectiveness of the information collection plan. They maintain awareness to identify gaps in coverage and identify the need to cue or recommend redirecting information collection assets to the primary operations staff officers.
- Update the collection management tools as requirements are satisfied, added, modified, or deleted. They remove satisfied requirements and recommend new requirements as necessary.

Requirements

3-17. For collection managers, there are three types of requirements resulting from collection management. The following three types of validated information requirements are prioritized for purposes of assigning information collection tasks:

- PIRs.
- Intelligence requirements.
- Information requirements.

3-18. Collection managers must understand how collection and PED assets are distributed as they develop and validate requirements. They must also understand that some requirements can be answered through intelligence reach. Figure 3-2 shows the process of developing requirements and integrating them into the information collection process. (See FM 3-55 and ATP 2-01 for more details on requirements and indicators.)

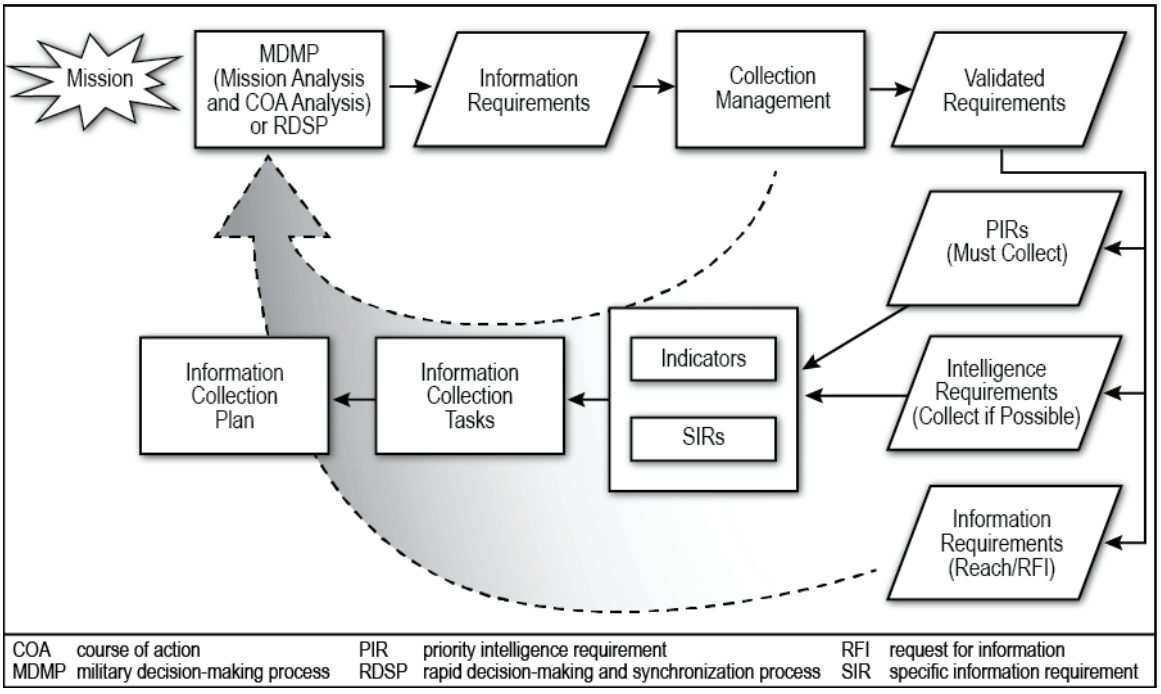


Figure 3-2. Requirements development

Intelligence Reach

3-19. ***Intelligence reach*** **is the activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command**. Information can be acquired through the push and pull of information, databases, homepages, collaborative tools, and broadcast services. Intelligence reach also supports reach PED and distributed analysis. (Reach PED refers to PED capabilities at centralized locations where sensor data is disseminated for intelligence PED support.) Three important aspects of intelligence reach are searches and queries, data mining, and collaboration. (See FM 2-0 for more information on intelligence reach.)

COLLECT AND PROCESS

3-20. The intelligence staff synchronizes collection and processing to provide critical information at key times throughout the phases of an operation. Collection and processing are mutually dependent. Staffs should never allow a seam to emerge between collection and processing, even when elements conducting those functions are separated geographically. The intelligence staff continuously monitors the results not only of information collection but also of processing to continuously assess the effectiveness of the overall information collection effort.

3-21. Information collection and processing activities transition when requirements change, the unit mission changes, the unit proceeds through the phases of an operation, or the unit prepares for future operations. Successful information collection and processing results in timely collection and reporting of relevant and accurate information, which supports the production of intelligence. The intelligence staff coordinates with other unit staffs, subordinate and lateral commands, and higher echelon units to ensure specific units, capabilities, personnel, equipment (especially communications), and procedures are in place.

3-22. *Collection* is, in intelligence usage, the acquisition of information and the provision of this information to processing elements (JP 2-01). Different units and systems collect information and data about threats, terrain and weather, and civil considerations through the four primary means of information collection: reconnaissance, surveillance, security operations, and intelligence operations. Collection includes the maneuver or movement of units and systems to effective locations and the associated force protection measures based on an order or tasking.

3-23. Successfully collecting timely, relevant, and useful information against an adaptive threat is difficult. It is critical for the staff to plan for and use well-developed procedures and flexible planning to track emerging targets, adapt to changing operational requirements, and meet the requirement for combat assessment. A successful collection and processing effort requires the intelligence staff, intelligence analysts, and collectors to form an efficient assessment and feedback loop. Success also requires the staff, analysts, and collectors to watch for threat countermeasures, denial activities, and threat deception. The last step of the feedback loop involves the intelligence staff evaluating reported information for its accuracy and responsiveness to information collection tasks and providing feedback to control elements and collectors.

3-24. Intelligence personnel distribute collected data and information via appropriately classified means and networks for further processing and analysis. During processing, intelligence personnel and systems convert raw data into forms of information commanders, staffs, intelligence analysts, and other consumers can use. Processing may occur immediately within the brain of the data collector, due to the collector's operational knowledge, experience, and situational understanding. However, intelligence personnel and systems often perform processing as a separate but associated function, either at the point of collection or at a separate location.

3-25. Processing includes first-phase imagery exploitation, data conversion and correlation, document and media translation, and signal decryption. For example, processing occurs when the technical parameters (frequency, pulse repetition frequency, and bandwidth) detected by an electronic intelligence (ELINT) collection system are compared and associated with the known parameters of a particular radar system. Rather than providing an analyst with an overwhelming mass of raw ELINT data, the system provides the analyst with the specific type of radar detected.

3-26. Different types of data require different degrees of processing before recipients can understand them. Within SIGINT, processing is increasingly automated and quickly performed by collection systems. Similarly, captured enemy documents may only require translation before an analyst can exploit the information they contain. On the other hand, technical exploitation of an item of enemy equipment may require months of intensive effort to determine its full capabilities. Following established guidelines, analysts must ensure data passes to standardized databases as soon as possible. In some situations, data requires processing to convert it into a format compatible with certain storage means.

3-27. At any point in the intelligence process, intelligence and time-sensitive combat information that affect the current operation are disseminated immediately upon recognition. *Combat information* is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01). The routing of combat information proceeds immediately in two directions—directly to the commander and through routine reporting channels for use by intelligence analysis and production elements.

3-28. Generally, intelligence PED capabilities execute processing for intelligence operations. Intelligence PED involves performing initial analysis to provide context, passing the information on for further analysis or reporting of combat information, and providing feedback on the effectiveness of the collection effort. These closely related PED functions are an inherent part of the collection effort. By performing them faster, more efficiently, and more accurately, intelligence personnel improve the entire intelligence process.

PRODUCE

3-29. Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format. The intelligence staff processes and analyzes information from single or multiple sources, disciplines, and complementary intelligence capabilities, and integrates the information with existing intelligence to create finished intelligence products.

3-30. Intelligence products must be timely, relevant, accurate, predictive, and tailored to facilitate situational understanding and support decision making. The accuracy and detail of intelligence products have a direct effect on operational success. Due to time constraints, analysts sometimes develop intelligence products that are not as detailed as they prefer. However, a timely, accurate answer that meets the commander's requirements is better than a more detailed answer that is late.

3-31. The intelligence staff prioritizes and synchronizes the unit's information processing and intelligence production efforts. The intelligence staff addresses numerous and varied production requirements based on PIRs and other requirements; diverse missions, environments, and situations; and user-format requirements. Through analysis, collaboration, and intelligence reach, the G-2/S-2 and staff use the intelligence capability of higher, lateral, and subordinate echelons to meet processing and production requirements.

3-32. Analysis occurs to ensure the information is relevant, to isolate significant elements of information, and to integrate the information into an intelligence product. Additionally, analysis of information and intelligence is important to ensure the focus, prioritization, and synchronization of the unit's intelligence production effort is in accordance with the PIRs and other requirements.

DISSEMINATE

3-33. Commanders and unified action partners must receive combat information and intelligence products in time and in an appropriate format to facilitate situational understanding and support decision making. Central to the successful dissemination to unified action partners is the early and continuous involvement of the foreign disclosure officer and supporting foreign disclosure representatives. Timely dissemination of intelligence and finished intelligence products is critical to the success of operations. Dissemination is deliberate and ensures consumers receive intelligence to support operations.

3-34. This step does not include the normal reporting and technical channels otherwise conducted by intelligence warfighting function organizations and units during the intelligence process. Each echelon with access to relevant information may perform analysis on that information. Thus, each echelon ensures that resulting intelligence products are properly disseminated. Determining the product format and selecting the means to deliver it are key aspects of dissemination.

3-35. The commander and staff must establish and support a seamless intelligence architecture including an effective dissemination plan. A dissemination plan can be a separate product or integrated into existing products, such as the collection management tools. The plan must include provisions for dissemination to unified action partners.

3-36. Intelligence and communications systems continue to evolve in their sophistication, application of technology, and accessibility to the commander, staff, and unified action partners. Their increasing capabilities also create an unprecedented volume of information available to commanders at all echelons. The commander and staff must have a basic understanding of intelligence dissemination systems and their contribution to the intelligence warfighting function.

Dissemination Methods and Techniques

3-37. There are numerous methods and techniques for disseminating information and intelligence. The appropriate technique in any particular situation depends on many factors, such as capabilities and mission requirements. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, time allocated, and commander's preferences all influence the information format. Answers to PIRs require direct dissemination to the commander, subordinate commanders, and staff. Direct dissemination is conducted person-to-person, by voice communications, or electronic means. Other dissemination methods and techniques include—

- Direct electronic dissemination (a messaging program).
- Instant messaging.
- Web posting (with notification procedures for users).
- Printing or putting the information on a compact disk and sending it.

3-38. Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods, and can be accomplished through various means—for example, push or broadcast.

