FM 2-0
INTELLIGENCE

OCTOBER 2023

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes FM 2-0, dated 06 July 2018.

HEADQUARTERS, DEPARTMENT OF THE ARMY

*FM 2-0

Field Manual
No. 2-0

Headquarters
Department of the Army
Washington, D.C., 01 October 2023

INTELLIGENCE

Contents

*This publication supersedes FM 2-0, dated 06 July 2018.

Figures

Tables

This page intentionally left blank.

Preface

FM 2-0 represents an important step toward changing the Army culture and improving Army readiness by addressing the fundamentals and tactics associated with intelligence across the Army strategic contexts, within multidomain operations—the Army's operational concept. This publication describes the role of the commander and staff in intelligence, intelligence staff activities, and how military intelligence (MI) units conduct intelligence operations as part of information collection. FM 2-0 also contains descriptions of the intelligence warfighting function tasks as well as doctrine on force projection and language support. This manual is designed to be used with ADP 2-0, ADP 3-0, ADP 3-07, ADP 3-19, ADP 3-28, ADP 3-90, and ADP 5-0, and with FM 3-0, FM 3-55, FM 3-60, FM 3-90, FM 3-94, FM 3-96, FM 5-0, FM 6-0, and FM 6-27.

The principal audience for FM 2-0 is every Soldier, Army Civilian, and Army contractor participating in or with the intelligence warfighting function. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning joint intelligence. FM 2-0 also serves as a reference for personnel who are developing doctrine, leader development, material and force structure, and institutional and unit training for intelligence operations.

Commanders, staffs, and subordinates, with assistance from their servicing judge advocates, ensure their decisions and actions comply with applicable United States (U.S.) laws and policy, to include but not limited to Executive Order 12333 as amended; relevant DOD instructions; DOD 5240.1-R; DODD 2310.01E; DODD 3115.09; DODD 5240.01, DODM 5240.01; AR 381-10; FM 2-22.3; FM 6-27, the Uniform Code of Military Justice; military orders, including fragmentary orders; and international treaties. Commanders at all levels ensure their Soldiers operate in accordance with the law of armed conflict and the rules of engagement. (See FM 6-27.)

FM 2-0's chapter 2 contains blue boxes throughout that follow operational concepts discussed in FM 3 0. The blue boxes address different aspects of intelligence related to those FM 3-0 operational concepts.

FM 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 FM 2-0 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which FM 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.

FM 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 FM 2-0 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Training and Doctrine, U.S. Army Intelligence Center of Excellence. Send written 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-DOT-D (FM 2-0), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017; by e-mail to usarmy.huachuca.icoe.mbx.doctrine@army.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

Intelligence drives multidomain operations and multidomain operations enable intelligence. FM 2-0 focuses on the role of intelligence during operations by Army forces and is closely nested with the operational doctrine in FM 3-0, *Operations*. Together, FM 3-0 and FM 2-0 take an important step forward to drive change in Army culture and prepare for multidomain operations across the Army strategic contexts.

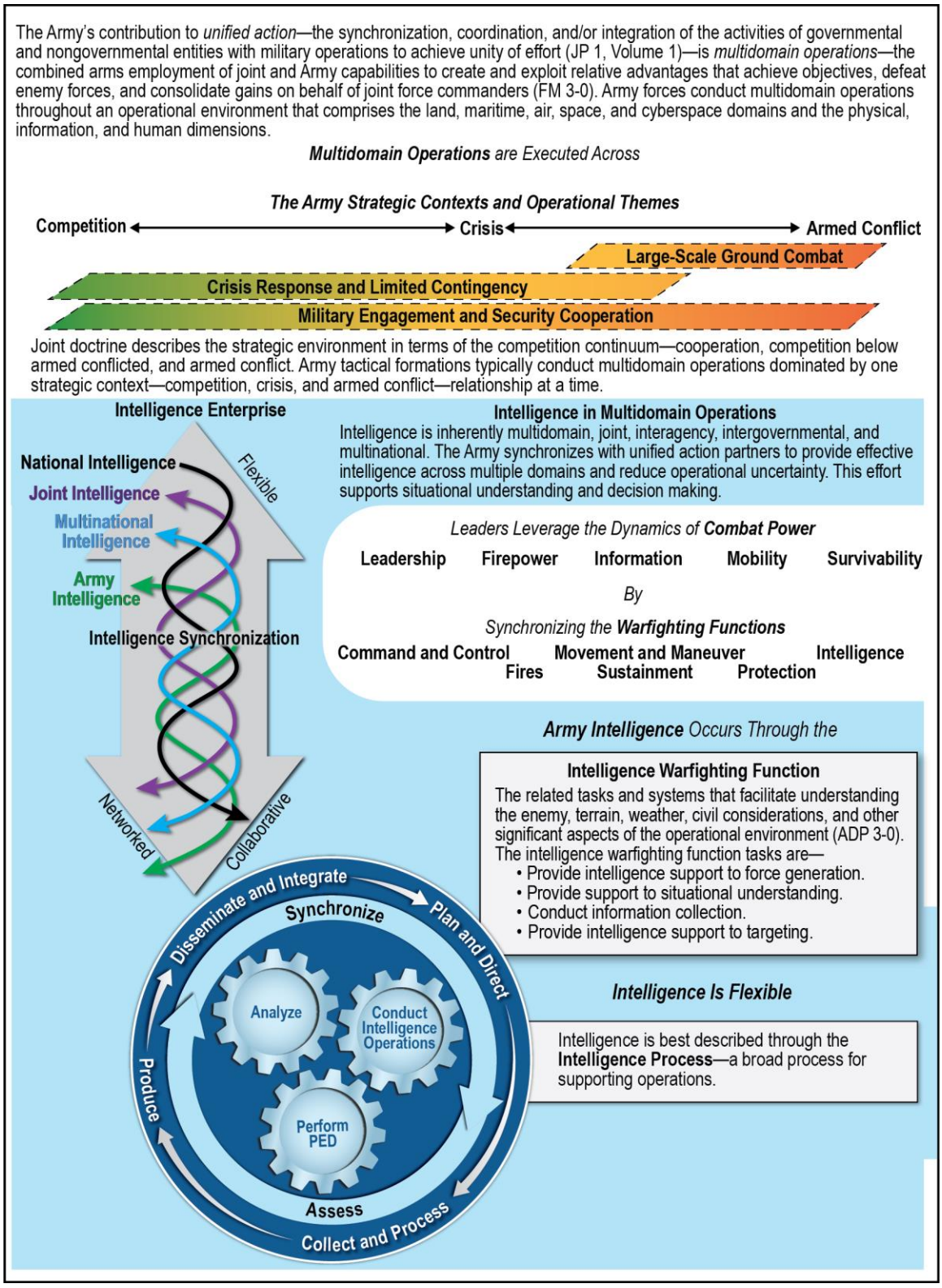
Since the formation of the Continental Army, intelligence support to operations has been critical in winning the Nation's conflicts. Effective intelligence then, now, and in the future is characterized as—

- Timely, relevant, accurate, and predictive, facilitating planning, decision making, and targeting.
- Collaborative with other warfighting functions to complement and reinforce effects against threat formations.

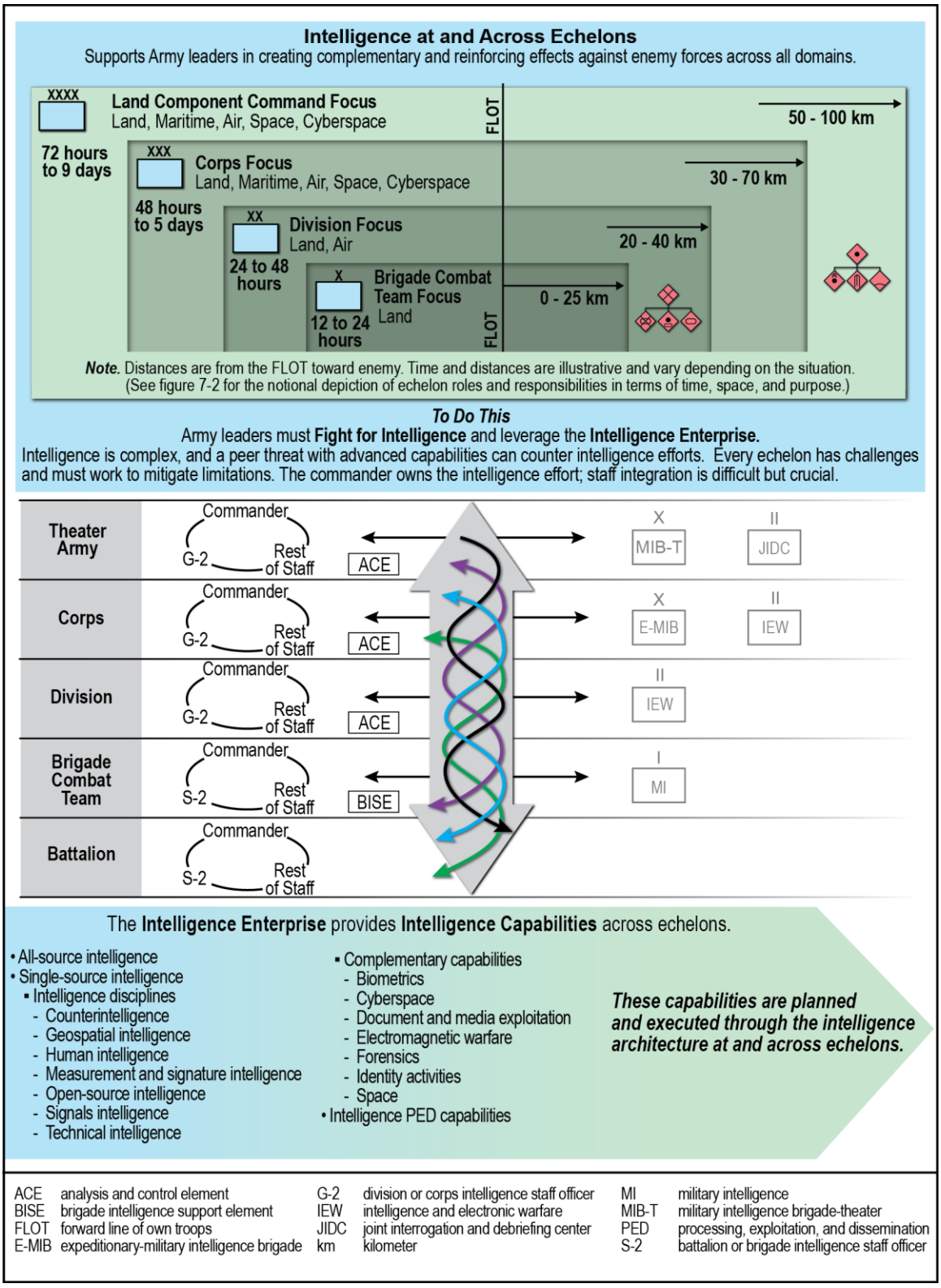
Providing effective intelligence is becoming more challenging as operations become more complicated. The current operational environment (OE) is dynamic, complex, and shaped by the intersection of worldwide trends driven by globalization, technology, climate change, shifting geopolitics, and varying stages of conflict and resolution. The Nation's adversaries are increasing capability, challenging Army forces to achieve enduring advantages, conduct integrated deterrence, and sustain active campaigning.

Intelligence must encompass the entirety of the OE. Intelligence professionals must understand the land, maritime, air, space, and cyberspace domains as well as the human, information, and physical dimensions to be effective. This level of understanding is critical to enable a commander's visualization and decision making during competition below armed conflict, crisis, and armed conflict. Commanders drive the intelligence warfighting function. The commander and staff continuously employ and sustain intelligence capabilities, shifting intelligence support, as necessary, to accomplish the mission. The G-2/S-2 is the intelligence warfighting function expert and advises the commander on intelligence capacities, capabilities, authorities, staff integration, certification, training, and employment. Effective intelligence requires collaboration among the commander, the G-2/S-2, the staff, and supporting intelligence unit commanders.