3-39. G-2/S-2s must plan methods and techniques to disseminate information and intelligence when normal methods and techniques are unavailable. For example, information and intelligence can be disseminated using liaisons or regularly scheduled logistic packages as long as any classified information is properly protected and individuals are issued courier orders.

Dissemination Channels

3-40. Intelligence leaders at all levels assess the dissemination of intelligence and intelligence products. Reports and other intelligence products move along specific channels within the intelligence architecture. The staff assists in streamlining information distribution within these channels by ensuring dissemination of the right information in a timely manner to the right person or element. The three channels through which commanders and their staffs communicate are command channels, staff channels, and technical channels.

Presentation Techniques and Procedures

3-41. Presentation is important and serves as the conclusion of the intelligence process. One of the most difficult challenges is effectively visualizing the operational environment. The intelligence staff must provide the commander with relevant information that supports the commander's visualization, facilitates situational understanding, and enables decision making. The presentation method is based on the commander's guidance but often requires creative solutions to most effectively and efficiently present the intelligence and other information.

3-42. Presentations can be formal or informal. The three general methods the staff uses to present information are written narrative, verbal narrative, and graphic format. Intelligence systems contain standard report formats, maps, and mapping tools that assist the staff in presenting information. Audio and video systems,

such as large format displays and teleconferencing systems, enable the staff to use a combination of these methods in multimedia presentations.

INTELLIGENCE PROCESS CONTINUING ACTIVITIES

3-43. Analyze and assess are two continuing activities that shape the intelligence process. Analyze and assess form part of the overall assessment activity of the operations process and occur continually throughout the intelligence process.

ANALYZE

3-44. Analysis assists commanders, staffs, and intelligence leaders in framing the problem, stating the problem, and solving it. Leaders at all levels conduct analysis to assist in making many types of decisions. Analysis occurs at various stages throughout the intelligence process and is inherent throughout intelligence support to situational understanding and decision making. Collectors and analysts perform initial analysis—often referred to within intelligence as exploitation during the collect and process step—before reporting or otherwise distributing the information to single and all-source analysis elements. For example, a collector may add context to information (analysis) based on previously acquired experience and knowledge, prior to dissemination.

3-45. Analysis in collection management is critical to ensuring information requirements receive the appropriate priority for collection. The intelligence staff analyzes each requirement to determine—

- The requirement's feasibility and whether it supports the commander's guidance.
- The best method of satisfying the requirement (for example, what unit or capability and where to position that capability).
- If the collected information satisfies the requirement.

3-46. Analysis is used in situation development to determine the significance of collected information and its significance relative to predicted threat COAs and PIRs and other requirements. Through predictive analysis, staffs attempt to identify threat activity or trends that present opportunities or risks to the friendly force. They often use indicators developed for each threat COA as the basis for their analysis and conclusions.

ASSESS

3-47. Assess is part of the overall assessment activity of the operations process. For intelligence purposes, assessment is the continuous monitoring and evaluation of the current situation, particularly significant threat activities and changes in the operational environment. Assessing the situation begins upon receipt of the mission and continues throughout the intelligence process. This assessment allows commanders, staffs, and intelligence leaders to ensure intelligence synchronization. Friendly actions, threat actions, civil considerations, and events in the area of interest interact to form a dynamic operational environment. Continuous assessment of the effects of each element on the others, especially the overall effect of threat actions on friendly operations, is essential to situational understanding.

3-48. The intelligence staff continuously produces assessments based on operations, the information collection effort, the threat situation, and the status of relevant aspects of the operational environment. These assessments are critical to—

- Ensure PIRs are answered.
- Ensure intelligence requirements are met.
- Redirect collection assets to support changing requirements.
- Ensure operations run effectively and efficiently.
- Ensure proper use of information and intelligence.
- Identify threat efforts at deception and denial.

3-49. The intelligence staff continuously assesses the effectiveness of the information collection effort. This type of assessment requires sound judgment and a thorough knowledge of friendly military operations; characteristics of the area of interest; and the threat situation, doctrine, patterns, and projected COAs.

Chapter 4
Army Intelligence Capabilities

The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. All-source intelligence and single-source intelligence are the building blocks by which the intelligence warfighting function facilitates situational understanding and supports decision making. The intelligence warfighting function receives information from a variety of capabilities. Some of these capabilities are commonly referred to as single-source capabilities. Single-source capabilities are employed through intelligence operations with the other means of information collection (reconnaissance, surveillance, and security operations). PED capabilities are also necessary to process information and prepare it for subsequent analysis. The intelligence produced based on all of those capabilities is called all-source intelligence.

ALL-SOURCE INTELLIGENCE

4-1. Army forces conduct operations based on all-source intelligence assessments and products developed by the intelligence staff. ***All-source intelligence*** **is the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations.** In joint doctrine, *all-source intelligence* is intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence (JP 2-0).

ALL-SOURCE ANALYSIS

4-2. The fundamentals of all-source intelligence analysis comprise intelligence analysis techniques and the all-source analytical tasks: situation development, generating intelligence knowledge, IPB, and support to targeting and information operations.

4-3. Through the receipt and processing of incoming reports and messages, the intelligence staff determines the significance and reliability of incoming information, integrates incoming information with current intelligence holdings, and through analysis and evaluation determines changes in threat capabilities, vulnerabilities, and probable COAs. The intelligence staff supports the integrating processes (IPB, targeting, risk management, information collection, and knowledge management) by providing all-source analysis of threats, terrain and weather, and civil considerations.

4-4. All-source intelligence is used to develop the intelligence products necessary to aid situational understanding, support the development of plans and orders, and answer information requirements. Although all-source intelligence normally takes longer to produce, it is more reliable and less susceptible to deception than single-source intelligence.

ALL-SOURCE PRODUCTION

4-5. Fusion facilitates all-source production. For Army purposes, ***fusion*** **is consolidating, combining, and correlating information together**. Fusion occurs as an iterative activity to refine information as an integral part of all-source analysis.

4-6. All-source intelligence production is continuous and occurs throughout the intelligence and operations processes. Most of the products from all-source intelligence are initially developed during planning and updated, as needed, throughout preparation and execution based on information gained from continuous assessment.

ALL-SOURCE AND IDENTITY ACTIVITIES

4-7. Joint doctrine describes identity activities as a collection of functions and actions that appropriately recognize and differentiate one person from another to support decision making. They include the collection of identity attributes and physical materials; their processing and exploitation; all-source analytic efforts, production of identity intelligence and DOD law enforcement criminal intelligence products; and dissemination of those products to inform policy and strategy development, operational planning and assessment, and the appropriate action at the point of encounter. These functions and actions are conducted by maneuver, intelligence, and law enforcement components.

4-8. Within intelligence, identity activities are the responsibility of the personnel within the all-source elements of the intelligence staff. Within all-source, identity activities combine the synchronized application of the complementary intelligence capabilities (biometrics, forensics, and document and media exploitation [DOMEX]) with intelligence and identity management processes. This establishes identity, affiliations, and authorizations in order to deny anonymity to the adversary and protect U.S. and partner nation assets, facilities, and forces. These all-source activities result in the discovery of true identities; link identities to events, locations, and networks; and reveal hostile intent. These outputs enable tasks, missions, and actions that span the range of military operations.

SINGLE-SOURCE INTELLIGENCE

4-9. Single-source intelligence includes the joint intelligence disciplines and complementary intelligence capabilities. Intelligence PED capabilities are a critical aspect of single-source intelligence activities that ensure the results of collection inform single- and all-source analysis. MI units can conduct intelligence operations with a single intelligence discipline or complementary intelligence capability or as a multifunction intelligence operation, which combines activities from two or more intelligence disciplines or complementary intelligence capabilities.

4-10. Information moves throughout various echelons along specific transmission paths or channels. Establishing command and support relationships directs the flow of reported information during intelligence operations. Channels assist in streamlining information dissemination by ensuring the right information passes promptly to the right people. Commanders and staffs normally communicate through three channels: command, staff, and technical. (See ADP 6-0 and ATP 6-02.71.)

TECHNICAL CHANNELS

4-11. Technical channels, while not a command or support relationship, often affect intelligence operations. For intelligence operations, technical channels are the transmission paths between intelligence units (including sections) performing a technical function requiring special expertise. Technical channels control the performance of technical functions. They neither constitute nor bypass command authorities; rather, they serve as the mechanism for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of unified land operations.

4-12. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess the unit's collection effort. Technical channels also involve translating information collection tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the information collection effort. Technical channels include but are not limited to—

- Defining, managing, or prescribing specific employment techniques.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized intelligence training.

4-13. Through technical channels, commanders and staffs ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant U.S. law, the law of war, international law, DOD directives and instructions, and orders. For specific intelligence discipline collection, regulatory authority is maintained by national and DOD intelligence agencies and is passed through technical channels. (See FM 2-0 for more on technical channels.)

THE INTELLIGENCE DISCIPLINES

4-14. In joint operations, intelligence collection and activities are commonly organized around the intelligence disciplines, which include—

- CI.
- GEOINT.
- HUMINT.
- Measurement and signature intelligence (MASINT).
- Open-source intelligence (OSINT).
- SIGINT.
- Technical intelligence (TECHINT).

4-15. The intelligence disciplines are integrated to ensure a multidiscipline approach to intelligence analysis, and ultimately, all-source intelligence facilitates situational understanding and supports decision making. Each discipline applies unique aspects of support and guidance through technical channels. (See JP 2-0.)

Counterintelligence

4-16. Army CI counters or neutralizes foreign intelligence collection efforts through collection, CI investigations, operations, analysis, production, and technical services and support. CI includes all actions taken to detect, identify, disrupt, neutralize, or exploit foreign intelligence entity collection efforts directed against DOD and Army personnel, operations, information, material, facilities, technology, and networks. It is the key intelligence community contributor to protecting U.S. interests and equities.

4-17. *Foreign intelligence entity* is any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire United States information, block or impair United States intelligence collection, influence United States policy, or disrupt United States systems and programs. The term includes foreign intelligence and security services and international terrorists (JP 2-01.2). It also includes insurgents, other adversary intelligence threats, and insider threats targeting or suspected of targeting U.S. forces personnel, operations, facilities, networks, information, and technology for intelligence gathering or planning and preparation for an attack or exploitation. (See ATP 2-22.2-1.)

4-18. The role of Army CI is to conduct aggressive, comprehensive, and coordinated investigations, operations, collection, intelligence PED, analysis and production, and technical services. These functions are conducted worldwide to detect, identify, assess, counter, exploit, or neutralize the foreign intelligence entity collection threat. Army CI has four primary mission areas:

- **Counterespionage.** Counterespionage refers to those CI defensive and offensive endeavors to detect, identify, assess, counter, neutralize, or exploit the foreign intelligence entity threat.
- **CI support to force protection.** While force protection is the responsibility of commanders at all levels, Army CI contributes to protection of the force. CI collection, analysis, investigations, and operations are designed to identify foreign intelligence and international terrorist activities that threaten military personnel, civilian employees, and units. Army CI exercises every available authority to support the force protection plans of Army and supported DOD commanders worldwide in accordance with AR 381-20 (classified), DODM 5240.01 for procedures 1-10, DOD 5240.1-R for procedures 11-15, and AR 381-10. In the performance of this function, CI will collect and report information that satisfies standing CI collection requirements.

- **CI support to research, development, and acquisition.** This support is accomplished to prevent the illegal diversion or loss of critical technology essential to the strategic advantage of the United States in future conflicts.
- **CI-cyber.** CI-cyber refers to the use of techniques and measures to identify, exploit, or neutralize adversary cyberspace espionage that uses the internet, information resources, and digital media as the primary tradecraft methodology.

4-19. CI core functions are interrelated, mutually supporting, and can be derived from one another. No single function can defeat the foreign intelligence entity collection threat. The CI core functions are—

- **Operations.** CI operations are broadly executed CI activities that support a program or specific mission. CI operations use one or more of the CI functions. CI operations can be offensive or defensive, and they are derived from, transitioned to, or used simultaneously—depending on the scope, objective, or continued possibility for operational exploitation.
- **Investigations.** Army CI will conduct aggressive and comprehensive investigations worldwide to detect, identify, assess, and counter, neutralize, or exploit the foreign intelligence entity, foreign and insider threat (as defined in DODI 5240.26) to the Army and DOD whenever such threat is within CI jurisdiction.
- **Collection.** CI collection is the systematic acquisition of information concerning the foreign intelligence entity collection threat. CI elements conduct collection activities to support the overall CI mission. CI collection is conducted by using sources, elicitation, official liaison contacts, debriefings, screenings, and OSINT to obtain information that answers standing CI collection requirements or other collection requirements.
- **Technical services and support.** CI technical services are used to assist the CI core functions of investigations, collections, and operations or to provide specialized technical support to a program or activity. The proliferation of sophisticated collection technology, surveillance, and "eaves-dropping" devices available in commercial markets enable any foreign intelligence entity with the ability to increase its capability and effectiveness.
- **Analysis and production.** CI analysis is used to satisfy the supported commander's intelligence requirements and provide focus and guidance to CI operations. CI analysis and production can be accomplished at any level in which Army CI assets are assigned to support any of the four primary mission areas.

4-20. CI organizations and force structure are designed to support Army forces through scalable team, operations management, and technical channel packages. The CI and HUMINT staff officer (also called G-2X/S-2X) structure supports decentralized CI operations. The establishment of the CI and HUMINT staff element (also called 2X) and the CI coordinating authority throughout the Army ensures a trained and experienced cadre of CI professionals to support operations. (See ATP 2-22.2-1 for more information on CI.)

Geospatial Intelligence

4-21. *Geospatial intelligence* is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (JP 2-03). (Section 467, Title 10, USC, establishes GEOINT.)

Note. GEOINT consists of any combination of the following components: imagery, and/or imagery intelligence with geospatial information.

4-22. *Imagery* is a likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likenesses and presentations produced by satellites, aircraft platforms, unmanned aircraft systems, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations) (JP 2-03).

4-23. *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03).

4-24. *Geospatial information* is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products (JP 2-03).

4-25. The GEOINT cell provides geospatial data generation, geospatial data analysis, geospatial data management, quality control, and data dissemination. GEOINT supports the multidirectional flow and integration of geospatially referenced data from all sources to achieve shared situational understanding of the operational environment, near real-time tracking, and collaboration between forces.

4-26. GEOINT activities necessary to support operations include the capability to define GEOINT requirements, discover and obtain GEOINT, put GEOINT in a useable form, and then maintain, use, and share GEOINT. The GEOINT cell interfaces directly with the user to define user requirements. Then the cell interfaces with the National System for Geospatial Intelligence to obtain and provide the best quality GEOINT possible directly to the Soldier. (For more information on GEOINT, see ATP 2-22.7, ATP 3-34.80, and AR 115-11.)

4-27. The GEOINT cell supports operations through five tasks:

- Define GEOINT mission requirements.
- Obtain mission-essential GEOINT.
- Evaluate available GEOINT data.
- Use and disseminate GEOINT.
- Maintain and evaluate GEOINT.

Human Intelligence

4-28. ***Human intelligence*** **is the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities**.

4-29. A HUMINT source is a person from whom foreign information is collected to produce intelligence. HUMINT sources can include friendly, neutral, or hostile personnel. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Categories of HUMINT sources include but are not limited to detainees, enemy prisoners of war, refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and nongovernmental organizations.

4-30. A HUMINT collector is a person who is trained, certified, and authorized to collect information from individuals (HUMINT sources) for the purpose of answering information collection requirements. HUMINT collectors are the only personnel authorized to conduct HUMINT collection operations. They are trained and certified enlisted personnel in military occupational specialty 35M, warrant officers in 351M, commissioned officers in 35F, and their Federal civilian employee counterparts. However, in order to conduct intelligence interrogations, trained HUMINT collectors must successfully complete one of the following courses, which are the only accepted interrogation training sources for military personnel:

- 35M Basic HUMINT Collector course at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona.
- U.S. Marine Corps Basic Marine Air-Ground Task Force CI/HUMINT course at the Navy and Marine Corps Intelligence Center, Dam Neck, Virginia.
- Joint Interrogation Certification course at the HUMINT Training-Joint Center of Excellence, Fort Huachuca, Arizona. (Although this course has been discontinued, successful course graduates are authorized to conduct interrogations.)
- Defense Intelligence Agency I-10 course, Alexandria, Virginia. (Although this course has been discontinued, successful course graduates are authorized to conduct HUMINT interrogations.)

Note. Certification is conducted at the discretion of the combatant commander in accordance with established combatant command policies and directives.

4-31. HUMINT collection operations must be conducted in accordance with all applicable U.S. law and policy, which include EO 12333 as amended; EO 13491; DODM 5240.01 for procedures 1-10; DOD 5240.1-R for procedures 11-15; the law of war; relevant international law; relevant directives, including DODD 2310.01E and DODD 3115.09; DOD instructions; AR 381-100; FM 2-22.3; and military orders, including fragmentary orders. Additional policies and regulations apply to the management of contractors engaging in HUMINT collection. Commanders will request assistance from their servicing judge advocate to interpret or deconflict these legal authorities. (See FM 2-22.3, ATP 2-22.31 [classified], and AR 381-100.)

4-32. HUMINT operations collect information from human sources through overt and clandestine means. HUMINT operations focus on a wide range of sources (such as detainees, refugees, civilians, friendly forces, and recruited personnel) for information that includes but is not limited to an adversary's plans, intentions, and strategies; research and development goals; physical and cultural infrastructure; and medical information.

4-33. Every HUMINT questioning session, regardless of the methodology used or the type of operation, consists of five phases. The five phases of HUMINT collection are—

- Planning and preparation.
- Approach.
- Questioning.
- Termination.
- Reporting.

4-34. The phases are generally sequential; however, reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced, as required, through the questioning and termination phases.

4-35. HUMINT collection methodologies include five categories:

- Screening.
- Interrogation.
- Debriefing.
- Military source operations.
- Liaison.

Measurement and Signature Intelligence

4-36. *Measurement and signature intelligence* is information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event (JP 2-0). (For more information on MASINT, see JP 2-0 and ATP 2-22.8 [classified]).

4-37. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, radio frequency, and seismic sensors, as well as techniques for collecting chemical, biological, radiological, and nuclear (CBRN) signatures and other materiel samples.

4-38. MASINT requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communications, data, and display processing technologies now provide MASINT to support operations.

4-39. MASINT provides intelligence to the commander to facilitate situational understanding and support targeting. Many sensors can defeat many of the camouflage, concealment, and deception techniques currently used to deceive information collection systems. Specifically, MASINT sensors have unique capabilities to detect missile launches; detect and track aircraft, ships, and vehicles; perform noncooperative target identifications and combat assessments; and detect and track fallout from nuclear detonations. Often, these sensors provide the first indicators of hostile activities.

4-40. The MASINT systems most familiar to Soldiers are employed by ground surveillance and CBRN reconnaissance elements. These systems span the entire EMS and their capabilities complement the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—

- Use automatic target recognition and aided target recognition.
- Penetrate man-made and natural camouflage.
- Penetrate man-made and natural cover, including the ability to detect subterranean anomalies or targets.
- Counter stealth technology.
- Detect recently placed mines.
- Detect natural or man-made environmental disturbances in the Earth's surface not discernible through other intelligence means.
- Provide signatures (target identification) to munitions and sensors.
- Enhance passive identification of friend or foe.
- Detect the presence of CBRN agents including before, during, or after employment.
- Detect signature anomalies that may affect target-sensing systems.

4-41. Within DOD, the Defense Intelligence Agency provides policy and guidance for MASINT. Its policy and guidance do not interfere with Service component operations. Each Service has a primary command or staff activity to develop requirements and coordinate the MASINT effort. The Army G-2 staff is the functional manager for Army MASINT resources, policy, and guidance. Army weapons systems programs that require MASINT information to support system design or operations submit requests through INSCOM channels for data collection and processing.

4-42. The scientific and technical intelligence (S&TI) community also performs MASINT collection and processing primarily to support research and development programs and signature development. Every S&TI center has some involvement in MASINT collection or production that reflects that center's overall mission (for example, NGIC has responsibility for armored vehicles and artillery). Service research and development centers, such as the Communications-Electronics Command Research, Development, and Engineering Center, the Army Research Laboratory, and the Night Vision and Electronic Systems Laboratory, are also involved in developing sensor systems for collecting and processing MASINT. Elements within the Army Space and Missile Defense Command also exploit satellite-collected data for the purpose of MASINT exploitation. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based operational collection to support the ASCCs and subordinate units.

Open-Source Intelligence

4-43. OSINT is integral to Army intelligence operations. *Open-source intelligence* is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Public Law 109-163). OSINT is exclusive to intelligence professionals using open-source information to answer specific intelligence requirements. In contrast, open-source *research* is the gathering of data, facts, instructions, or other material that is publicly available and used for general knowledge about a specific person, location, weapons system, or other item of interest. Open-source research is not OSINT. Any staff element may use open-source information to answer many different types of requirements.

4-44. Section 3038, Title 50, USC, and EO 12333 as amended govern OSINT. As such, OSINT is produced by intelligence professionals to support Army commanders in developing an understanding of complex situations, support fused all-source analysis, tip, and support intelligence operations and activities in other intelligence disciplines. (For more information, see ATP 2-22.9.)

4-45. *Open-source information* is information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access (JP 2-0). *Publicly available information* is information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public (DODM 5240.01).