The FM 2-0 logic chart is the introductory figure on pages xii and xiii. It illustrates the overarching *why*, *who*, *what*, *where*, and *how* associated with intelligence support to multidomain operations. Each successive chapter in this publication builds on the fundamentals established in the previous chapters. FM 2-0 discusses many aspects of intelligence support, including the commander and staff's role within intelligence, intelligence staff activities, and how MI units conduct intelligence operations as part of information collection. The last two chapters discuss a key theme: *fighting for intelligence*—the struggle to provide intelligence on uncooperative and determined threats.



Introductory figure. FM 2-0 logic chart



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

FM 2-0 encompasses eight chapters and five appendixes:

- **Chapter 1** presents the fundamentals of Army intelligence doctrinal constructs.
- **Chapter 2** discusses intelligence within multidomain operations.
- **Chapter 3** discusses integrating and synchronizing intelligence into operations.
- **Chapter 4** discusses intelligence within the Army strategic contexts.
- **Chapter 5** discusses how the intelligence staff provides intelligence support to the commander and staff.
- **Chapter 6** addresses intelligence operations, emphasizing the command and control (C2) of MI units. Intelligence operations conducted by MI units follow the Army's framework for exercising C2—the operations process. Chapter 6 also provides intelligence operations guidelines and task-organizing considerations.
- **Chapter 7** discusses intelligence staffs and units from theater army to the battalion level, as well as their intelligence collection and all-source intelligence capabilities.
- **Chapter 8** discusses fighting for intelligence during large-scale combat operations. It emphasizes the intelligence challenge, different information requirements, overcoming some information collection challenges, and the continuous nature of information collection.
- **Appendix A** addresses considerations that G-2/S-2s must address when operating as part of a joint task force or multinational force.
- **Appendix B** lists the intelligence warfighting function tasks, including their descriptions.
- **Appendix C** describes force projection operations and the required intelligence support.
- **Appendix D** discusses intelligence provisions and authorities.
- **Appendix E** discusses the considerations for language support.

The introductory table outlines changes to terminology reflected in FM 2-0.

Introductory table. New and modified terms

Term	*Remarks*
combat information	New Army-specific definition
deep sensing	New term and definition
document and media exploitation	FM 2-0 becomes the proponent.
intelligence handover line	New term and definition
intelligence preparation of the operational environment	Replaces intelligence preparation of the battlefield; FM 2-0 becomes the proponent.

This publication—

- Uses the term *threat*, which includes all enemies and adversaries that are a part of the OE.
- Uses the word *theater* to indicate theater of operations.
- Refers to elements of intelligence staff organizations by the name used for them in tables of organization and equipment. When task-organized in a command post, these organizations fulfill the role of staff elements as described in FM 6-0.
- Introduces acronyms 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 8 and appendixes A, C, D, and E). Appendix B can be treated as a stand-alone appendix; therefore, acronyms and definitions have been reintroduced.
- Uses U.S. as a modifier (for example, *U.S. forces*) and United States as a noun (for example, the *United States, a country in North America*).

PART ONE

Fundamentals

Effectively providing doctrine on the nature of intelligence and operations requires a sequential approach. Therefore, FM 2-0 is structured in three parts, starting with fundamental concepts and progressing to detailed discussions. Part I focuses on intelligence and operational fundamentals, concluding with how those fundamentals apply across the Army strategic contexts. Part I comprises three chapters that include the following points of emphasis:

- The intelligence warfighting function and intelligence warfighting function tasks (IWFTs).
- The intelligence process.
- Intelligence capabilities.
- Fighting for intelligence.
- Understanding an operational environment (OE).
- Multidomain operations, the Army's operational concept.
- Large-scale combat operations.
- Operational tenets and imperatives.
- Operational approach and operational framework.
- Integrating intelligence into operations.
- Fighting for intelligence within and across the Army strategic contexts.

Chapter 1

Intelligence

SECTION I – OVERVIEW

1-1. *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. 3. The organizations conducting such activities (JP 2-0). It is useful to view intelligence in three ways, depending on the context of the discussion—intelligence as a function, as a product, and as a process—which together enable the conduct of operations by supporting the commander and command and control (C2) (which is accomplished by supporting the rest of the staff).

1-2. The purpose of intelligence (the function) is to provide commanders and staffs with timely, accurate, relevant, predictive, and tailored intelligence (the product) about the threat and other aspects of the OE. Intelligence (the process) supports the conduct of operations. Intelligence is most meaningful when it directly supports operations or force generation. Intelligence professionals consistently strive to provide intelligence that facilitates the commander and staff's situational understanding.

Note. *Force generation* is an element of military force. It is the operation that creates and provides units for projection and employment to enable military effects and influence across multiple operational environments. It is the primary responsibility of the Services to develop, provide, and preserve forces in support of the national military strategy to enable the combatant commanders to execute their missions (AR 525-29).

1-3. The goal is to provide effective and flexible intelligence support across the competition continuum. However, this is a significant challenge. While not all encompassing, three key aspects of providing effective intelligence support are—

- Knowing and adapting the intelligence fundamentals (as largely captured within Army doctrine) in the context of the current situation and a unit's mission or operation.
- Employing and adapting all available intelligence capabilities in the context of the current situation and a unit's mission or operation.
- Building and maintaining tactically and technically proficient intelligence professionals who are effective in both the profession of arms and the intelligence profession.

JP 2-0, *Intelligence*

The joint intelligence doctrine in JP 2-0 is a great resource and the authoritative doctrinal source for the Joint Staff, combatant commands, joint task forces (JTFs), and subordinate components of those commands. Among other topics, JP 2-0 thoroughly discusses—

- The Joint Staff.
- Combatant command intelligence.
- Subordinate joint force intelligence.
- National intelligence.
- Interagency, international, and multinational intelligence sharing.
- The joint intelligence process.

Army forces not serving in one of those roles should use Army doctrine. The content in JP 2-0 was considered in developing this publication, and the content in FM 2-0 is consistent with JP 2-0 while also accounting for the differences between Army and joint structures, capabilities, authorities, and operations.

1-4. In order to know and adapt intelligence fundamentals, intelligence professionals must read more than FM 2-0; they must be doctrinally proficient in a number of intelligence and combined arms publications, depending on their position, unit or organization, and the unit or organization's mission or operation. To assist in building proficiency in intelligence fundamentals, this chapter provides discussions on the following:

- Intelligence, in general, including intelligence as a product and the intelligence enterprise.
- Army intelligence fundamentals, including the intelligence warfighting function and the intelligence process.
- Employing Army intelligence capabilities.
- Fighting for intelligence.

INTELLIGENCE AS A PRODUCT

1-5. Through the effective integration of intelligence into operations, intelligence and operational products are mutually supportive and enhance the commander and staff's *situational understanding*—the product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables (ADP 6-0). Intelligence professionals ultimately disseminate intelligence products, either analog (face-to-face, radio, hardcopy) or digital, in many ways. These intelligence products are tailored to the commander and staff's needs and preferences, and they are dictated by the OE, current situation, standard operating procedures (SOPs), and battle rhythm.

1-6. It is an art to describe intelligence production and dissemination and to ensure it is effectively integrated into unit planning, execution, and targeting, but it is not an exact science to execute intelligence as a function and create it as a product. There is always a degree of uncertainty when producing intelligence. Understanding intelligence as a product, with its strengths and limitations, includes understanding the categories of intelligence products, characteristics of effective intelligence, and the goal to adhere to the highest analytic standards.

CATEGORIES OF INTELLIGENCE PRODUCTS

1-7. Intelligence products are generally placed in one of eight production categories, based primarily on the purpose of the produced intelligence. The categories of intelligence products can and do overlap; analysts can find and use some of the same intelligence and information in each of the categories (see JP 2-0):

- *Warning intelligence* are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests (JP 2-0). For Army purposes, warning intelligence includes the threat's use of new or first-use of significant existing capabilities, tactics, or courses of action (COAs).
- *Current intelligence* provides updated support for ongoing operations. It involves the integration of time-sensitive, all-source intelligence analysis and information reporting on the area of operations (AO). The term *current* is relative to the commander or decision maker's time sensitivity and the context of the type of operation that is supported.
- *General military intelligence* is intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations (JP 2-0).
- *Target intelligence* is intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance (JP 3-60).
- *Scientific and technical intelligence* is foundational all-source intelligence that covers: a. foreign developments in basic and applied research and applied engineering techniques and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture (JP 2-0).
- *Counterintelligence* is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities (JP 2-0).
- *Estimative intelligence* is intelligence that identifies and describes adversary capabilities and intentions, and forecasts the full range of alternative future situations in relative order of probability that may have implications for the development of national and military strategy, and planning and executing military operations (JP 2-0).
- *Identity intelligence* is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0).

Note. Intelligence related to the information dimension across all domains can be categorized by threat entity: intent, capability, access, resources, and expertise.

CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

1-8. The effectiveness of intelligence is measured against different criteria. A concise list of intelligence characteristics includes timely, relevant, accurate, and predictive. Within Army combined arms doctrine, intelligence is a subset of relevant information. In FM 6-0, the relevance of information is determined based on the following characteristics: accurate, timely, useable, complete, precise, and secure. Effective intelligence must meet all those characteristics.

Note. Intelligence professionals must protect classified intelligence.

1-9. The following is an intelligence-centric list of characteristics:

- **Timely.** Intelligence, provided early, supports operations and prevents surprise from threat actions. It must flow continuously to the commander and staff before, during, and after an operation. Intelligence organizations, databases, and products must be available to develop estimates, make decisions, and plan operations.
- **Relevant and tailored:**
  - Intelligence supports the commander's requirements.
  - Intelligence is shared and disseminated in the format requested by the commander, subordinate commanders, and staffs. The intelligence staff presents clear, concise intelligence that meets the commander's preferences, facilitates situational understanding, and is usable for decision making or other actions.
- **Accurate and reliable:**
  - To the extent possible, intelligence should accurately identify threat intentions, capabilities, limitations, composition, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Assumptions should be clearly identified, and there should be a distinction between facts and assumptions. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and unbiased intelligence and present planners with alternate assumptions and different potential indicators.
  - Intelligence evaluates and determines the extent that the collected information and the information being used in intelligence briefings and products are trustworthy, uncorrupted, and undistorted. Concerns about the underlying sources' reliability that affect confidence in the intelligence, or any other issues must be stated up front.
- **Predictive.** Intelligence informs the commander about what the threat can do (threat capabilities, emphasizing the most dangerous threat COA) and is most likely to do (the most likely threat COA). The intelligence staff should anticipate the commander's intelligence needs, as well as threat options that may potentially impact the commander's decision making and a unit's freedom of action. Predictive intelligence also considers possible threat activities and the employment of threat and friendly capabilities over longer time windows before those enemy forces can affect friendly forces or the AO. Determining time windows can assist decision makers on when to leverage forces and capabilities to mitigate predicted changes in an OE.
- **Meet unit or organization and intelligence enterprise standards:**
  - **Usable.** Intelligence must be in the correct data-file specifications for databasing and display. Usability facilitates further analysis, intelligence production, product integration across the staff, and use within operations.
  - **Complete.** Intelligence briefings and products convey the necessary components to be as complete as possible.
  - **Precise (as possible).** Intelligence briefings and products provide the required level of detail and complexity to answer the requirements.

ANALYTIC STANDARDS

1-10. As much as possible, intelligence products and their conclusions should adhere to analytic standards, such as those established by the Director of National Intelligence in Intelligence Community Directive (ICD) 203. These standards assist in determining the relevance and value of information before updating existing intelligence assessments. These standards also govern the production and evaluation of national intelligence analysis to meet the highest standards of integrity and rigorous analytic thinking. Although created for national-level intelligence agencies, these analytic standards are also valid at the operational and tactical levels. (See ATP 2-33.4.)

THE INTELLIGENCE ENTERPRISE

1-11. Multinational, interagency, intergovernmental (to the national level), and joint intelligence are crucial for Army intelligence activities. Multinational, national, and joint intelligence form the basis and set the context for more specific Army operational and tactical intelligence. This national to tactical aspect of intelligence explains why the intelligence enterprise is essential to Army intelligence activities as it provides certain intelligence, capabilities, broadcast downlinks, and other services.