4-46. There are many different forms of open sources, to include social, print, broadcast media; internet; and open public-speaking forums. The collection means (techniques) for obtaining publicly available information from these communications media must be nonintrusive.

> ***Note.*** When there is any doubt about the conduct of OSINT activities, intelligence personnel consult their unit or organization staff judge advocate. All OSINT operations conducted by intelligence professionals must comply with the legal restrictions in EO 12333 as amended, DODM 5240.01 for procedures 1-10, DOD 5240.1-R for procedures 11-15, Army Directive 2016-37, and AR 381-10. Intelligence personnel conducting OSINT activities must comply with all operations security requirements prescribed in AR 530-1 to prevent disclosure of critical and sensitive information.

4-47. The following characteristics from the role of OSINT in Army operations:

- **OSINT provides the foundation.** Open-source information provides updates to foundation information and real-time ongoing information to assist in developing and enhancing intelligence products and the intelligence disciplines. There is much information about the political, military, economic, social, and infrastructure of a region or local area obtainable from open-source information and readily changed to OSINT products. This foundation information and intelligence products can be essential to generating a clear picture for the commander. The variety of foundational websites associated with social structures, education systems, and news services provides a foundational perspective for intelligence knowledge.
- **OSINT addresses requirements.** The availability, depth, and range of open-source information enable intelligence professionals to satisfy many PIRs and information requirements without the use of specialized human or technical means of collection.
- **OSINT enhances collection.** Open-source information supports other requirements and provides information that optimizes the employment and performance of sensitive human and technical collection means. Examples of this type of information include biographies, cultural information, geospatial information, and technical data.
- **OSINT enhances production.** As part of single-source and all-source intelligence production, the use and integration of OSINT ensure commanders have the benefit of all sources of available information.

Signals Intelligence

4-48. *Signals intelligence* is intelligence derived from communications, electronic, and foreign instrumentation signals (JP 2-0). SIGINT provides unique intelligence information, complements intelligence derived from other sources, and is often used for cueing other sensors to potential targets of interest. For example, SIGINT, which identifies activities of interest, may be used to cue GEOINT to confirm that activity. Conversely, changes detected by GEOINT can cue SIGINT collection. The discipline is subdivided into three subcategories: communications intelligence (also called COMINT), ELINT, and foreign instrumentation signals intelligence (also called FISINT).

4-49. *Communications intelligence* is technical information and intelligence derived from foreign communications by other than the intended recipients (JP 2-0). Communications intelligence includes collecting data from target or adversary automated information systems or networks. It also may include imagery when pictures or diagrams are encoded by a computer network or radio frequency method for storage or transmission. The imagery can be static or streaming.

4-50. *Electronic intelligence* is technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (JP 3-13.1). ELINT consists of two subcategories:

- **Operational ELINT**—is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems.

- **Technical ELINT**—is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.

4-51. *Foreign instrumentation signals intelligence* is a subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems (JP 2-01).

4-52. SIGINT provides intelligence on threat intentions, capabilities, compositions, and dispositions. In addition, SIGINT provides information for the delivery of fires. The intelligence staff needs to understand how SIGINT assets are organized not only within the Army but also throughout DOD. The majority of SIGINT assets from the Armed Services, combined with national SIGINT assets, collaborate to support commanders from tactical to strategic levels. Only by understanding the SIGINT structure that transcends traditional Service components can the intelligence staff understand how to use SIGINT effectively.

Technical Intelligence

4-53. *Technical intelligence* is intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0). The role of TECHINT is to ensure Soldiers understand the threat's full technological capabilities. With this understanding, U.S. forces can adopt appropriate countermeasures, operations, and tactics, techniques, and procedures. (For more information, see ATP 2-22.4.)

4-54. A comprehensive TECHINT network is vital to providing precise direction and purpose to DOD research and development and exploitation processes. This ensures quick and efficient neutralization of threat technological advantages and networks in direct support of the commander and S&TI community.

4-55. TECHINT has two primary responsibilities within Army intelligence operations:

- Provide information to supported commands based on the technical analysis of foreign material in accordance with those commands' stated requirements.
- Provide technical assessments of foreign technological threat capabilities, limitations, and vulnerabilities.

4-56. TECHINT includes S&TI, the Army Foreign Materiel Program, and weapons technical intelligence (WTI):

- S&TI organizations track and analyze foreign technological developments. They analyze the performance and operational capabilities of captured materiel that may have military applications.
- The Army Foreign Materiel Program is managed by the Army G-2. It is divided into foreign material acquisition, foreign material exploitation, and disposition of material no longer needed. The Army Foreign Materiel Program responds to U.S. weapons materiel developer TECHINT requirements, tactical requirements, and training requirements.
- As a function of counter-improvised explosive device operations, *weapons technical intelligence* is a subcategory of technical intelligence derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other systems (JP 3-15.1).

4-57. As a specific application of TECHINT, WTI combines technical assessments, forensic science, and other critical enablers with all-source intelligence for use against irregular and nontraditional threats. WTI operationalizes TECHINT and focuses on immediate exploitation of captured weapons to rapidly respond to the tactical commander's PIRs and other requirements. WTI integrates a range of collection, exploitation, and analysis capabilities to support four critical outputs:

- To enable targeting by identifying, selecting, prioritizing, and tracking individuals and matching them with groups, weapons materiel, financiers, suppliers, insurgent leaders, and other related elements.

- To technically and forensically examine events and devices or weapons to identify observables, signatures, and to better understand linkages between technical design and tactical use to guide efforts of the protection warfighting function, as well as tip and cue information collection.
- To provide trend, pattern, and forensic analysis of improvised explosive devices, improvised weapons, and weapons components usage to identify the origin of materiel and components.
- To use information from captured enemy materiel collected during site exploitation activities to further detain and potentially support the prosecution of individuals for criminal activity.

4-58. Every TECHINT mission supports tactical through strategic requirements by the timely collection and processing of materiel and information, follow-on analysis and resulting production of intelligence, and dissemination to a wide range of consumers. Commanders rely on TECHINT to provide them with tactical and technological advantages to successfully synchronize and execute operations. TECHINT combines information to identify specific individuals, groups, and nation-states, matching them to events, places, devices, weapons, equipment, or contraband that associates their involvement in hostile or criminal activity.

COMPLEMENTARY INTELLIGENCE CAPABILITIES

4-59. Complementary intelligence capabilities contribute valuable information for all-source intelligence to facilitate the conduct of operations. The complementary intelligence capabilities are specific to the unit and circumstances at each echelon and can vary across DOD. These capabilities include but are not limited to—

- Biometrics-enabled intelligence (also called BEI).
- Cyber-enabled intelligence.
- DOMEX.
- Forensic-enabled intelligence (also called FEI).

Biometrics-Enabled Intelligence

4-60. Joint doctrine defines *biometrics* as the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). Biometrics as a process of confirming identity is not exclusive to the intelligence warfighting function. This enabler supports multiple activities and tasks of other warfighting functions. Army doctrine defines *biometrics-enabled intelligence* as intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements (ATP 2-22.82).

Biometric Analysis

4-61. It is important for commanders, intelligence staffs, and all-source intelligence analysts across all echelons to assist in consolidating identities, other information, and intelligence to support tactical objectives as well as longer-term operational and strategic objectives. The production of biometrics-enabled intelligence products is critical as persons of interest move from location to location (within an AO) or are elevated in status (and move from one position to another) or as they transit from one AO to another. Products derived from biometric collection can provide context that is critical—related to persons of interest and their intent—to analysts across all echelons.

4-62. DOD biometric-enabled watchlist (BEWL) management is a mission assigned to NGIC. As the DOD BEWL mission manager, NGIC is responsible for: discovering threat identities; reviewing unit nominations (to ensure nominations meet DOD and intelligence community standards); maintaining, managing, and disseminating BEWL subsets; and managing encounters. Development and management of the unit watchlist is an intelligence staff duty. In producing their BEWL, units include collected biometric identities, related contextual information, and intelligence for future reference or further analysis in the analytic system. Unit-level and DOD BEWLs are shared through a dissemination process to provide an unclassified data set on handheld devices to the other U.S. Government systems and the DOD biometric network for positive identification of threat personnel.

Biometric Reports

4-63. Division and above echelons develop many biometrics-enabled intelligence products to support operations, including—

- **Biometric intelligence analysis reports (also called BIARs).** This report is an intelligence product that associates a biometric match with an individual in the biometric database. It is produced by sorting, analyzing, and linking the biometric match with the individual's history, along with all-source intelligence. It may contain the identification, background, assessment, and intelligence value of the subject.
- **BEWLs.** The BEWL is the primary analytic product produced through the all-source analysis production of collected and processed identity records. It is exported from the analytic tool and shared with the biometric network to identify persons of interest within biometric matching systems and handheld devices. Establishing the BEWL to support specified missions is an intelligence staff-level responsibility. The intelligence staff can customize the BEWL based on the unit's assigned mission and rules of engagement. Assistance in establishing a new customized BEWL based on a unit's assigned mission can be coordinated through INSCOM and NGIC. After establishing the customized BEWL, the nomination, removal, or change process is automated through the analytic tool. (For more information, see ATP 2-22.82).

Cyber-Enabled Intelligence

4-64. The cyberspace domain provides another medium for information collection. Cyber-enabled intelligence is a complementary intelligence capability that provides the ability to collect information and produce intelligence products that portray the threat's ability to operate within the cyberspace domain and the effect of the threat on friendly capabilities. Cyber-enabled intelligence is produced through the combination of intelligence analysis and information concerning activities in cyberspace and the EMS. This intelligence supports situational understanding of the cyberspace domain. Cyber-enabled intelligence is based on operations conducted within the cyberspace domain and does not include operations and dominance within the EMS.

Note. The results of cyberspace electromagnetic activities can provide intelligence professionals with a significant amount of information concerning both the physical domain and the information environment.

4-65. Cyber-enabled intelligence facilitates decision making at all levels through the analysis and production of relevant and tailored intelligence on activities in the cyberspace domain that may affect the unit's ability to conduct operations. The intelligence can range from broadly disseminated products focused on general users to very specific and narrowly focused analysis and reports distributed via classified channels. The use of cyber-enabled intelligence facilitates an understanding of the threat's cyberspace electromagnetic capabilities, intentions, potential actions, and vulnerabilities, and their impacts on the environment, friendly operations, and the local populace.

4-66. The mission, authority, and oversight of an activity determine whether the activity is cyber-enabled intelligence or cyberspace-controlled. For example, the use of computers, technology, and networks facilitate all-source intelligence, the intelligence disciplines, and the other complementary intelligence capabilities. However, their use of computers, technology, and networks does not mean these are cyberspace operations. The authority for each discipline or capability governs the guiding methods and regulations for the conduct of each intelligence discipline or complementary intelligence capability.