Note. The Army Intelligence and Security Enterprise (AISE) provides capabilities to the larger intelligence enterprise. The enterprise provides important support to joint, multinational, and combined organizations and intelligence activities, including DOD combat support agencies. (See paragraph 7-15 for the specific AISE offices.)

1-12. Higher-level intelligence is key to the depth and quality of the intelligence disseminated to Army commanders and staffs, and it provides some forms of intelligence the Army cannot produce that are important to Army multidomain operations. From an overarching perspective, every aspect of intelligence is synchronized, federated, databased, networked, and, to some extent, collaborative across all unified action partners. This synchronization (including the provision of certain authorities) occurs through national to tactical support across the intelligence enterprise. Intelligence enterprise assets include all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. The most important element is the people who make it work.

1-13. Not all echelons have the same degree of activity with other members of the intelligence enterprise, but Army intelligence professionals should understand what they receive or can access from the intelligence enterprise. The main value provided to the commander is the ability to leverage—

- Specialized collection capabilities.
- Large volumes of OE-related information.
- Unique intelligence databases.
- Specialized analysis and analytic products.

1-14. Analysts leverage higher-level intelligence organizations and databases to create a more comprehensive and detailed assessment of threats and other relevant aspects of the OE (such as deep analysis across each domain and the human and information dimensions) to facilitate situational understanding and visualization of the AO. The effectiveness of Army intelligence hinges directly on the ability to collaborate and share within the intelligence enterprise.

1-15. Collaboration is the central principle of conducting analysis across intelligence organizations. Army tactical units provide accurate and detailed intelligence about the threat and other relevant aspects of the OE (especially those related to Army activities) through the intelligence enterprise, while other intelligence organizations provide expertise and access not readily available to the Army at the tactical level.

1-16. United States (U.S.) Government members of the larger intelligence enterprise are referred to as the intelligence community (IC), which is under the purview of the Office of the Director of National Intelligence. *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). While multinational and nongovernmental partners are important, the U.S. IC forms a major portion of the intelligence enterprise. Numerous DOD and non-DOD agencies and organizations in the IC support Army operations by providing specific intelligence products and services. Additionally, national-level intelligence organizations provide governance and standards over certain intelligence methods and activities. Cooperation can benefit every echelon. (See appendix A for JTF and unified action partner considerations.)

1-17. The U.S. IC is increasingly important as new technologies facilitate collaborative analysis and production. Effective intelligence operations must include familiarity with the IC and methods to obtain information, intelligence, and services from the various members, as necessary. Table 1-1 on page 1-6 lists DOD and non-DOD IC members.

Table 1-1. U.S. intelligence community members

Department of Defense members	*Non-Department of Defense members*
• Defense Intelligence Agency • National Security Agency • National Geospatial-Intelligence Agency • National Reconnaissance Office • U.S. Army • U.S. Navy • U.S. Air Force • U.S. Marine Corps • U.S. Space Force	• Office of Director of National Intelligence • Central Intelligence Agency • Department of State • Department of Energy • Federal Bureau of Investigation • Department of the Treasury • U.S. Coast Guard • Department of Homeland Security • Drug Enforcement Administration
U.S. United States	

SECTION II – ARMY INTELLIGENCE

1-18. Army intelligence is unique from joint and other Service intelligence activities for several reasons, some of which include the nature of Army operations and missions (primarily within the land domain), the fog and friction associated with Army operations sometimes creating time and environmental challenges, and the unique branch and staff structure. Army intelligence is—

- Focused on the commander and staff.
- Requirements-driven to support visualization, situational understanding, and targeting.
- Synchronized and integrated within operations through the staff integrating processes and working groups.
- Detailed, as much as required and possible, and usually time sensitive.
- Employed as a warfighting function, which encompasses more than the military intelligence (MI) branch. The varied nature of the intelligence warfighting function occurs through four tasks: provide intelligence support to force generation, provide support to situational understanding, conduct information collection, and provide intelligence support to targeting.
- Executed through the intelligence process, based on the joint intelligence process but modified to account for Army operations.

1-19. Commanders and staffs require accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and COAs across the domains and dimensions. Precise intelligence is also critical in detecting, identifying, and targeting threat capabilities at the right time and place and in opening windows of opportunity across domains and dimensions, particularly during large-scale combat operations. Commanders and staffs must have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, training, employing and controlling forces, and tactics to plan for and contribute to unified action across the Army strategic contexts (competition below armed conflict, crisis, and armed conflict). This requires using the intelligence warfighting function to provide the detailed knowledge necessary to support the operations process.

1-20. Intelligence drives the conduct of operations and operations enable intelligence, making intelligence and operations inseparable. Therefore, G-2/S-2s must ensure the intelligence warfighting function operates effectively and efficiently. G-2/S-2s are not simply managers; they are commanders' primary advisors on employing collection assets and driving information collection. The result is the dissemination of intelligence or combat information to the right person at the right time and place. ***Combat information*** **is a report that is gathered by or provided to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence before being used to support decision making**. The commander and unit may create a level of risk by relying too much on combat information instead of intelligence.

THE INTELLIGENCE WARFIGHTING FUNCTION

1-21. Intelligence is one of the warfighting functions that enables the Army to generate combat power during the conduct of operations. 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). Other significant aspects of the OE include—

- The operational variables not already covered by the mission variables of enemy, terrain, weather, and civil considerations.
- Other aspects that are not a threat or hazard to operations, for example, using the intelligence warfighting function to provide intelligence on unique requirements to support medical and humanitarian operations in an African country.

1-22. The intelligence warfighting function must be effective and flexible to legally meet the commander and staff's requirements. One way to ensure this effectiveness and flexibility is focusing on those other aspects of the OE, as needed, when they are important to the commander, type of operation, and specific mission.

1-23. The intelligence warfighting function supports operations through a broad range of supporting doctrinal tasks, referred to as IWFTs. Army units and organizations perform IWFTs through the intelligence process by employing intelligence capabilities to support the commander and staff. Therefore, commanders and staffs must know the intelligence staff considerations discussed in chapter 3.

1-24. IWFTs are interrelated, require the commander and staff's participation, and are often conducted simultaneously. Appendix B provides a detailed description of the IWFTs, which comprise the following:

- **Provide intelligence support to force generation (IWFT 2.1)** supports the Army's efforts to maintain a ready, effective, and flexible intelligence warfighting function globally. This task spans intelligence across the entire competition continuum and includes the following subtasks:
  - Provide intelligence readiness (IWFT 2.1.1).
  - Plan, establish, and revise an intelligence architecture (IWFT 2.1.2).
  - Provide intelligence overwatch (IWFT 2.1.3).
  - Tailor the intelligence force (IWFT 2.1.4).
- **Provide support to situational understanding (IWFT 2.2)** entails providing information and intelligence to commanders to clearly understand the threat and other relevant aspects of the OE. This task includes the following subtasks:
  - Conduct pre-mission analysis of the OE (IWFT 2.2.1). ***Note.*** This task was formerly known as generate intelligence knowledge.
  - Leverage data, information, and intelligence (IWFT 2.2.2).
  - Perform intelligence preparation of the operational environment (IPOE) (IWFT 2.2.3).
  - Perform situation development (IWFT 2.2.4).
  - Provide intelligence support to unique missions (IWFT 2.2.5).
  - Conduct police intelligence operations (IWFT 2.2.6). ***Note.*** Police intelligence is not an MI task; police intelligence operations encompass different aspects of law enforcement and criminal investigations. United States Codes (USCs), executive orders, DOD directives, and Army regulations contain specific guidance on the conduct of police intelligence operations.
- **Conduct information collection (IWFT 2.3)** synchronizes and integrates the planning and employment of sensors and assets as well as processing, exploitation, and dissemination (PED) capabilities in direct support (DS) of current and future operations. This task includes the following subtasks:
  - Collection management (IWFT 2.3.1).
  - Direct information collection (IWFT 2.3.2).
  - Execute collection (IWFT 2.3.3).
  - Conduct intelligence-related missions and operations (IWFT 2.3.4).

- **Provide intelligence support to targeting (IWFT 2.4)** entails providing the commander with information and intelligence to support targeting to achieve lethal and nonlethal effects. This task includes the following subtasks:
  - Provide intelligence support to target development (IWFT 2.4.1).
  - Provide intelligence support to target detection (IWFT 2.4.2).
  - Provide intelligence support to combat assessment (IWFT 2.4.3).

THE INTELLIGENCE PROCESS

1-25. Army units and organizations use the intelligence process to integrate intelligence support and provide the commander and staff the intelligence needed to facilitate situational understanding, effectively make decisions, and exercise C2. As a key fundamental, it is important to understand both the joint and Army intelligence processes.

1-26. The joint intelligence process provides the basis for common terminology. (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, and evaluation and feedback). The Army intelligence process consists of four steps (plan and direct, collect and process, produce, and disseminate and integrate) and five continuing activities (synchronize, conduct intelligence operations, perform PED, analyze, and assess). (See figure 1-1.)

1-27. The Army intelligence process steps are very similar to the joint process interrelated categories; however, due to the unique characteristics of Army operations, the Army intelligence process steps differ in some important but subtle ways. Some of the differences stem from J-2 authorities and responsibilities not tasked to G-2/S-2s. Despite these differences, the steps and continuing activities of the Army process account for each of the categories of the joint process.

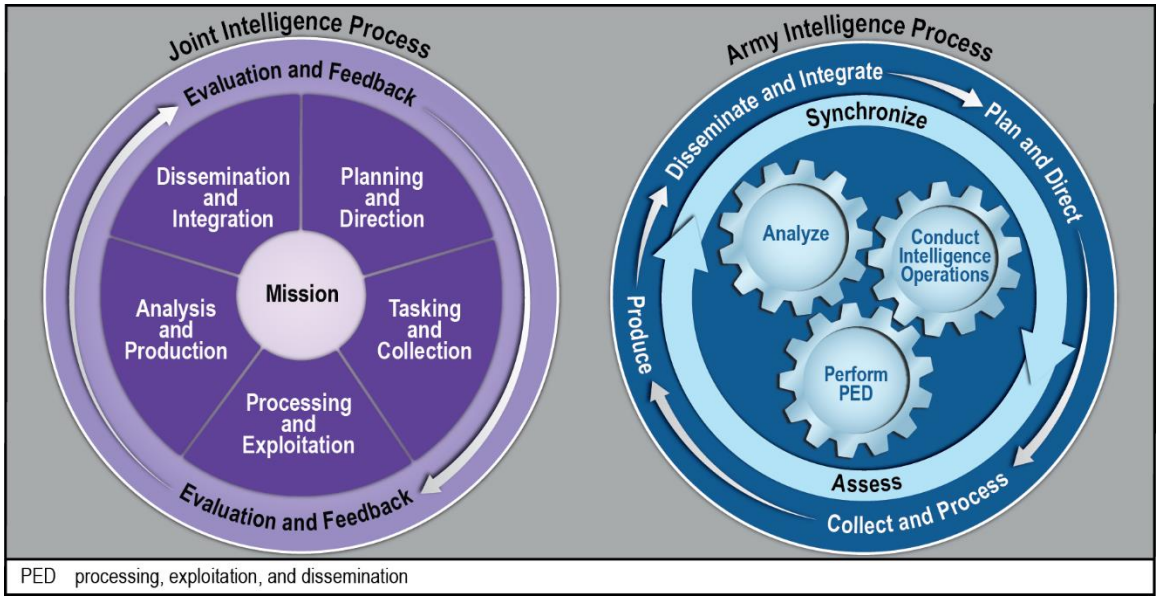


Figure 1-1. The joint and Army intelligence processes

1-28. The Army views the intelligence process as a model and common framework to guide Army professionals in their thoughts, discussions, plans, and assessments about intelligence. When applying the intelligence process, Army intelligence professionals must consider each domain and dimension of the OE to properly account for threat capabilities and plan for information collection. The Army intelligence process leverages all sources of information and expertise, including the IC and nonintelligence entities (through the intelligence enterprise) to provide situational awareness to the commander and staff. The intelligence warfighting function uses the intelligence process as a synchronization and integration tool to ensure the right information and intelligence get to the right user at the right time in the right format without inundating users.