Document and Media Exploitation

4-67. *Document and media exploitation* is the processing, translation, analysis, and dissemination of collected hardcopy documents and electronic media that are under the U.S. Government's physical control and are not publicly available (ATP 2-91.8). Threat intent, capabilities, and limitations may be derived through the exploitation of captured documents and media.

4-68. DOMEX is an increasingly specialized, full-time mission requiring advanced automation and communications support, analytical support, and expert linguists. When conducted properly, DOMEX—

- Provides the commander an initial assessment of captured information.
- Maximizes the value of intelligence gained from captured enemy documents and media.
- Provides the commander with timely and relevant intelligence to effectively enhance awareness of the threat's capabilities, operational structures, and intent.
- Assists in criminal prosecution or legal proceedings by maintaining chain of custody procedures and preserving the evidentiary value of captured enemy materiel, documents, and media.

4-69. DOMEX products become a force multiplier only when captured materials are rapidly exploited at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and accurate intelligence support. These assets are primarily responsible for screening and tactical exploitation of captured documents and media. This practice not only enables rapid exploitation and evacuation of captured materials but also hastens the feedback commanders receive from the higher echelon analysis. DOMEX assets also deliver items of operational or strategic value to higher level processing facilities for further exploitation. Intelligence staffs need to use the appropriate communications medium to pass vital information to the lowest echelon, especially to the capturing unit.

4-70. It is essential to pass critical information quickly to those who need it, specifically, tactical commanders. Intelligence staffs are responsible for reporting and disseminating DOMEX-derived information in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

4-71. DOMEX personnel are usually not available below the battalion level except in MI organizations. This requires maneuver battalion intelligence staffs to prepare their subordinate units for DOMEX tasks. When intelligence and personnel qualified in the appropriate languages for the AO are available, they can be task-organized as intelligence support teams and placed with companies or platoons. Alternatively, the intelligence section can train company or platoon personnel in specific handling, screening, and inventorying techniques.

4-72. Where tactical assets are insufficient, operational and strategic assets can support a unit's organic assets, either by personnel augmentation or by virtual support from DOMEX support elements, who provide this support worldwide. These organizations use specialized techniques and procedures to extract additional information from captured audio and video materials. Application of specialized processing techniques and procedures may require the classification of the processed information and restrict its dissemination. (For more information on DOMEX, see ATP 2-91.8.)

Forensic-Enabled Intelligence

4-73. Forensics involves the scientific analysis of linking persons, places, things, and events. *Forensic-enabled intelligence* is the intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest (JP 2-0).

4-74. Forensic techniques provide timely and accurate information that facilitates situational understanding and supports decision making. This includes collecting, identifying, and labeling collected items for future exploitation. The collection of latent fingerprints, deoxyribonucleic acid (known as DNA), and other forensic data can aid in more in-depth analysis and better intelligence about the operational environment.

4-75. Forensic-enabled intelligence assists in accurately identifying persons, networks, and complex threats, and attributes them to specific incidents and activities. The effort is often critical in supporting the targeting process. Forensic-enabled intelligence can identify and determine the source of origin of captured materiel, documents, and media. Accurate site documentation of incidents or events, material and structural analysis, and supporting data and information from the various forensic processes and techniques can provide valuable data and enhance operational tactics, techniques, and procedures. For example, timely trace detection or material analysis of unknown substances can assist in protecting the force from contaminants, toxins, and other hazards. Incorporating information obtained via toxicology, pathology and other forensic techniques into forensic-enabled intelligence can assist in identifying health threats within the AO.

INTELLIGENCE PROCESSING, EXPLOITATION, AND DISSEMINATION CAPABILITIES

4-76. Intelligence PED capabilities are the personnel, specialized intelligence and communications systems, software and advanced technologies that execute the PED functions. Intelligence PED operations can be performed either from a deployed expeditionary location or a reach site in theater or the United States. Intelligence PED capabilities can be organic to the intelligence unit, task-organized, or distributed from a centralized location through the network as required.

4-77. The G-2/S-2 advises the staff on intelligence PED requirements and capabilities when planning information collection operations. The commander and staff resource and prioritize supporting intelligence capabilities, including expeditionary or reach PED capabilities, through thorough staff planning (based on recommendations from the G-2/S-2).

4-78. When requesting intelligence PED capabilities, the gaining G-2/S-2 and intelligence unit commander are responsible for coordinating and planning intelligence PED activities. However, the allocating echelon is also responsible for ensuring adequate planning, coordination, and use of PED capabilities. Some intelligence PED capability employment considerations for the gaining G-2/S-2 and intelligence unit commander include—

- **Intelligence architecture.** Employment of intelligence PED capabilities depends on how the collection asset and supporting PED element or unit fits into the intelligence architecture. The employment is also specific to the intelligence discipline or complementary intelligence capability and supported echelon. MI units should capture their functional requirements during planning to ensure they request adequate intelligence PED capabilities.
- **Communications.** All intelligence operations depend on integrating multiple communications systems, networks, and information services. It is important to consider and understand hardware and software requirements and compatibility, interoperability issues, bandwidth priority and capacity, and maintenance requirements.
- **Reporting.** Operating effectively within the intelligence architecture requires system operators to understand PED and reporting procedures, requirements, and timelines for operations and intelligence channels as well as for technical channels.
- **Targeting criteria.** Supporting lethal and nonlethal effects require system operators to be thoroughly knowledgeable with the different targeting criteria, including minimum accuracy and timeliness standards for each specific high-payoff target.
- **Technical channels.** System operators must understand how technical channels operate and how to use technical guidance to enhance collection. Additionally, intelligence PED capabilities assist in refining technical guidance.
- **Training.** Intelligence leaders inform the commander and staff on intelligence PED capabilities and limitations. Facilitating the integration of intelligence PED capabilities requires intelligence leaders to conduct training with the intelligence unit and intelligence PED system operators, analysts, and maintainers.
- **Sustainment.** Intelligence PED capabilities and resources can provide a significant maintenance and logistic challenge to the intelligence unit. Reducing these challenges requires the intelligence unit to conduct thorough planning and coordination.

This page intentionally left blank.

Chapter 5
Fighting for Intelligence

Since Army forces compete with an adaptive enemy; perfect planning and information collection seldom occurs. Intelligence is not perfect, information collection is not easy, and a single collection capability is not persistent and accurate enough to provide all of the answers. During large-scale ground combat operations, Army forces will have to fight for intelligence. To achieve situational understanding against peer threats, friendly forces must strive to identify or open windows of opportunity across domains. Staff integration is difficult but crucial; the staff must collaborate to overcome challenges and mitigate information collection capability and system limitations by developing an integrated information collection plan. Fighting for intelligence also encompasses the basics of establishing an effective intelligence architecture, synchronizing the intelligence warfighting function, and planning and conducting information collection.

THE CHALLENGE

5-1. Producing intelligence and executing information collection differ significantly based on the Army's strategic role. For example, intelligence operations conducted during shaping operations differ drastically from intelligence operations conducted during large-scale ground combat operations.

5-2. Of the Army's four strategic roles (shape, prevent, conduct large-scale ground combat, and consolidate gains), the intelligence warfighting function is most challenged to meet the vast number of large-scale ground combat operation requirements. Large-scale ground combat operations are intense, lethal, and brutal—creating conditions, such as complexity, chaos, fear, violence, fatigue, and uncertainty. Battlefields will include noncombatants crowded in and around dense urban areas. To further complicate operations, enemies will employ conventional and unconventional tactics, terrorism, criminal activities, and information warfare. Activities in the information environment, which includes cyberspace, will often be inseparable from land operations. The fluid and chaotic nature of large-scale ground combat operations will cause the greatest degree of fog, friction, and stress on the intelligence warfighting function.

5-3. When fighting a peer threat during large-scale ground combat operations, units must be prepared to fight for intelligence against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the operational environment. The challenges to information collection include integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and EW operations, and camouflage, concealment, and deception.

5-4. A successful information collection effort is key to achieving and exploiting positions of relative advantage. The intelligence staff can then analyze collected information and provide products, updates, and predictive assessments that support targeting, decision making, and the execution of branches and/or sequels. Staff integration, operational planning, and information collection plans are not foolproof and can become ineffective. Conceptually, fighting for intelligence is not new, but the Army must emphasize this principle due to the complexity of large-scale operations. Conducting information collection requires thorough and creative planning, aggressive execution, and adjustments based on the situation. Key aspects of fighting for intelligence to support operations include the following:

- Commanders drive intelligence.
- Effective staff integration is crucial.
- Effective intelligence requires a comprehensive intelligence architecture.

- A thoroughly developed and flexible information collection plan is critical.
- A successful information collection plan begins with identifying the right requirements.
- Together, commanders, staffs, and subordinate units strive and constantly adjust to develop and execute a layered and aggressive information collection plan.

THE COMMANDER'S ROLE AND STAFF INTEGRATION

5-5. Commanders and staffs need timely, accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and COAs. Precise intelligence is critical to targeting threat capabilities at the right time and place to open windows of opportunity across domains. Commanders and staffs must have detailed knowledge of the threat's strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations.

5-6. Collaboration within and between the entire staff produces integration essential to effective command and control and synchronized operations. While all staff sections have clearly defined functional responsibilities, they cannot work efficiently without complete cooperation and coordination among all sections and cells. Key staff synchronization and integration occur during—

- IPB.
- Army design methodology, the military decision-making process (MDMP), and the rapid decision-making and synchronization process.
- Information collection.
- Targeting.
- Assessments.

5-7. The G-2/S-2 supports the commander's ability to understand the operational environment and visualize operations by leading the IPB process and portraying the enemy throughout the MDMP, developing the information collection plan, updating the intelligence running estimate, and developing intelligence products and reports. The commander's role is to direct the intelligence warfighting function through this relationship with the G-2/S-2. Commanders must stay constantly engaged with their G-2 or S-2; close interaction between them is essential as the intelligence staff supports unit planning and preparation through the integrating processes.

5-8. Commanders and staffs use the integrating processes (IPB, targeting, risk management, information collection, and knowledge management) to synchronize specific functions throughout the operations process. The intelligence staff supports the integrating processes by providing all-source analysis of threats, terrain and weather, and civil considerations. (See ADP 5-0 for more on the integrating processes.)

INTELLIGENCE AND THE INTEGRATING PROCESSES

5-9. There is an ever-growing volume of data and information from numerous sources about the operational environment that can improve the commander's visualization of the battlefield in time and space. Situational understanding enables the commander to better—

- Make decisions.
- Prioritize and allocate resources.
- Assess and take necessary risks.
- Understand the needs of higher and subordinate commanders.