1-29. Commanders drive the Army intelligence process, which G-2/S-2s synchronize and track. The intelligence process, similar to the intelligence warfighting function, involves more than just intelligence professionals; the entire staff—including but not limited to the G-3/S-3, G-6/S-6, G-9/S-9, engineer officer, and fire support coordinator—also has an important role in the intelligence process.

1-30. The intelligence process supports the activities (plan, prepare, execute, and assess) of the operations process; it is performed continuously to support each activity. Although the intelligence process includes unique aspects and activities, it is designed similarly to the operations process:

- The *plan and direct* step and *synchronize* continuing activity of the intelligence process closely correspond to the *plan* activity of the operations process.
- The *collect and process*, *produce*, and *disseminate and integrate* steps and the *conduct intelligence operations*, *perform PED*, and *analyze* continuing activities of the intelligence process together correspond to the *execute* activity of the operations process.
- The *assess* continuing activity is part of the overall *assess* activity of the operations process.

1-31. Figure 1-2 illustrates the Army intelligence process steps, continuing activities, and the interaction between them.

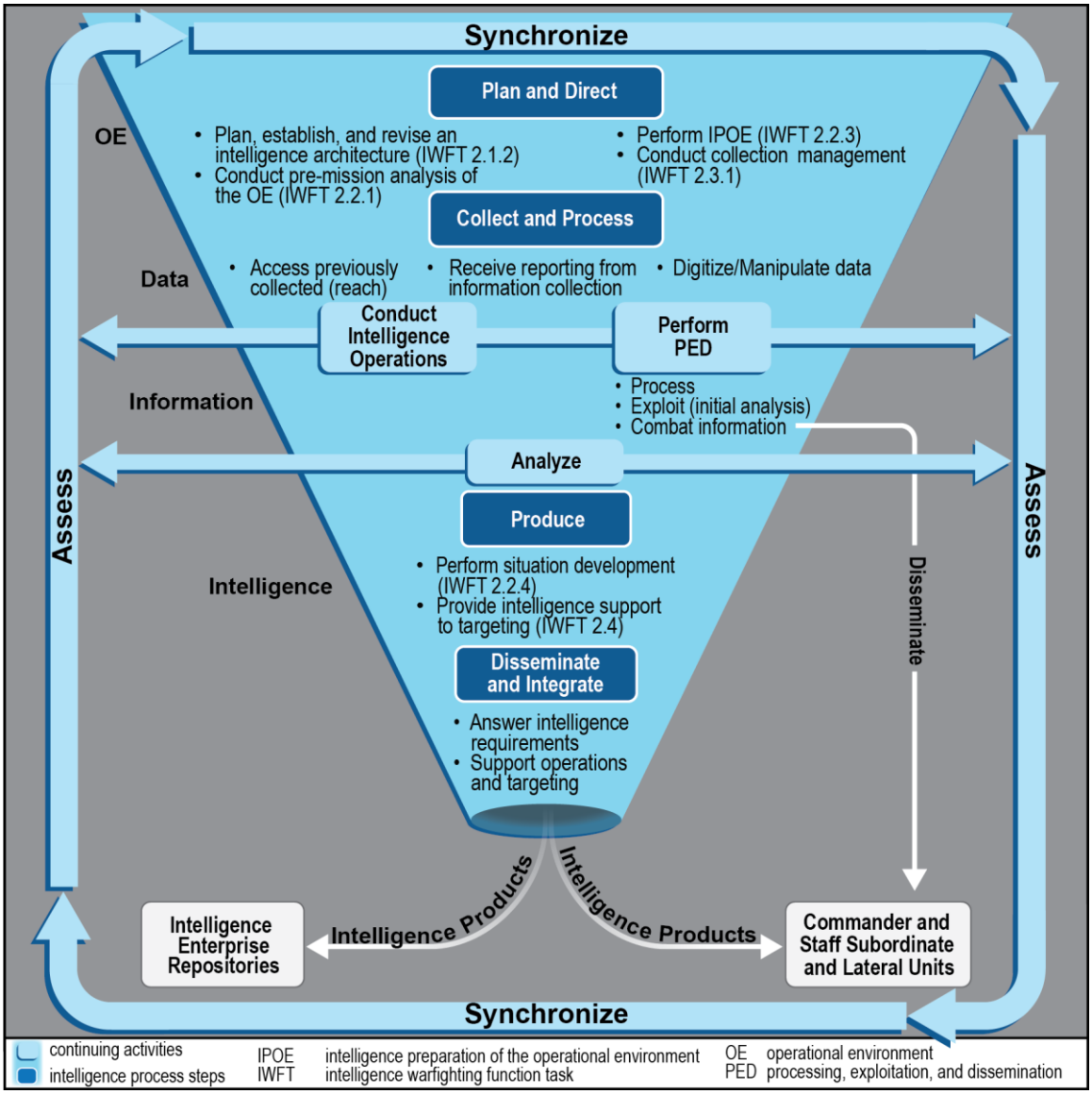


Figure 1-2. The Army intelligence process

INTELLIGENCE PROCESS STEPS

1-32. The intelligence process steps are the most basic actions from the initial planning of an operation to answering an intelligence requirement and ensuring the answer is integrated into the operation. Just as the activities of the operations process overlap and recur as the mission demands, so do the steps of the intelligence process.

Plan and Direct

1-33. Pre-mission analysis of the OE occurs far in advance of detailed planning and orders production. This intelligence assists in focusing information collection and detailed planning upon mission receipt. Intelligence planning is inherent in the Army design methodology (ADM) and the military decision-making process (MDMP). IPOE is an especially important task in planning and directing, as initial IPOE assists in driving the subsequent steps of the MDMP. Intelligence planning should be as collaborative as possible across echelons and encompass various aspects of the OE (in terms of leveraging the intelligence enterprise, considering the different domains and dimensions, and including the entire staff). The goal is to provide effective and flexible intelligence support and thoroughly integrate intelligence with operations.

1-34. The plan and direct step also includes activities that identify key information requirements and develop the means to satisfy those requirements. The intelligence staff collaborates with the operations and signal staffs to plan the intelligence architecture (based on the planned use of intelligence capabilities). Collaboration facilitates parallel planning and enhances all aspects of the intelligence process by enriching analysis, incorporating different points of view, and broadening situational understanding (across all domains and dimensions of the OE). The staff produces a synchronized and integrated information collection plan (based on the collection management plan) focused on answering intelligence requirements.

Intelligence Requirements

An *intelligence requirement* is 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces (JP 2-0). Intelligence requirements primarily comprise priority intelligence requirements (PIRs) but may also include targeting intelligence requirements and other intelligence requirements. After the staff compiles all intelligence requirements, the commander must prioritize them, so the staff understands the exact prioritization of all requirements:

- **PIRs.** A *priority intelligence requirement* is the intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support (JP 2-0). In Army usage, PIRs refer to intelligence requirements that the commander and staff need to understand the threat and other aspects of the OE. PIRs are part of the commander's critical information requirements (CCIRs).
- **Targeting intelligence requirements.** Targeting intelligence requirements refer to those high-payoff target (HPT)-related requirements, outside of what is already captured in PIRs, that the commander specifies as part of the information collection effort. Units are not required to develop targeting intelligence requirements.
- **Other intelligence requirements.** Other intelligence requirements refer to those commander-specified requirements that are either information requirements that do not qualify as PIRs or unanticipated requirements over the course of an operation that are not characterized as PIRs.

Collect and Process

1-35. The entire staff, led by the intelligence staff, synchronizes collection and processing to provide critical information and intelligence at key times throughout the phases of an operation. Collection and processing are mutually dependent. Staffs must not allow a seam to emerge between collection and processing, even when elements conducting those functions are separated geographically. The intelligence staff continuously monitors not only information collection results but also processing results to assess the effectiveness of the overall information collection effort.

1-36. Information collection and processing activities transition when requirements change, the unit mission changes, the unit proceeds through the phase of an operation, or the unit prepares for future operations. Successful information collection and processing results in the timely collection and reporting of relevant and accurate information, which supports intelligence production. The intelligence staff coordinates thoroughly to ensure specific units, capabilities, personnel, equipment (especially communications), and procedures are ready for effective collection and processing.

1-37. Successfully collecting timely, relevant, and useful information against an adaptive threat, especially a peer 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, meet the requirements to collect in the deep, close, and rear areas, and meet the requirements for combat assessment. A successful collection and processing effort requires the operations staff, the intelligence staff, other key staff members, intelligence analysts, and collectors to form an efficient 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 collection control elements and collectors.

Produce

1-38. Production refers to the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections/predictions regarding threats and other relevant aspects of the OE to answer known or anticipated requirements in an effective format. The intelligence staff processes information from single or multiple sources, disciplines, and complementary capabilities and integrates the information with existing intelligence to create finished intelligence products.

1-39. Intelligence products must be timely, relevant, accurate, predictive, and tailored to facilitate situational understanding and support decision making and targeting. The accuracy and detail of intelligence products have a direct effect on operational success. Due to time constraints, analysts sometimes develop products that are not as detailed as they would prefer. However, a timely, accurate answer that meets the commander's requirements is better than a more detailed answer that is late.

1-40. Part of intelligence synchronization is prioritizing and synchronizing the unit's PED and intelligence production efforts. The intelligence staff addresses numerous and varied production requirements based on intelligence 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.

Disseminate and Integrate

1-41. Timely dissemination and integration of intelligence and finished intelligence products are critical to operational success. This dissemination must be deliberate and carefully controlled to ensure the commander, staff, and other appropriate personnel receive the intelligence when needed in the right form at the right time. Additionally, the importance of the intelligence must be understood. Commanders, staff members, and unified action partners must receive and use combat information and intelligence to facilitate situational understanding and support decision making and targeting. Central to successful dissemination to unified action partners is the early and continuous involvement of foreign disclosure officers and supporting representatives.

1-42. The commander and staff must establish and support a seamless intelligence architecture, including an effective dissemination and integration plan. Just because intelligence is delivered does not mean it will be used effectively for planning, decision making, or targeting. The intelligence staff must take appropriate steps to ensure the intelligence is properly considered and used in planning and controlling operations and in conducting targeting. A dissemination and integration plan can be a separate product or integrated into existing products, such as the collection management plan. The plan must include specifications on how it will be integrated and have provisions for dissemination to unified action partners.

INTELLIGENCE PROCESS CONTINUING ACTIVITIES

1-43. The intelligence process continuing activities add details and areas of emphasis to the intelligence process steps. The continuing activities also assist in filling gaps from some of the detailed aspects of the intelligence warfighting function. To support operations, the intelligence warfighting function makes observations about the threat, terrain, weather, civil considerations, and other relevant aspects of the OE. MI units **conduct intelligence operations** resulting in collected data. A dedicated effort **performs PED** to convert the data into useable information for **analysis**. This effort results in intelligence. Because of its complexity, intelligence professionals continually **synchronize** and **assess** this effort to ensure the effectiveness of the intelligence warfighting function.

Synchronize

1-44. *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 (ADP 2-0). Intelligence synchronization integrates intelligence with operations and ensures all requirements are met, as much as feasible, through close collaboration between the commander, G-2/S-2, G-3/S-3, and other members of the intelligence warfighting function.

1-45. Intelligence synchronization occurs through a broader perspective than collection management and includes aspects of long-range intelligence planning, maintaining, and revising the intelligence architecture. Intelligence synchronization could be considered the *orchestration* of the intelligence warfighting function. This holistic activity ensures intelligence support is effective and flexible to meet changing conditions and requirements. While the commander drives the intelligence warfighting function, and the MI unit commander performs an invaluable role, the G-2/S-2 is ultimately responsible for successful intelligence synchronization.

Conduct Intelligence Operations

1-46. *Intelligence operations* are the tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements (ADP 2-0). MI units use the operations process to conduct intelligence operations using mission orders and standard command and support relationships. Flexibility and adaptability to changing circumstances, as well as continuous assessments, are critical for effective intelligence operations. Chapter 6 provides detailed discussion on conducting intelligence operations.

Perform Processing, Exploitation, and Dissemination

1-47. *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 (ADP 2-0). *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 (dissemination) for further analysis or as combat information to the commander and staff.

Analyze

1-48. There are many forms of analysis within Army operations. Analysis assists commanders, staffs, and intelligence leaders in framing the problem, stating the problem, and solving the problem. Leaders and staffs at all levels conduct analysis to assist in making many types of decisions and to conduct targeting. Analysis also occurs in many forms throughout the intelligence process. For example, in collection management

analysis is critical in ensuring information requirements receive the appropriate priority for collection and are assigned to the proper collection asset. The most important form of analysis within the intelligence process is intelligence analysis.

1-49. *Intelligence analysis* is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production (ADP 2-0). The purpose of intelligence analysis is to describe current and predict future threats, terrain and weather, and civil considerations. The following represent two distinct examples of intelligence analysis:

- A single-source collector performing initial analysis—in intelligence, often referred to as exploitation during the collect and process step. The collector adds context to information (analysis) based on experience and knowledge before reporting the information to single-source or all-source analysis elements.
- An all-source analyst performing predictive analysis to identify threat activities and trends that present possible windows of opportunity and subsequent positions of relative advantage to friendly forces. The analyst uses indicators for each threat COA as well threat characteristics and threat models as the basis for the analysis and conclusions.

1-50. Intelligence personnel performing PED as well as analysis must understand and effectively deal with potential information overload. As time progresses, intelligence professionals will experience increases in the volume, pace, and complexity of the data they receive. MI professionals must develop data literacy skills to confront this issue effectively. Until institutional training is adjusted to incorporate data literacy, intelligence professionals must build those skills through self-development. There are some excellent online resources that provide a good starting point to build data literacy skills, such as courses offered through Army MI Data Fundamentals. Data literacy skills will become more important as artificial intelligence/machine learning technologies become more prevalent within intelligence software and systems.

Note. Enrollment information for Army MI Data Fundamentals courses is available on Percipio, the Army eLearning website, on NIPRNET.

Assess

1-51. Assess is part of the overall assessment continuing activity of the operations process. For intelligence purposes, assessment refers to the continuous monitoring and evaluation of the current situation, particularly significant threat activities and changes in the OE. Assessing the situation begins upon receipt of 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 (AOI) interact to form a dynamic OE. The continuous assessment of the effects of each element on the other elements, especially the overall effect of threat actions on friendly operations, is essential to situational understanding. Analysts must consider the domains and dimensions of the OE when performing this continuous assessment.

1-52. The intelligence staff continuously produces assessments based on operations, the threat situation, the information collection effort, and the status of other relevant aspects of the OE. These assessments are critical in—

- Ensuring intelligence requirements are answered.
- Redirecting collection assets to support changing requirements.
- Ensuring operations run effectively.
- Ensuring the proper use of information and intelligence.
- Identifying threat deception and denial efforts.

1-53. The intelligence staff continuously assesses the effectiveness of the information collection effort. This type of assessment requires sound judgment and thorough knowledge of—

- Friendly operations.
- Characteristics of the AOI.
- The threat situation, doctrine, patterns, and projected COAs.

SECTION III – INTELLIGENCE CAPABILITIES

1-54. The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. These capabilities comprise personnel, systems, and supporting technology—all of which are maintained, trained, and employed to conduct intelligence operations to facilitate situational understanding and provide intelligence support to targeting.

1-55. The intelligence staff (chapter 5) and MI units/organizations (chapter 7) collaborate closely to ensure the commander and staff receive all-source and single-source intelligence—the building blocks by which the intelligence warfighting function facilitates situational understanding and supports decision making and targeting. The intelligence warfighting function receives information from a variety of sources. Some of the intelligence sources are commonly referred to as single-source collection. Single-source collection is employed through intelligence operations (the means of information collection performed by MI units), or it is one of the closely related operations (complementary capabilities). Intelligence PED capabilities are also necessary to process information and prepare it for subsequent analysis or target nominations. The intelligence produced from access to information from all (or several) of those information sources or from single-source intelligence is called all-source intelligence.

ALL-SOURCE INTELLIGENCE

1-56. Army forces conduct operations primarily based on all-source intelligence assessments and products developed by the intelligence staff. In joint doctrine, *all-source intelligence* is 1. Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that, in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked (JP 2-0). For the Army, *all-source intelligence* is the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations (ADP 2-0).

ALL-SOURCE ANALYSIS

1-57. The fundamentals of all-source analysis comprise intelligence analysis techniques and the all-source analytical tasks: perform situation development, conduct pre-mission analysis of the OE, perform IPOE, and provide intelligence support to targeting.

1-58. The intelligence staff determines the significance and reliability of the incoming information by comparing it with current intelligence holdings; subsequent analysis and evaluation assist the intelligence staff in determining changes in threat capabilities, vulnerabilities, and probable COAs across the domains and dimensions of the OE. The intelligence staff supports the integrating processes (IPOE, information collection, targeting, risk management, and knowledge management) and the integration of intelligence support into operations by providing all-source analysis of threats, terrain and weather, civil considerations, and other significant aspects of the OE. This support also accounts for human and information dimension effects within the operational and mission variables.

1-59. All-source intelligence is used to develop the intelligence products necessary to aid situational understanding, support the development of plans and orders, and answer intelligence requirements. Although all-source intelligence takes longer to produce, it is more reliable and less susceptible to deception than single-source intelligence.

ALL-SOURCE PRODUCTION

1-60. Fusion facilitates all-source production. For Army purposes, *fusion* is consolidating, combining, and correlating information together (ADP 2-0). Fusion occurs as an iterative activity to refine information as an integral part of all-source analysis.

1-61. All-source intelligence production is continuous and occurs throughout the intelligence and operations processes. Most of the products from all-source intelligence and initially developed during planning are updated, as needed, throughout preparation and execution based on information gained from continuous assessment.

SINGLE-SOURCE INTELLIGENCE

1-62. Single-source intelligence includes the joint intelligence disciplines, which are also the Army intelligence disciplines, and when available (it can differ by echelon) and properly planned, the complementary capabilities from warfighting functions and branches other than intelligence. Intelligence PED capabilities also have an important role within the intelligence disciplines. MI units can conduct intelligence operations with a single intelligence discipline or multiple intelligence disciplines. The intelligence staff depends on non-MI units to provide complementary capabilities as part of the intelligence architecture. However, some complementary capabilities, such as space, document and media exploitation (DOMEX), and electromagnetic warfare (EW) routinely cooperate and provide information to the intelligence architecture.

This publication and ATP 2-01 primarily discuss single-source, multisource, and ancillary collection systems as collection assets. ATP 2-01 added to the discussion to ensure a clear and accurate understanding and use of the term:

- *Collection assets* is a collection system, platform, or capability that is supporting, assigned to, or attached to a particular commander (JP 2-0). In many contexts, *collection assets* are referred to as intelligence assets, intelligence collection assets, or information collection assets to describe units, systems, and sensors that perform information collection.
- *Available collection assets* describe organic, assigned, and attached assets as well as those assets under operational control (OPCON) or in DS of that unit. The unit lists the organic, assigned, attached, OPCON, and supporting units and the overall task organization in Annex A (Task Organization) to the order.
- A *collection resource* refers to a collection system, platform, or capability is not assigned or attached to a specific commander, unit, or echelon and is requested and coordinated through the chain of command of the unit that directs and controls them. A collection asset is subordinate to the requesting unit or echelon, while a collection resource is not.

INTELLIGENCE DISCIPLINES

1-63. An *intelligence discipline* is a well-defined area of intelligence planning, collection, exploitation, analysis, and reporting using a specific category of technical or human resources (JP 2-0). The intelligence disciplines are—

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

1-64. Most intelligence collection, which is part of intelligence operations, occurs within the context of the intelligence disciplines. The intelligence disciplines and the capabilities they provide are varied, effective, and complex. The variety and complexity become most evident when addressing collection and analysis requirements across the domains and dimensions. It requires training and experience to fully understand the intelligence disciplines across echelons. Each intelligence discipline is unique in terms of its authorities, doctrine, training requirements, collection strengths and vulnerabilities, employment techniques, force structure, terminology, technical channels and means of mission management, and supporting PED capabilities.

1-65. Collection from the various intelligence disciplines is integrated during collection management to ensure a multidiscipline approach, which supports effective intelligence analysis, and, ultimately, all-source intelligence. In turn, all-source intelligence facilitates accurate situational understanding, decision making, and support to targeting.

Publicly Available Information Research

Publicly available information (PAI) research is an important aspect of tipping and cueing and planning for intelligence collection as it enhances situational understanding of the OE and enriches the analysis of collected intelligence. While the concept and execution of PAI research is not new, the articulation of PAI research in doctrine and an emphasis on institutional PAI research training are new. Using PAI research thoughtfully within intelligence is critical to effective intelligence support. Using and integrating PAI research ensure commanders and staffs consider the vast amounts of PAI for planning, decision making, and targeting purposes.

Army intelligence staffs, units, and organizations must comply with DODM 5240.01 when conducting intelligence activities such as PAI research. Conducting PAI research and OSINT activities are different from one another. PAI research primarily entails using safe sites or no-risk sites to gather data, facts, instructions, or other material for supporting an intelligence mission; OSINT is derived from PAI collected by trained and certified OSINT collectors/practitioners, who use tools, processes, and analytics to generate operationally relevant intelligence from the vast amounts and variety of PAI. (See ATP 2-22.9.)

Counterintelligence

1-66. CI focuses on the detection, identification, analysis, neutralization, or exploitation of foreign intelligence entities, foreign terrorist organizations, and insider threats to protect Army and designated DOD forces, information, and technologies worldwide. Army CI applies its resources to four primary mission areas—counterespionage, CI support to force protection, information collection to identify and counter threat intelligence collection targeting Army equities, and CI support to technology and critical infrastructure protection. Army CI accomplishes these missions by conducting—

- **Operations** that are broadly executed CI activities that support a program or specific mission. They can be offensive, defensive, or a combination of both, depending on the scope, objective, and/or continued possibility for exploitation.
- **Investigations** to assist in detecting, identifying, countering, and/or neutralizing threat intelligence collection. They also assist in identifying systematic security problems that may have damaging implications to operations and national security interests.
- **Collection** to acquire information about insider threats, foreign intelligence entities, terrorists, and insurgent intelligence collection targeting U.S. operations, personnel, facilities, information, networks, technology, and resources.
- **Analysis and production** to provide the supported commander with the information necessary to gain and maintain situational awareness of threat intelligence information collection targeting Army equities. Complete and effective CI analysis must leverage all intelligence disciplines to assess the full range of threat intelligence capabilities.
- **Technical services and activities** to provide support activities and specialized technical capabilities that support CI operations, investigations, collection, analysis and production, and other intelligence disciplines.

Countering the Foreign Intelligence Entity Threat

A *foreign intelligence entity* is any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupts U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists (DODD 5240.02). Traditionally, CI has focused on countering the foreign intelligence entity HUMINT threat. However, to properly execute the CI mission, CI personnel and organizations must leverage all other intelligence disciplines to assess the full range of threat intelligence capabilities. Multidisciplined intelligence threat assessments and associated countermeasure recommendations are incorporated into strategies, plans, orders, and programs. Therefore, close coordination and cooperation between CI personnel, the supported commander's staff, and interagency partners are essential. Applying CI as a mission supports the targeting process and provides additional options for supported commanders to counter, exploit, and/or neutralize threat intelligence capabilities.

1-67. CI capabilities consist of CI teams and assigned biometric collection equipment. These capabilities produce the following products:

- Intelligence information reports.
- CI investigative reports.
- Threat assessments.
- Notices of intelligence potential.
- Size, activity, location, unit, time, and equipment (SALUTE) and/or spot reports.
- Input to multiagency vulnerability assessments.

1-68. ATP 2-22.2-1 and ATP 2-22.2-2 provide detailed discussions about CI.

Geospatial Intelligence

1-69. *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 or about the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (JP 2-0). GEOINT supports operations through various types of imagery collection within an OE. GEOINT data assists commanders in visualizing the domains and dimensions of the OE. This data includes literal and nonliteral still and motion imagery and geospatial information, all of which allow analysts to see what or who exists in the OE while also assessing what it is doing across time and space. Army GEOINT accomplishes its mission by using elements of the Army Geospatial Enterprise (also known as AGE) and through its subdisciplines:

- *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 likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, 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 2-0).
- *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-0).
- *Geospatial information* is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on or about the Earth, including: data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geomatics data, and related products and services (JP 2-0).