5-10. The commander and staff depend on a skilled intelligence staff to answer PIRs and other requirements through the synchronization of the intelligence warfighting function with command and control. The intelligence staff conducts all-source analysis that facilitates the production of IPB products; supports the information collection effort, the targeting effort, and risk management; and provides all-source intelligence analysis (including conclusions and projections of future conditions or events).

PERFORM INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-11. The G-2/S-2 leads the staff through the IPB process. The IPB process considers all threat capabilities within and across each domain within the unit's AO and area of interest and the relevant aspects of the information environment. The other staff sections assist the intelligence staff in developing the IPB products required for planning. The IPB process consists of the following four steps: define the operational environment, describe environmental effects on operations, evaluate the threat, and determine threat COAs. IPB starts immediately upon receipt of the mission, is refined throughout planning, and is updated to support subsequent operational planning. (See ATP 2-01.3 for more on IPB.) The following aspects of IPB support mission analysis:

- Evaluate military aspects of the terrain, weather effects, and civil considerations.
- Identify threat capabilities.
- Develop threat models.
- Develop high-value target lists.
- Develop an event template and matrix.

PROVIDE INTELLIGENCE SUPPORT TO TARGETING

5-12. The intelligence staff is essential to targeting (both lethal and nonlethal actions). Intelligence supports the planning (target development), preparation, execution, and assessment of direct and indirect fires and EW. The intelligence staff also ensures the information collection plan supports the finalized targeting plan (target detection). Table 5-1 lists the most important subtasks, products, and considerations associated with intelligence support to targeting. (For more on targeting, see ATP 3-60; for more on intelligence support to targeting, see ADRP 1-03 and ATP 2-01.3.)

Table 5-1. Intelligence support to targeting

Receive guidance on—	• Commander's intent • High-payoff targets • Attack criteria • Rules of engagement	• Lead time between decision points and target areas of interest • Combat assessment requirements
Develop—	• Modified combined obstacle overlay • Situation and event templates	• High-value targets • Information collection plan
Explain—	Threat courses of action, as part of war gaming, based on friendly courses of action: • Refine the event template • Assist in developing the high-payoff target list, target selection standard matrix, and attack guidance matrix	
Produce—	Collection management tools	
Collect—	Information for target nomination, validation, and combat assessment	
Disseminate—	• High-payoff target-related information and intelligence to the fires cell or appropriate location immediately • Pertinent information and battle damage assessment in accordance with standard operating procedures or other instructions	

PROVIDE INTELLIGENCE SUPPORT TO RISK MANAGEMENT

5-13. Risk management is the Army's primary process for identifying and controlling risks during operations. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). The chief of protection (or S-3 in units without a protection cell), in coordination with the safety officer, integrates risk management into the MDMP. The intelligence staff participates in the overall risk management process and integrates risk management into collection management when recommending tasks for information collection assets.

5-14. Commanders must focus and use intelligence to explicitly understand the lethality of large-scale ground combat operations and to preserve their combat power and take the appropriate operational risk to achieve the end state. Using intelligence to see and understand within each domain can reduce risk to the friendly force and enhance success in chaotic and high-tempo operations. The distribution of specific

intelligence collection systems, personnel, and equipment enhances the capability of the combined arms team to concentrate combat power and reduce risk. Intelligence provides the commander the ability to detect adversary capabilities and activities, analyze enemy intentions, and track enemy capabilities across all domains to inform decisions and provide realistic assessments of operational and tactical risk. During situation development, analysts determine the significance of collected information and its significance relative to predicted threat COAs. Through predictive analysis, the staff templates threat activity or trends that present opportunities or risks to the friendly force. This support assists the commander and staff in deciding when and where to concentrate sufficient combat power to defeat the threat while mitigating risk.

CONDUCT INFORMATION COLLECTION

5-15. *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). Information collection is an integrated intelligence and operations function. The intelligence staff conducts information collection in collaboration with the operations staff to collect, process, and analyze information the commander requires concerning threats, terrain and weather, and civil considerations that affect operations. The primary Army information collection missions/means are reconnaissance, surveillance, security operations, and intelligence operations.

5-16. A successful information collection effort results in the timely collection and reporting of relevant and accurate information, which either supports the production of intelligence or is disseminated as combat information. The information collection effort includes organic units and capabilities and support from DOD intelligence assets, as well as nonintelligence sources, which provide civil considerations and sociocultural information. (See FM 3-55 and ATP 3-55.4.) The information collection tasks are collection management, direct information collection, execute collection, and conduct intelligence-related missions and operations.

Collection Management

5-17. Collection management is the task of analyzing requirements, evaluating available assets (internal and external), recommending taskings to the operations staff for information collection assets, submitting requests for information for adjacent and higher collection support, and assessing the effectiveness of the information collection plan. The continuous functions of collection management identify the best way to satisfy the requirements of the supported commander and staff. These functions are not necessarily sequential. Collection management inherently requires an understanding of the relative priority of incoming requests for collection and PED. Additionally, collection management includes the staff vetting requirements against current intelligence holdings to ensure resources are not wasted collecting information that is already available. (See ATP 2-01.)

Direct Information Collection

5-18. The operations staff (based on recommendations from the rest of the staff) tasks, directs, and when necessary, retasks information collection assets. By tasking and directing information collection assets, the staff ensures the most effective and balanced use of assets across the subordinate units in order to answer all requirements. The operations staff tasks units and information collection assets by issuing warning orders, fragmentary orders, and operation orders. Additionally, they continuously monitor the information collection effort and retask assets as requirements are refined, updated, and added. (See FM 3-55.)

Execute Collection

5-19. Executing collection focuses on specific requirements. This collection is accomplished through the execution of tactical missions (such as the primary means of information collection: reconnaissance, surveillance, security operations, and intelligence operations) based on CCIRs and other requirements. Collection activities acquire data and information about threats and relevant aspects of the AO. They provide that information to intelligence PED and analysis elements. Typically, collection activities begin soon after receipt of the mission and continue throughout preparation and execution of operations. They do not cease after the operation concludes but continue as required. This allows the commander to focus combat power, execute current operations, and prepare for future operations simultaneously.

APPLY KNOWLEDGE MANAGEMENT

5-20. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). Knowledge flow refers to the ease of movement of knowledge within and among organizations. Knowledge management provides the methods and means to efficiently share knowledge and distribute relevant information where and when it is needed. Knowledge management is supported by four tasks that bring an organization closer to situational and shared understanding. The four knowledge management tasks are creating knowledge, organizing knowledge, applying knowledge, and transferring knowledge. (See ATP 6-01.1 for more information on knowledge management.)

PLANNING CONSIDERATIONS AND INFORMATION REQUIREMENTS

5-21. By supporting the integrating processes, the intelligence warfighting function supports the commander's decisions, situational understanding, MDMP, targeting, and force protection considerations. During all operations, both friendly and enemy forces will endeavor to set conditions to develop a position of relative advantage.

5-22. Through generating intelligence knowledge, IPB, and situation development, the intelligence staff enables commanders and staffs to develop a realistic and sufficiently flexible plan to account for enemy objectives, COAs, and capabilities. The intelligence staff also provides warning intelligence, which indicates the start of hostilities, a major change or escalation to the nature of the conflict, or the introduction of a significant new capability.

PLANNING CONSIDERATIONS FOR THE INTELLIGENCE WARFIGHTING FUNCTION

5-23. The intelligence warfighting function is designed to systematically answer intelligence requirements. Commanders focus the effort by clearly articulating intent, stating requirements, prioritizing targets, and assessing effectiveness as operations progress. However, in order to drive intelligence, commanders and staffs must have realistic expectations about intelligence capabilities and available assets. The following are intelligence warfighting function planning considerations:

- **Intelligence reduces uncertainty; it does not eliminate it.** The commander has to determine the presence and degree of risk involved in conducting a particular operation. The time available to plan and prepare is directly related to the risk. Usually, the more time allotted to planning and preparation, the lower the risk. One of the commander's considerations is determining the appropriate balance between the time allotted for collection weighed against the operational necessity for quickly executing an operation. It takes time to collect information and develop it into detailed and precise intelligence products.
- **The intelligence warfighting function comprises finite resources and capabilities.** Intelligence systems and Soldiers trained in specific skills are limited. Once lost to action or accident, these systems and Soldiers are not easily replaceable; in some cases, it may not be possible to replace them during the course of the current operation. The loss of Soldiers and equipment can result in the inability to detect or analyze threat actions. Additionally, the loss of qualified language-trained Soldiers, especially those trained in low-density languages or skills, could adversely affect intelligence operations.
- **To provide effective intelligence, the intelligence warfighting function must have adequate communications and network-enabled capabilities.** Commanders and staffs must ensure the allocation of communications support and resources to intelligence is appropriate.

INFORMATION REQUIREMENTS

5-24. Information requirements differ significantly based on the defensive or offensive operation, the specific situation, and unique requirements for concurrent supporting operations such as deep operations and missions in the various consolidation areas. During both friendly defensive and offensive operations, there are consolidation area requirements to detect enemy bypassed or stay-behind forces, special purpose forces, irregular forces, terrorists, and efforts to create an insurgency or conduct information warfare. (See FM 3-0 and FM 2-0 for more detailed discussions on the defensive and offensive operations and the specific intelligence support to each form of the defense and offense.)

Defensive Operations

5-25. During friendly defensive operations, enemy forces employ precision fires, other long-range fires, and nonlethal capabilities (such as cyber and EW) to attack friendly command and control and key supporting and sustaining capabilities. Friendly forces aim to prepare defensive positions and set conditions while the enemy attempts to set the timing of, location of, and conditions for battle. The three basic friendly defensive operations are area defense, mobile defense, and retrograde.

5-26. Intelligence supports friendly force efforts to protect the force, disperse and reassemble the force as necessary, and answer requirements on when, where, and in what strength the enemy will attack. This intelligence supports decisions on setting the defense, employing various capabilities, repositioning forces, conducting counterattacks, and when possible, transitioning to offensive operations.

5-27. The intelligence staff leads the rest of the staff in identifying when, where, with what strength, and how the enemy will attack. This allows the commander to identify opportune times to conduct spoiling attacks and reposition forces. The entire staff also identifies threats to support and consolidation areas, such as enemy special purpose forces and irregular activities, which may interfere with control of the defense. The intelligence staff leads the rest of the staff in determining—

- The threat intent, objectives, and associated decision points tied to the decisive and/or key terrain associated with the operation.
- General trafficability and mobility considerations, ground mobility corridors, avenues of approach, intervisibility lines within key areas, specific terrain analysis, and weather effects on the operation.
- The likely composition, focus, routes, and a time window for arrival of enemy reconnaissance formations.
- The likely scheme of maneuver for the attacking enemy force.
- Intent, activities, orientation, and predicted locations for: enemy command and control and communications command posts; enemy artillery formations and air defense systems; enemy aviation units; threat EW capabilities; enemy engineer support, chemical support, and special operations forces; and enemy activities in friendly consolidation areas.
- The likely use and intent for threat cyberspace capabilities and likely enemy use of deception.
- The likely location of and time window to commit enemy reserve forces, likely use of second echelon enemy forces to isolate or encircle friendly forces, and likely times and locations where the friendly commander can launch a spoiling attack.

Offensive Operations

5-28. During friendly offensive operations, enemy forces attempt to disrupt friendly activities by employing precision fires, other long-range fires, and nonlethal capabilities (like cyber and EW). Therefore, friendly forces strive to conduct the necessary movements, prepare logistical support, and set other conditions while the enemy attempts to prevent friendly forces from effectively synchronizing adequate combat power. The four basic friendly offensive operations movement to contact, attack, exploitation, and pursuit.

5-29. Intelligence determines when and where the enemy will concentrate combat power, find gaps and vulnerabilities in enemy defenses, and predict how the enemy will conduct any counterattacks. This intelligence supports decisions on conducting information collection, executing long-range fires, penetrating enemy security areas, overcoming obstacles, avoiding enemy strengths, defeating enemy counterattacks, and when possible, transitioning to exploitation or pursuit.

5-30. The intelligence staff leads the rest of the staff in a careful analysis of the terrain, including ground and air avenues of approach, and other significant factors of the operational environment. Then the staff identifies a broad range of enemy COAs with emphasis on the enemy's most likely and most dangerous COAs in the war-gaming portion of the MDMP. Because of the inherent vulnerability of friendly forces during a movement to contact, the intelligence staff must not underestimate the enemy and complexities of the mission. Predictions of enemy COAs should be thorough; at a minimum, they should account for enemy maneuver units (two echelons below) and all key enemy capabilities and enablers. A thorough IPB and war-gaming effort indicates areas where contact with the enemy is likely, as well as friendly and enemy vulnerabilities by phase of the operation. The intelligence staff leads the rest of the staff in determining—

- The threat intent, objectives, and associated decision points tied to decisive and/or key terrain associated with the operation.
- General trafficability and mobility considerations, ground mobility corridors, avenues of approach, intervisibility lines within key areas, specific terrain analysis, and weather effects on the operation.
- The intent, activities, orientation, and predicted locations for: obstacles, including areas the enemy is likely to use fire support coordination measures; enemy reconnaissance, security forces, and observation posts; enemy aviation units, including forward arming and refueling points; enemy defensive locations with likely close obstacles and engagement areas within the main defensive zone; enemy command and control and communications facilities and systems; enemy artillery, rocket units, and air defense systems; enemy engineer support, chemical support, and special operations forces; threat EW capabilities; enemy reserve forces, including when they would be committed; and enemy activities in friendly consolidation areas.
- The likely use and intent for threat cyberspace capabilities and likely enemy use of deception.
- Indications that the enemy is still conducting movement, possibly turning the operation into a meeting engagement or causing friendly forces to employ a hasty defense.

Other Key Tasks for Shaping Large-Scale Ground Combat Operations

5-31. There are many important aspects of all offensive and defensive operations, including the tactical enabling tasks. In combat, seizing the initiative involves conducting reconnaissance, maintaining security, performing defensive and offensive operations at the earliest possible time, forcing the enemy to culminate offensively, and setting the conditions for decisive operations. Operations in the deep area involve efforts to prevent uncommitted or out-of-contact enemy maneuver forces from being committed coherently or preventing enemy enabling capabilities, such as fires and air defense, from creating effects in the close area. The purpose of operations in the deep area is to set conditions for success in the close area or to set conditions for future operations. Therefore, units must execute successful reconnaissance, security operations, and deep operations before or as part of all offensive and defensive operations:

- **Reconnaissance.** Reconnaissance is typically conducted to gain more information about a terrain feature, geographic area, enemy force, or other operational or mission variable that is important for a commander to formulate, confirm, or modify a COA. Commanders normally assign reconnaissance objectives, which can be information about a specific geographic location, a specific enemy activity to be confirmed or denied, or a specific enemy unit to be located and tracked. Therefore, every reconnaissance is different and there is no general list of information requirements. (See FM 3-0.)
- **Security operations.** The main difference between performing security tasks and reconnaissance tasks is that security tasks orient on the force or facility being protected, while reconnaissance tasks are enemy- and terrain-oriented. The goal of security tasks is protecting a force from surprise and reducing the unknowns in any situation. Commanders may perform security tasks to the front, flanks, or rear of a friendly force. Security tasks are shaping operations. As a shaping operation, economy of force is often a consideration when planning. Intelligence support for security operations simply follows the intelligence considerations for the offensive or defensive operation the main unit is conducting. Security operations encompass five tasks: screen, guard, cover, area security, and local security. (See FM 3-0.)

- **Deep operations.** Deep operations are combined arms operations directed against uncommitted enemy forces or capabilities before they can engage friendly forces in the close fight. Deep operations also contribute to setting the conditions to transition to the next phase of an operation (for example, from a defensive to an offensive operation). Deep operations are not simply attacking an enemy force in depth. Instead, they are the sum of all activities that influence when, where, and in what condition enemy forces will be committed. Deep operations are normally planned and controlled at theater army, corps, and division levels, and typically include information collection, target acquisition, ground and air maneuver, fires, cyberspace electromagnetic activities, and information operations either singly or in combination. Intelligence support to deep operations is an inherent part of intelligence support to targeting. The intelligence staff leads the rest of the staff in identifying when, where, in what strength, and how the enemy will begin movement, launch attacks, or defend. (See ATP 3-94.2.)

THE INFORMATION COLLECTION PLAN AND THE INTELLIGENCE ARCHITECTURE

5-32. After completing the MDMP (to include developing requirements), the commander and staff complete an information collection plan. Developing the information collection plan involves overlaying the information requirements on the current situation, operational plan, and the existing intelligence architecture.

DEVELOPING THE INFORMATION COLLECTION PLAN

5-33. Commanders and staffs use the principles of information collection, IPB and other key staff products, and knowledge of information collection capabilities and limitations to develop the information collection plan. As commanders and staffs develop the plan, they may encounter information collection gaps due to factors that include but are not limited to inadequate collection range, unfavorable terrain, or lack of technical capabilities.

5-34. PIRs and the most important intelligence requirements and targeting requirements form the basis of an integrated information collection plan. Through analysis, the staff determines the best way to satisfy each requirement. Based on the MDMP, including a thorough war game, the commander and staff develop a detailed and realistic information collection plan to answer as many requirements as possible.

5-35. Staff integration and synchronization ensures the enemy situation and the operational environment (not just a predetermined operational plan) drive the information collection effort. Generally, intelligence units and collectors are allocated based on priorities and the unit's main effort. Additionally, a unit may have to depend on the higher echelon to provide intelligence support during a particular operational phase because the unit is constantly moving or has a high operating tempo and cannot produce its own intelligence.

5-36. The information collection plan must be simple enough to execute, should avoid being predictable to enemy forces, and should include adequate operations security measures to protect friendly operations. Effective information collection planning depends on collaboration across the echelons in order to vertically and horizontally layer the information collection effort. A layered and continuous information collection effort provides better opportunities for detecting enemy formations, fires capabilities, and critical specialized capabilities that pose the greatest threat to friendly forces. (See FM 3-55 and ATP 2-01 for more on developing an information collection plan.)

ESTABLISHING THE INTELLIGENCE ARCHITECTURE

5-37. When the commander and staff start planning, many aspects of and limitations to information collection have already been set based on the specifics of the intelligence architecture and command and control network. While units can change a few components of the intelligence architecture within a short timeframe, most components are already set or require a fairly long lead time to change. Therefore, setting the intelligence architecture is an important aspect of the shape and deter roles.

5-38. The intelligence architecture is developed well before deployment based on future planning and assumptions on the employment of intelligence capabilities. Periodically, units will revise the intelligence architecture based on new planning factors and assumptions, as well as the addition of new capabilities. Before deployment, units task-organize information collection capabilities based on the intelligence architecture and other factors such as the command post structure and other key nodes. Following initial deployment, the intelligence architecture will already be largely established and each unit will develop an information collection plan within the context of the architecture.

5-39. The command and staff must understand the relationship of national to tactical intelligence; theater-specific procedures, networks, and systems; the strengths and vulnerabilities of organic and supporting intelligence units, personnel, and systems; and the overarching operation plan in order to establish the intelligence architecture.

DEVELOPING THE SITUATION AND CONTINUOUS INFORMATION COLLECTION

5-40. The fight for intelligence becomes more difficult as units receive long-range fires and make contact with enemy forces. Information collection and intelligence analysis are integral to developing the situation. Additionally, the corps and division intelligence staffs may attend or watch theater-level collection management boards, giving them insight into national and joint priorities and coverage. This insight, coordination, and preparation create opportunities for tactical units to leverage national and joint capabilities. The theater army, corps, and division G-2s convene an operations and intelligence working group, or some form of synchronization meeting, with key staff and subordinate units. These intelligence synchronization meetings (normally conducted via video teleconferencing) create a common understanding of the enemy, ensure information collection plans address changes in the situation, and coordinate continuous information collection across echelons and units.

5-41. The intelligence staff conducts synchronizing activities to assist the unit in developing the situation and adjusting information collection. Information collection requires airspace, terrain, and space deconfliction and coordination as well as adequate PED capabilities to ensure assets are able to operate efficiently and effectively. The staff considers whether the unit has the intelligence collection and PED capabilities, capacity, and architecture required to support planned and projected operations. There are many requirements for the G-2/S-2 and the intelligence staff to participate in unit battle rhythm activities to synchronize intelligence support and the information collection effort. The intelligence staff provides updates on the situation and briefs changes to the information collection plan during various commander updates, boards, cell meetings, and other meetings. This creates a common understanding of the enemy, ensures information collection plans address changes in the situation, and coordinates continuous information collection across echelons and units.