1-70. GEOINT capabilities consist of manned and unmanned platforms and aerial and space-based collection platforms. These capabilities produce the following products:

- Phases I, II, and III full-motion video.
- Panchromatic, infrared, synthetic aperture radar, and moving target indicator exploitation.
- Imagery, initial phase, and supplemental phase interpretation reports.

- Reconnaissance exploitation reports.
- Imagery-derived products.
- Change detection and route density analysis.
- Support to IPOE, target mensuration, and tactical identification of equipment.
- Deliberate and dynamic targeting support.
- Collateral damage and BDA intelligence products.

1-71. ATP 2-22.7 provides detailed discussions about GEOINT.

Human Intelligence

1-72. *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 (ADP 2-0). HUMINT uses human sources as a tool to gather information about the plans, intentions, capabilities, and operations methods of threat military forces. Army HUMINT accomplishes its mission through interrogations, source operations (recruited, nonrecruited, and debriefing), and HUMINT collection support activities (screenings, liaisons, support to targeting, and DOMEX).

1-73. HUMINT capabilities consist of HUMINT collection teams, HUMINT operations cells, and assigned biometric collection equipment. These capabilities produce the following products:

- Intelligence information reports.
- Biographic intelligence information reports.
- Notices of intelligence potential.
- Knowledgeability briefs.
- Collection emphasis messages.
- SALUTE and/or spot reports.

1-74. ATP 2-22.31 and FM 2-22.3 provide detailed discussions about HUMINT.

Measurement and Signature Intelligence

1-75. *Measurement and signature intelligence* is information produced by quantitative and qualitative analysis of physical attributes of targets and events to detect, characterize, locate, and identify targets and events; and derived from specialized, technically derived measurements and signatures of physical phenomenon intrinsic to an object or event (JP 2-0). The purpose of MASINT is collecting technical data associated with warfighting equipment, people, developmental weapons programs, and disseminating data for exploitation to commanders, planners, weapons developers, and policy makers.

1-76. MASINT is based on the principle that every object and event have a signature that can be measured. The measurement aspect of MASINT refers to actual parameter measurements of an event or object such as a biometric attribute, demonstrated flight profile, or range of a cruise missile. Signatures are typically the products of multiple measurements collected over time and under varying circumstances. These signatures are used to develop target classification profiles and discrimination and reporting algorithms for operational surveillance and weapons systems.

1-77. MASINT capabilities consist of unattended ground sensors, infrasonic monitors, and chemical, biological, radiological, and nuclear (CBRN) detectors. Intelligence reach capabilities include scientific and technical intelligence (S&TI), research and development, foreign weapons exploitation, and foreign materiel exploitation. These scientific and technical capabilities—electro-optical, geophysical, human signatures, material, nuclear, radar, and radio frequency—produce the following products:

- Spot reports.
- Preliminary technical reports.
- Complementary technical reports (types A, B, C).
- Attack scene investigation reports.

1-78. ATP 2-22.8 provides detailed discussions about MASINT.

Open-Source Intelligence

1-79. *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 derived from PAI collected by trained and certified OSINT collectors/practitioners, who use tools, processes, and analytics to generate operationally relevant intelligence from the vast amounts and variety of PAI.

1-80. Successful OSINT operations rely heavily on the commander's understanding and guidance about the application of OSINT. Additionally, the intelligence architecture is vital; without it, intelligence capabilities, including OSINT, cannot support operations effectively. OSINT, like all intelligence capabilities, must be fully integrated into the operations process (planning through execution) to support the commander's intent and requirements. The Defense Open-Source Council and the National Open-Source Committee manage OSINT.

1-81. OSINT may include—

- Social media exploitation.
- Access to large data sets for analysis.
- Warning intelligence and tipping and cueing for other collection disciplines.
- Support to targeting and battle damage assessment (BDA).
- Traditional monitoring of press and news outlets, publications, and periodicals.

1-82. Units may obtain OSINT capabilities through the Army OSINT Office. OSINT collectors/practitioners produce the following stand-alone products:

- OSINT reports (also known as OSIR), which may be incorporated into intelligence estimates, intelligence summaries (INTSUMs), intelligence running estimates, and others.
- Tactical OSINT report format (also known as OSINT tipper).

1-83. ATP 2-22.9 and ATP 2-22.9-2 provide detailed discussions about OSINT.

Signals Intelligence

1-84. *Signals intelligence* is intelligence derived from communications, electronic, and foreign instrumentation signals (JP 2-0). SIGINT is one of several military functions operating within the electromagnetic spectrum (EMS); it provides EW support when used in military operations for threat warning, combat information, and situational awareness. According to Title 10, USC, SIGINT teams can perform additional analysis on threat signals to produce intelligence. According to Title 50, USC, Army cryptologic forces produce SIGINT to support the formulation of strategy, policy, military plans, and operations at national to tactical levels.

1-85. SIGINT comprises—

- *Communications intelligence*—technical information and intelligence derived from foreign communications by other than the intended recipients (JP 2-0). Communications intelligence (also called COMINT) is produced from the collection and processing of foreign communications transmitted by radio, wire, or other electromagnetic means and by processing foreign encrypted communications, however transmitted.
- *Electronic intelligence*—technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (JP 3-85). Electronic intelligence (also called ELINT) is produced from the collection (observation and recording) and processing of foreign noncommunications emitters.
- *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 aerospace, surface, and subsurface systems (JP 2-0). Foreign instrumentation SIGINT (also called FISINT) is produced from the intercept, processing, and analysis of foreign telemetry, which refers to the use of telecommunications for automatically indicating or recording measurements at a distance such as signals transmitted by a missile to a ground station.

1-86. SIGINT capabilities consist of terrestrial collection systems; airborne intelligence, surveillance, and reconnaissance (ISR) systems; and theater army collection and survey systems. These capabilities result in the following products:

- CRITIC, KLIEGLIGHT, and tactical (SIGINT) reports.
- IGRAMs (integrated graphics and multimedia reports).
- EGRAMs (electronic serialized SIGINT reports).
- Pattern of life analysis.
- Radar tracking and operational status reporting.
- Tear-line reporting.
- Message transcripts.
- Direction finding/geolocation information.
- Low-level voice intercept.

1-87. ATP 2-22.6 and ATP 2-22.6-2 provide detailed discussions about SIGINT.

Technical Intelligence

1-88. *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 enemy's technological advantages (JP 2-0). TECHINT ensures the Army understands the threat's full technological capabilities as well as its limitations and vulnerabilities. This enables friendly forces to adopt the appropriate countermeasures, operations, and tactics, techniques, and procedures (TTP).

1-89. TECHINT involves the application of forensic science and various technical specialties across seven categories:

- **Communications and electronic equipment**—foreign communications, computers, radars, intercept and jamming equipment, and similar systems, including electro-optical and directed-energy technology.
- **Automation systems**—foreign automation hardware and software.
- **Weapons**—foreign weapons and weapons systems, including improvised explosive devices, associated components, improvised weapons, and conventional weapons (for example, rockets, tube artillery, mortars, small arms, guided missiles, and associated fire control).
- **Munitions**—foreign munitions, including missiles; chemical, biological, and nuclear munitions; direct and indirect fire weapons ammunition; explosives; and mines.
- **CBRN materiel**—foreign CBRN materiel, including toxic industrial materials.
- **Medical materiel**—medical materiel, including general-purpose systems modified for medical support, and biological and chemical agent samplings.
- **Mobility systems**—mobility systems, including vehicles, engineer equipment, materiel-handling equipment, and power generation, which the threat uses to maneuver and support combat forces.

1-90. TECHINT is an intelligence reach capability that includes S&TI, research and development, foreign weapons exploitation, and foreign materiel exploitation. TECHINT products include—

- Spot reports.
- Preliminary technical reports.
- Complementary technical reports (types A, B, C).
- Attack scene investigation reports.

1-91. ATP 2-22.4 provides detailed discussion about TECHINT.

COMPLEMENTARY CAPABILITIES

1-92. JP 2-0 recognizes the following intelligence applications: identity intelligence (I2), biometrics, forensics, and DOMEX. The Army also recognizes various specialized capabilities that can contribute to all-source or single-source intelligence through intelligence coordination with other warfighting functions and branches. These specialized and technical capabilities, many of which are not typically conducted by MI units, can provide valuable insight into threat activities and intentions and can fill intelligence gaps. In some instances, they can provide critical information that supports security, consolidating gains, and rear area operations. These capabilities include but are not limited to the following:

- Biometrics.
- Cyberspace.
- DOMEX.
- EW.
- Forensics.
- Identity activities.
- Space.

Biometrics

1-93. *Biometrics* is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). According to DODD 8521.01E, the Secretary of the Army is the DOD executive agent for biometrics. A *biometric* refers to a measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. The term biometrics designates characteristics of an individual and a process. As a process, biometrics consists of the automated methods used to recognize an individual based on measurable biometric characteristics.

1-94. The collecting, processing, matching, and intelligence analysis of biometric data support the positive identification and characterization of individuals who may pose a threat to U.S. national security. They provide a powerful capability for DOD to identify and respond to threat personnel, protect friendly forces, and defend national interests. The success of DOD and DOD's partners in identifying such threats is further improved by sharing biometric data with interagency and international partners. Therefore, it is important to employ a comprehensive, coordinated approach for biometric data collection as well as foster sharing agreements with interagency and foreign partners.

1-95. Incorporating biometric information into all-source intelligence analysis is a highly successful technique for enabling U.S. forces to strip away the anonymity of threat fighters. Biometric information is one of the identity attributes that contributes to I2. With an extraordinary degree of confidence, U.S. forces can link enemy activity to previously unidentified threat personnel using biometric technology.

Cyberspace

1-96. A *cyberspace capability* is a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace (JP 3-12). The use of cyberspace capabilities facilitates understanding the threat's cyberspace capabilities, intentions, potential actions, and vulnerabilities, as well as their impacts on the environment, friendly operations, and the local populace. Cyberspace capabilities depend on an established technical architecture. Intelligence produced using cyberspace capabilities 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 a 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.

1-97. Due to its very nature, intelligence operations in the cyberspace domain require significant lead time to accomplish. Intelligence operations and analysis in the cyberspace domain also require additional and specific authorities, oversight, training, and specialized equipment. For example, the use of computers, technology, and networks facilitates all-source intelligence, the intelligence disciplines, and other intelligence capabilities. However, intelligence professionals' use of computers, technology, and networks does not mean they are conducting cyberspace operations. The authority for each discipline or capability governs the guiding methods and regulations for the conduct of each intelligence discipline or intelligence capability.

Note. The results of cyberspace electromagnetic activities (CEMA) can provide intelligence professionals a significant amount of information about the human, information, and physical dimensions.

Document and Media Exploitation

1-98. ***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**. Threat intent, capabilities, and limitations may be derived through the exploitation of captured documents and media.

1-99. DOMEX is an increasingly specialized, full-time mission requiring advanced automation and communications support, analytical support, and qualified 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 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.

Electromagnetic Warfare

1-100. *Electromagnetic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-85). EW consists of three distinct divisions—electromagnetic attack (EA), electromagnetic support (ES), and electromagnetic protection (EP). JP 3-85 and FM 3-12 provide detailed discussions about EW and its three divisions.

1-101. *Electromagnetic attack* is division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). EA requires close coordination with intelligence to ensure assets are used at the correct location and time and operate in the correct portions of the EMS to achieve desired effects. Throughout an EA mission, intelligence provides reattack recommendations and BDAs to the CEMA section to inform the continuation, redirection, conclusion, or outcome of an EA. EA denies the threat the ability to use the EMS or spectrum-dependent equipment (see ATP 3-12.3). The deliberate use of EA can provide opportunities for intelligence collection and expose threat capabilities and vulnerabilities.

1-102. *Electromagnetic support* is division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations (JP 3-85). ES acquires adversary combat information to support the commander's maneuver plan. Data collected through ES can also support SIGINT PED to support the commander's intelligence and targeting requirements and provide situational understanding. ES assists in conducting analysis of the EMS for inclusion in IPOE. This analysis must include updating the electromagnetic order of battle and providing the intelligence staff threat EW capabilities and information for inclusion in threat characteristics and threat models. Through the integration of significant aspects of ES and CEMA into IPOE, SIGINT, EW, and spectrum management operations information are integrated into the threat, situation, and event templates, which are developed during IPOE, and the decision support template, which is developed during the MDMP. ES also provides the CEMA section with indicators of EA measures of effectiveness by monitoring target frequencies and ranges. Frequency monitoring efforts are supplemented by intelligence assets, as needed.

1-103. *Electromagnetic protection* is division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). EP facilitates the friendly use of the EMS if, through analysis of the EMS, the threat is understood; this supports IPOE. In coordination

with the G-6/S-6 and the CEMA section, ES, intelligence systems, and personnel may inform EP efforts by providing information about an organization's radio frequency signatures throughout all emission control levels as well as sources and locations of EMS interference or jamming.

Electromagnetic Spectrum Actions

Although EMS actions and EW capabilities are different, they are related. Ensuring the effective integration of SIGINT operations, EW, cyberspace operations, and spectrum management operations requires the technical control and analysis cell and the CEMA section to coordinate their operations in the EMS. SIGINT operations and EW in the EMS may overlap, requiring constant and close coordination for spectrum deconfliction and mutual support. This coordination and support can reduce instances of intelligence loss and improve collection and targeting for SIGINT collection teams, EW teams, and cyberspace operations. Although SIGINT, EW, and cyberspace operations function under different authorities and regulations, they are complementary in providing input to the electromagnetic order of battle developed for integration into IPOE. SIGINT, EW, and cyberspace operations can cross-cue for warning intelligence, collection, and electromagnetic reconnaissance.

Forensics

1-104. *Forensic science* is the application of multidisciplinary scientific processes to establish facts (DODD 5205.15E). 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 (also called DNA), and other forensic data can aid in more in-depth analysis and better intelligence about the OE.

1-105. Forensics can assist in identifying an adversary's key personnel, tactics, intent, and capabilities (current and future). Forensic exploitation of collected exploitable material—

- Provides answers to commanders' information requirements.
- Supports offensive and defensive operations.
- Influences decision making.
- Develops timely, relevant, accurate, predictive, and tailored intelligence.
- Increases situational understanding of complex, uncertain OEs.

1-106. *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). Forensic-enabled intelligence assists in accurately identifying persons, networks, and complex threats, and it attributes them to specific incidents and activities. (See JP 2-0 for doctrine on forensic-enabled intelligence.)

Identity Activities

1-107. Identity activities refer to a collection of functions and actions that appropriately recognize and differentiate one person or persona from another person or persona to support decision making as well as security, force protection, and law enforcement. They include the collection, processing, and exploitation of identity attributes and physical materials to inform policy and strategy development, planning, and assessment and to enable prosecution and the appropriate action at the point of encounter. Some of this data and information can inform all-source analytic efforts, leading to the production of I2.

1-108. I2, as defined in paragraph 1-7, is used to disrupt competitors, support joint operations, counter threats, deny anonymity to the Nation's adversaries, and protect the Nation's assets, facilities, and forces. Units and organizations use I2 products informed by capabilities such as biometrics, forensics, and DOMEX as well as information from the intelligence disciplines.

1-109. I2 is currently produced at echelons corps and above from the fusion of all-source and multidisciplined reporting. It results in intelligence from the human dimension, which encompasses the interaction among individuals and groups, how they understand information and events, make decisions, generate will and act within an OE. Intelligence analysts use I2 products to identify relevant actors and provide intelligence that allows a commander to anticipate those actors' behaviors and the potential consequences of their behaviors. *Relevant actors* refer to actors who could substantially impact campaigns, operations, or tactical actions. Understanding this human element across the strategic contexts is essential to commanders' efforts to defeat, destroy, deny, or disintegrate the enemy.

Space

1-110. A *space capability* is 1. The ability of a space asset to accomplish a mission. 2. The ability of a terrestrial-based asset to accomplish a mission in or through space. 3. The ability of a space asset to contribute to a mission from seabed to the space domain (JP 3-14). The use of space capabilities is inherently joint. The Army uses space capabilities and effects to support its dominance in land operations. The need for the Army to accomplish space-enabled operations is firmly established in policy and practice. Space capabilities are integrated into Army operations across all domains. Army space operations executed through the seven codified joint space capabilities impact intelligence support:

- *Space situational awareness* is the requisite foundational, current, and predictive knowledge and characterization of space objects and the operational environment upon which space operations depend (JP 3-14). Space situational awareness involves characterizing, as completely as necessary, the space capabilities operating within the terrestrial environment and the space domain. It is the contribution of space and intelligence knowledge and analysis to IPOE.
- *Positioning, navigation, and timing* refers to a space-based capability that is a mission-essential element in nearly every modern weapons system. Army space Soldiers assigned to units at multiple echelons or attached to units during crisis or armed conflict can provide tailored products and system expertise about the capabilities of satellite-based positioning, navigation, and timing systems to enable precision fires. They can also assess and provide an understanding of the usage of adversary positioning, navigation, and timing systems as well as counter-positioning, navigation, and timing capabilities.
- *Space control* is operations to ensure freedom of action in space for the United States and its allies and deny a threat freedom of action in space (JP 3-14). Army space control assets can sense and detect activity within or from the space domain that can influence Army operations. Army space control systems are manned by Soldiers that are trained to understand significant operational aspects of friendly or enemy use of the space domain and can significantly contribute to IPOE, targeting, and planning to support multidomain operations and convergence.
- *Satellite communications* provide—
  - The necessary connectivity for worldwide communications and mobile forces operating over large, dispersed areas.
  - The Army with critical connectivity to tactical maneuver forces and Soldiers, whose rapid movement and geographically dispersed deployments move them away from direct access to land lines and line of sight communications.
  - The means for Army intelligence reach to theater or continental United States (CONUS)-based analytic centers for PED support.
  - Through its assets, analytic reach and possibly the first indication of adversary activities to disrupt U.S. satellite communications that may not be detected by other Army collection assets. This contributes to situational understanding.
- *Missile warning* refers to a space-based system of systems that provides warnings to the Army and joint force of adversary long-range fires, including missiles, rockets, and artillery. Missile warning assets can also contribute to greater situational awareness through battlefield characterization capabilities inherent to space-based missile warning sensors. Missile warning assets can likely provide deep sensing to Army intelligence and provide warnings and assessments of potential adversary missile-unit targeting efforts.

- *Environmental monitoring* enables space forces to provide data on meteorological, oceanographic, and space environmental factors that might affect military operations. Space capabilities provide data for space-environment forecasts, alerts, and warnings that may negatively impact space assets, space operations, and terrestrial users. Imagery capabilities can provide joint force planners current information on subsurface, surface, and air conditions, such as trafficability and land use, beach conditions, vegetation, cloud cover, and moonlight percentage. Knowledge of these factors allows ground forces to avoid adverse environmental conditions while taking advantage of other conditions to enhance operations. This space-based capability supports IPOE by providing the information needed to identify and analyze potential COAs.
- *Space-based ISR* is a joint space capability. Space-based sensors allow Army intelligence components to access information and characterize activity in denied areas. They also provide a key capability that enables long-range fires during Army multidomain operations.

1-111. FM 3-14 discusses Army space operations and Army space forces, capabilities, and formations, as well as their contributions to multidomain operations.

INTELLIGENCE PROCESSING, EXPLOITATION, AND DISSEMINATION CAPABILITIES

1-112. Intelligence PED capabilities are the personnel, specialized intelligence and communications systems, software and advanced technologies that execute the PED continuing activity. Intelligence PED capabilities can perform PED from a deployed location or reach site in theater or the United States. Intelligence PED can be organic to the intelligence unit, task-organized, or distributed from a centralized location through the network, as required.

1-113. The intelligence staff advises the rest of the staff on intelligence PED requirements when planning information collection operations. The commander and staff resource and prioritize supporting intelligence capabilities, including PED, through thorough staff planning based on G-2/S-2recommendations.

1-114.When requesting intelligence PED, the gaining G-2/S-2, intelligence unit commander, and the allocating unit commander are responsible for coordinating and planning intelligence PED activities. Some intelligence PED employment considerations for the gaining G-2/S-2 and intelligence unit commander include—

- **Intelligence architecture.** Employing intelligence PED capabilities depends on how the collection assets and supporting PED fit into the intelligence architecture. The employment is also specific to the intelligence discipline, and in some instances, the complementary 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.** System operators must be thoroughly knowledgeable of the different requirements needed to support targeting criteria, including minimum accuracy and timeliness standards for each specific HPT to meet the commander's desired effects.
- **Technical channels.** System operators must understand how technical channels operate and how to use technical guidance to enhance collection. Additionally, intelligence PED personnel assist in refining technical guidance.

- **Training.** Intelligence leaders inform the commander and staff of intelligence PED capabilities and limitations. Facilitating the integration of intelligence PED activities requires intelligence leaders to train the intelligence unit and intelligence PED system operators, analysts, and maintainers.
- **Sustainment.** Intelligence PED capabilities can pose a significant maintenance and logistics challenge to the intelligence unit. Reducing these challenges requires the intelligence unit to conduct thorough planning and coordination.

SECTION IV – THE INTELLIGENCE ARCHITECTURE

1-115. The intelligence architecture is the compilation of all relevant intelligence and communications capabilities, data repositories, organizations, supporting capabilities, and personnel necessary to ensure the successful execution of the intelligence process. This architecture enables intelligence activities and intelligence operations, including leveraging the intelligence enterprise, that in turn supports operations. At the most basic level, the intelligence architecture connects the many different all-source, single-source, and PED capabilities (which include people, systems, technology, mission management, and technical control, among other aspects) across a unit's AO and to higher, lower, and adjacent headquarters and units. The intelligence architecture depends highly on both specialized intelligence communications and the standard communications network.

1-116. To establish an effective intelligence architecture, it is important to understand its key aspects and limitations:

- The commander and staff must adequately resource the intelligence architecture. This includes sufficient network capability (for example, bandwidth) and access. Network access and effective unit communications are especially critical.
- All intelligence support is meaningless without communications, which should be planned using a primary, alternate, contingency, and emergency (PACE) plan unique to echelon and theater.
- There are almost always more requirements for intelligence collection than there are capabilities and systems.
- All-source intelligence analysis forms the central portion of the analytical backbone of the intelligence architecture.
- The PED structure is an important component of the intelligence architecture. Processing is inherent within all intelligence collection.
- MI unit C2, technical channels, and technical control are important parts of the intelligence architecture.
- Each echelon has unique challenges based on the strategic context, operation, threat, situation, and specific mission. The threat always attempts to counter or minimize friendly intelligence collection.
- Intelligence capabilities and specific collectors face challenges such as communications, technical parameters, weather, terrain effects, survivability, sophisticated equipment, and intelligence and electronic warfare (IEW) maintenance and other logistics support.
- The intelligence architecture must account for any augmentation or task organization of additional intelligence capabilities.

1-117. Establishing and maintaining the intelligence architecture requires well-trained, highly proficient intelligence professionals due to the highly technical nature of portions of the architecture. At any point in time, different MI units, different echelons, and the different Components (Active Component, United States Army Reserve [USAR], and the Army National Guard [ARNG]) are fielded with different intelligence systems, different versions of the same intelligence system, or with different versions of software on the intelligence systems.

Note. When necessary, for the sake of relevance, usefulness, and content comprehensibility, this publication discusses specific intelligence systems, regardless of their impending replacement before this publication's next revision.

1-118. The complexity of the intelligence architecture can be exemplified through a portion of the architecture referred to as *foundation layer*. The foundation layer supports all-source and single-source analysis and production through technical aspects such as data management, sensor processing, interoperability, data standards, and other advanced services. Examples of fielded and partially fielded systems and applications within the foundation layer include the GEOINT Workstation (also known as GWS), Carbon/Capability Drop 1 (also known as CD1), and Army Intelligence Data Platform/Capability Drop 2 (also known as AIDP/CD2).

Note. Due to the variety of fielded and partially fielded systems and applications, this publication will refer to them generically as *intelligence analysis systems*.