5-42. Information collection is continuous through the execution of operations and transition to consolidate gains. The all-source analytical effort is key to informing the commander and staff, who in turn support the continued fight for intelligence. Therefore, G-2/S-2s, all-source analysts, and collection managers must collaborate closely. Intelligence analysis assists in discovering collection gaps, generating more information requirements, and driving all operations. Additionally, analysis assists in determining the effectiveness of the information collection effort. That assessment leads to adjustments in the information collection plan, making it more efficient and effective. Thorough planning allows continuous collection planning through all phases, branches, and sequels of an operation.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The glossary lists terms for which ADP 2-0 is the proponent with an asterisk (*) before the term. For other terms, it lists the proponent publication in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AO	area of operations
AR	Army regulation
ASCC	Army Service component command
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
AUTL	Army Universal Task List
BCT	brigade combat team
BEWL	biometric-enabled watchlist
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
CI	counterintelligence
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COA	course of action
DOD	Department of Defense
DODD	Department of Defensive directive
DODI	Department of Defense instruction
DODM	Department of Defensive manual
DOMEX	document and media exploitation
DSCA	defense support of civil authorities
ELINT	electronic intelligence
E-MIB	expeditionary-military intelligence brigade
EMS	electromagnetic spectrum
EO	executive order
EW	electronic warfare
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal

GCC	geographic combatant command
GEOINT	geospatial intelligence
HUMINT	human intelligence
INSCOM	United States Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
JP	joint publication
MASINT	measurement and signature intelligence
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MI	military intelligence
MIB-T	military intelligence brigade-theater
NGIC	National Ground Intelligence Center
OSINT	open-source intelligence
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
S&TI	scientific and technical intelligence
SIGINT	signals intelligence
TECHINT	technical intelligence
U.S.	United States
USC	United States Code
WTI	weapons technical intelligence

SECTION II – TERMS

***all-source intelligence**

(Army) The integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations.

(joint) Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. (JP 2-0)

adversary

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

biometrics

(joint) The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (JP 2-0)

biometrics-enabled intelligence

(Army) Intelligence resulting from the combination of biometric information with other intelligence, threat information, or information relating to other aspects of the operational environment in order to answer intelligence requirements. (ATP 2-22.82)

collection

In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 2-01)

combat information

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 2-01)

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)

communications intelligence

Technical information and intelligence derived from foreign communications by other than the intended recipients. (JP 2-0)

decisive action

The continuous, simultaneous execution of offensive, defensive, and stability operations or defense support of civil authorities tasks. (ADP 3-0)

defense support of civil authorities

Support provided by United States Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. (DODD 3025.18)

defensive operation

An operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations. (ADP 3-0)

document and media exploitation

The processing, translation, analysis, and dissemination of collected hardcopy documents and electronic media that are under the U.S. Government’s physical control and are not publicly available. (ATP 2-91.8)

electronic intelligence

Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 3-13.1)

foreign instrumentation signals intelligence

A subcategory of signals intelligence consisting of technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-United States aerospace, surface, and subsurface systems. (JP 2-01)

foreign intelligence entity

Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire United States information, block or impair United States intelligence collection, influence United States policy, or disrupt United States systems and programs. The term includes foreign intelligence and security services and international terrorists. (JP 2-01.2)

forensic-enabled intelligence

The intelligence resulting from the integration of scientifically examined materials and other information to establish full characterization, attribution, and the linkage of events, locations, items, signatures, nefarious intent, and persons of interest. (JP 2-0)

***fusion**

(Army) Consolidating, combining, and correlating information together.

geospatial information

Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03).

geospatial intelligence

The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (JP 2-03)

hazard

A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. (JP 3-33)

***human intelligence**

(Army) The collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities.

imagery

A likeness or presentation of any natural or man-made feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likenesses and presentations produced by satellites, aircraft platforms, unmanned aircraft systems, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations). (JP 2-03)

imagery intelligence

The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 2-03)

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)

intelligence

(1) 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. (2) The activities that result in the product. (3) The organizations engaged in such activities. (JP 2-0)

***intelligence analysis**

The process by which collected information is evaluated and integrated with existing information to facilitate intelligence production.

intelligence community

All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 2 0)

***intelligence operations**

(Army) The tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements.

***intelligence reach**

The activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command.

intelligence, surveillance, and reconnaissance

An integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. (JP 2-01)

***intelligence synchronization**

The art of integrating information collection; intelligence processing, exploitation, and dissemination; and intelligence analysis with operations to effectively and efficiently fight for intelligence in support of decision making.

intelligence warfighting function

The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment. (ADP 3-0)

joint operations

Military actions conducted by joint forces and those Service forces employed in specific command relationships with each other, which of themselves, do not establish joint forces. (JP 3-0)

knowledge management

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

large-scale combat operations

(Army) 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)

large-scale ground combat operations

Sustained combat operations involving multiple corps and divisions. (ADP 3-0)

measurement and signature intelligence

Information produced by quantitative and qualitative analysis of physical attributes of targets and events to characterize, locate, and identify targets and events, and derived from specialized, technically derived measurements of physical phenomenon intrinsic to an object or event. (JP 2-0)

offensive operation

An operation to defeat and destroy enemy forces and gain control of terrain, resources, and population centers. (ADP 3-0)

open-source information

(joint) Information that any member of the public could lawfully obtain by request or observation as well as other unclassified information that has limited public distribution or access. (JP 2-0)

open-source intelligence

(DOD) Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (Public Law 109-163)

operation

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

operational environment

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

***processing, exploitation, and dissemination**

The execution of the related functions that converts and refines collected data into usable information, distributes the information for further analysis, and, when appropriate, provides combat information to commanders and staffs.

publicly available information

(DOD) Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. Publicly available information includes information generally available to persons in a military community even though the military community is not open to the civilian general public. (DODM 5240.01)

regionally aligned forces

Those forces that provide a combatant commander at up to joint task force capable headquarters with scalable, tailorable capabilities to enable the combatant commander to shape the environment. They are those Army units assigned to combatant commands, those Army units allocated to a combatant command, and those Army capabilities distributed and prepared by the Army for combatant command regional missions. (FM 3-22)

risk management

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

signals intelligence

Intelligence derived from communications, electronic, and foreign instrumentation signals. (JP 2-0)

stability operation

An operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-0)

technical intelligence

Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. (JP 2-0)

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, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

unified action partners

Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations. (ADP 3-0)

unified land operations

The simultaneous execution of offense, defense, stability, and defense support of civil authorities across multiple domains to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action. (ADP 3-0)

weapons technical intelligence

A subcategory of technical intelligence derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other systems. (JP 3-15.1)

References

All URLs accessed on 14 June 2019.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. June 2019.

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

ADP 3-0. *Operations*. 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.

FM 2-0. *Intelligence Operations*. 6 July 2018.

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

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

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

Most DOD publications are available at the DOD Issuances website: http://www.dtic.mil/whs/directives.

CJCSI 3121.01B. *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces* (S). 18 June 2008.

DOD Law of War Manual. December 2016. Available online: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.* 7 December 1982.

DODD 2310.01E. *DOD Detainee Program*. 19 August 2014.

DODD 3025.18. *Defense Support of Civil Authorities (DSCA)*. 29 December 2010.

DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 11 October 2012.

DODI 5240.26. *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat.* 4 May 2012.

DODM 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities.* 8 August 2016.

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

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

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

JP 2-01.2. *(U) Counterintelligence and Human Intelligence in Joint Operations* (S). 6 April 2016. This publication is classified. Access information is available online: https://jdeis.js.mil/jdeis/index.jsp?pindex=2.

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

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

JP 3-13.1. *Electronic Warfare*. 8 February 2012.
JP 3-15.1. *Counter-Improvised Explosive Device Operations*. 17 July 2018.
JP 3-28. *Defense Support of Civil Authorities*. 29 October 2018.
JP 3-33. *Joint Task Force Headquarters*. 31 January 2018.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.
ADP 3-07. *Stability*. 31 August 2012.
ADP 3-28. *Defense Support of Civil Authorities*. 11 February 2019.
ADP 3-90. *Offense and Defense*. 13 August 2018.
ADRP 1-03. *The Army Universal Task List*. 2 October 2015.
AR 115-11. *Geospatial Information and Services*. 28 August 2014.
AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.
AR 381-20. *(U) Army Counterintelligence Program* (S). 25 May 2010.
AR 381-100. *(U) Army Human Intelligence Collection Programs* (S). 22 February 2016.
AR 530-1. *Operations Security.* 26 September 2014.
ATP 2-01. *Plan Requirements and Assess Collection.* 19 August 2014.
ATP 2-01.3. *Intelligence Preparation of the Battlefield.* 1 March 2019.
ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)*. 11 December 2015.
ATP 2-22.4. *Technical Intelligence*. 4 November 2013.
ATP 2-22.7. *Geospatial Intelligence*. 26 March 2015.
ATP 2-22.8. *(U) Measurement and Signature Intelligence* (S//NF). 30 May 2014.
ATP 2-22.9. *Open-Source Intelligence (U)*. 30 June 2017.
ATP 2-22.31. *(U) Human Intelligence Military Source Operations Techniques* (S//NF). 17 April 2015.
ATP 2-22.82. *Biometrics-Enabled Intelligence (U)*. 2 November 2015.
ATP 2-33.4. *Intelligence Analysis*. 18 August 2014.
ATP 2-91.7. *Intelligence Support to Defense Support of Civil Authorities*. 29 June 2015.
ATP 2-91.8. *Techniques for Document and Media Exploitation*. 5 May 2015.
ATP 3-34.80. *Geospatial Engineering*. 22 February 2017.
ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations*. 5 April 2016.
ATP 3-60. *Targeting*. 7 May 2015.
ATP 3-94.2. *Deep Operations*. 1 September 2016.
ATP 6-01.1. *Techniques for Effective Knowledge Management*. 6 March 2015.
ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 30 April 2019.
FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.
FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.
FM 3-22. *Army Support to Security Cooperation.* 22 January 2013.
FM 3-55. *Information Collection*. 3 May 2013.
FM 27-10. *The Law of Land and Warfare*. 18 July 1956.
U.S. Army Directive 2016-37. *U.S. Army Open-Source Intelligence Activities*. 22 November 2016.

OTHER PUBLICATIONS

EO 12333. *United States Intelligence Activities*. 4 December 1981. Amended by EO 13284 (2003) and 13470 (2008). Available online: http://www.archives.gov/federal-register/executive-orders/disposition.html.

EO 13491. *Ensuring Lawful Interrogations.* 22 January 2009. Available online: http://www.archives.gov/federal-register/executive-orders/disposition.html.

Public Law 109-163. *National Defense Authorization Act for Fiscal Year 2006*. 6 January 2006. Available online: https://www.gpo.gov/fdsys/pkg/PLAW-109publ163/content-detail.html.

Title 10, USC. *Armed Forces*. Available online: http://uscode.house.gov/.

Title 32, USC. *National Guard*. Available online: http://uscode.house.gov/.

Title 50, USC. *War and National Defense*. Available online: http://uscode.house.gov/.

SOURCES USED

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. 2014. Dillon Beach, CA: Foundation for Critical Thinking. 2017. Available online: http://www.criticalthinking.org/.

Elder, Linda and Richard Paul. *The Thinker's Guide to Analytic Thinking*. 2017. Dillon Beach, CA: Foundation for Critical Thinking. 2017. Available online: http://www.criticalthinking.org/.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

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

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

This page intentionally left blank.

Index

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

This page intentionally left blank.

ADP 2-0
31 July 2019

By Order of the Secretary of the Army:

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

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1919006

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 111117, requirements for ADP 2-0.

PIN: 103029-000