1-119. For more discussion on the intelligence architecture see chapter 5 and appendix B.

SECTION V – FIGHTING FOR INTELLIGENCE AT AND ACROSS ECHELONS

1-120. Providing effective and flexible intelligence support against a determined and adaptive threat—whether a peer threat or terrorist cell—is a significant challenge referred to as *fighting for intelligence*. Fighting for intelligence spans the Army strategic contexts; several factors create this challenge, hindering the provision of effective and flexible intelligence support:

- Threat efforts to deny, minimize, or confuse friendly information collection from camouflage, countermeasures, and deception to lethal counterreconnaissance during armed conflict.
- The inherent complexities of information collection. Any single collection capability is likely not effective enough in answering all intelligence requirements; managers should employ multiple capabilities to enhance collection results.
- The complexities associated with intelligence readiness and the intelligence enterprise and architecture.
- The complexities of multidomain operations and many competing demands on the intelligence warfighting function.
- The difficulties inherent in understanding the domains and dimensions of the OE, especially the human and information dimensions where events do not occur purely based on logic, and the information dimension where activities are often inseparable from ground operations.
- The fog and friction of operations; this can occur even during competition below armed conflict and crisis.
- Perfect planning and intelligence production seldomly occurring. There are frequent time constraints and other complications in performing important staff planning and intelligence processes.

1-121. The challenge to provide effective and flexible intelligence support constantly changes. Factors that influence this challenge include but are not limited to—

- The threat (or threats) and how it adapts.
- Threat countermeasures against friendly information collection.
- The OE and conditions within a particular Army strategic context.
- The friendly echelon and type of unit.
- The friendly overall operation.
- The friendly mission.
- Intelligence authorities and architecture.
- Intelligence requirements.

1-122. Two concepts related to fighting for intelligence during competition below armed conflict and crisis that are critical to setting conditions for effective intelligence support during a large-scale combat operation (armed conflict) are—

- **Setting the globe:** The United States Army Intelligence and Security Command (INSCOM) and other echelons above corps intelligence staffs, organizations, and units constantly collaborate to address the ends, ways, and means to sustain and improve national to tactical intelligence capabilities globally. This concept focuses on supporting modernization and preparing for the future fight—a fight that is faster and more lethal, information-centric, and globally interconnected—while building near-term strategic readiness and executing current intelligence missions.
- **Setting the theater:** This describes the broad range of actions conducted to establish the conditions in an operational area. The intelligence warfighting function must constantly set the theater for 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 engagements and operations as the Army transitions from one strategic context to the next. (See ADP 2-0.)

1-123. Fighting for intelligence is most challenging during large-scale combat operations as the threat can apply operational reach, contest friendly deployments, leverage highly lethal and effective nonlethal capabilities across multiple domains, and influence friendly forces across multiple dimensions. Gaining situational understanding of a peer threat is very complicated because of antiaccess (A2) and area denial (AD) capabilities such as long-range precision fires and integrated air defense systems (IADSs). Situational understanding is often more difficult to reach within the relevant aspects of the human and information dimensions. Maneuver units, not just MI units, must be prepared to fight for intelligence to gain information against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the OE. The commander and staff will have to make difficult choices in terms of accepting risk to Soldiers conducting information collection.

1-124. Key aspects of fighting for intelligence include the following:

- Commanders drive intelligence.
- Effective staff integration is crucial.
- Effective intelligence requires leveraging the intelligence enterprise and actively maintaining the intelligence architecture.
- The struggle to gain and maintain a continuous and relatively complete understanding of the OE across the domains and dimensions.
- A thoroughly developed and flexible information collection plan focused on the right requirements is critical.

1-125. During the fight for intelligence, conducting information collection requires thorough and creative planning, aggressive execution, and adjustments based on the situation. The G-2/S-2—in coordination with the G-3/S-3 and integration with other staff members, leveraging national to tactical collection capabilities—has an integral part in fighting for intelligence to identify and ultimately open windows of opportunity at the right time and place to leverage one or more capabilities across domains. Staff integration is crucial; the staff must collaborate to overcome challenges and mitigate information collection capability risks and system limitations by developing an integrated information collection plan synchronized and nested across echelons.

Chapter 2
Multidomain Operations and Intelligence

SECTION I – OVERVIEW

2-1. To provide effective and flexible intelligence support, intelligence professionals must understand multidomain operations. FM 3-0 provides many doctrinal concepts that are important to intelligence professionals. (See figure 2-1.) This chapter presents the following FM 3-0 doctrinal concepts and how intelligence relates to each concept:

- Army operations within a joint strategic context; challenges for Army forces; the strategic environment, including threats and peer threats; and the Army strategic contexts (section II).
- Understanding a broad OE and focusing the elements of the OE to support an Army unit's specific mission (section II).
- The fundamentals of operations—Army operations, multidomain operations, large-scale combat operations, combined arms and combat power, multidomain operations as the Army's operational concept, and operational approach and operational framework (section III).

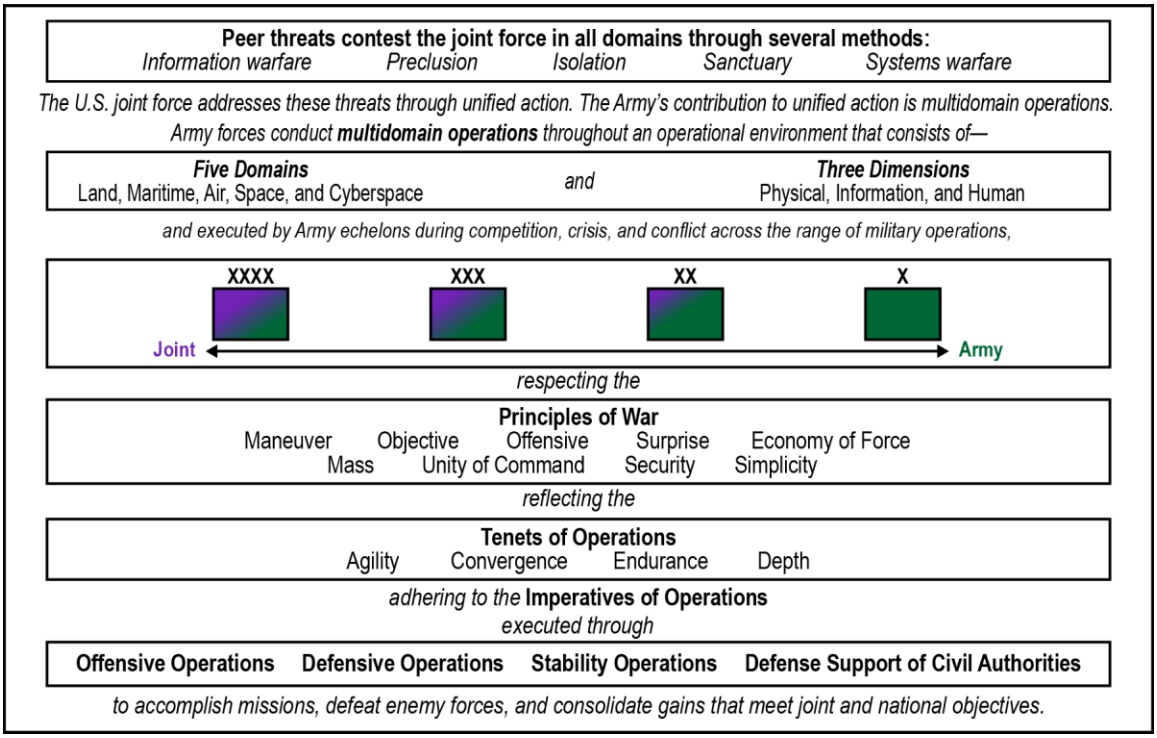


Figure 2-1. FM 3-0 logic chart

Note. Throughout this chapter are blue boxes following operational concepts discussed in FM 3-0. These blue boxes address different aspects of intelligence related to these operational concepts.

Intelligence (Multidomain and Multidimension)

All Army operations are multidomain operations. Similarly, Army intelligence activities, at and across echelons, consider the domains and dimensions:

- The information collection effort, including collection by the intelligence disciplines and complementary capabilities.
- Intelligence PED, analysis, and production in developing threat objectives and intent, characteristics, capabilities, targets, and COAs, as well as in analyzing civil considerations and other significant aspects of the OE.
- All intelligence analysis tasks, such as pre-mission analysis of the OE, IPOE, situation development, and intelligence support to targeting, as well as collection management and intelligence architecture tasks.

Readers should not misinterpret any isolated portions of FM 2-0 and assume the intelligence activity or task does not account for all domains and the human, information, and physical dimensions.

SECTION II – STRATEGIC AND OPERATIONAL ENVIRONMENTS

2-2. The Army intelligence warfighting function is designed to provide effective and flexible intelligence support to all Army forces. However, providing this intelligence support is challenging; the corresponding Army strategic context, relevant factors of the OE, echelon, unit type, and specific mission all significantly affect intelligence support. Therefore, there are several aspects to consider when providing effective and flexible intelligence support; while not all encompassing, three important general aspects are—

- Employing and adapting all available intelligence capabilities in the context of the current situation and a unit's mission/operation.
- Knowing and adapting intelligence and operational fundamentals (largely captured in Army doctrine) in the context of the current situation and a unit's mission/operation.
- Building and maintaining tactically and technically proficient intelligence professionals who are effective in both the profession of arms and the intelligence profession.

ARMY STRATEGIC CHALLENGES

2-3. The joint force deters most adversaries from achieving strategic objectives through direct military confrontation with the United States. Therefore, adversaries pursue their objectives indirectly through malign activities and armed conflict, targeting others in ways calculated to avoid war with the United States. These activities include subversive political and legal strategies, establishing physical presence on the ground to buttress resource claims, coercive economic practices, supporting proxy forces, and spreading disinformation. However, several adversaries have both the ability and the will to conduct armed conflict with the United States under certain conditions. This requires Army forces to be prepared for limited contingencies and large-scale combat operations.

2-4. Global and regional adversaries apply all instruments of national power to challenge U.S. interests and the joint force. Militarily, they have extended the battlefield by employing network-enabled sensors and long-range fires to deny access during conflict and challenge friendly forces' freedom of action during competition. These standoff approaches seek to—

- Counter U.S. space, air, and naval advantages to make the introduction of land forces difficult and exploit the overall joint force's mutual dependencies.
- Increase the cost to the joint force and its partners in the event of armed conflict.
- Hold the joint force at risk both in the United States and at its overseas bases and contest Army forces' deployment from home station to forward tactical assembly areas overseas.

Note. *Instruments of national power* are all of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational, and military (JP 1, Volume 1).

2-5. Adversary actions increase the level of risk to the U.S. joint force in order to raise the threshold at which the United States might respond to a provocation with military force. By reducing the joint force's conventional deterrence, adversaries believe they have greater freedom of action to conduct malign activities both within and outside the U.S. homeland. Adversaries exploit this freedom of action through offensive cyberspace operations, disinformation, legal operations, influence operations, unconventional forces, and the aggressive positioning of ground, air, and naval forces to support territorial claims. Adversaries employ different types of forces and capabilities to attack private and government organizations, threaten critical economic infrastructure, and disrupt political processes, often with a degree of plausible deniability that reduces the likelihood of a friendly military response.

2-6. During crisis and armed conflict, enemies typically initiate their aggression under conditions optimal for their success, requiring U.S. forces to respond at a disadvantage. U.S. combat operations typically involve force projection over long distances, providing advantages for enemy forces operating closer to their bases of support. Enemies typically have a degree of popular support cultivated through decades of propaganda and isolation from the free flow of information. This increases the enemy's will to fight and can make local populations hostile to U.S. forces and objectives.

2-7. Army forces overcome challenges posed by threats and the environment with credible formations able to employ lethal capabilities. Credible combat forces are those able to overcome the advantages adversaries generate within a specific regional context. *Lethality* is the capability and capacity to destroy (FM 3-0). Employing and threatening the employment of lethal force are at the core of how Army forces achieve objectives and enable the rest of the instruments of national power to achieve objectives.

2-8. Lethality is enabled by formations maneuvering into positions of relative advantage where they can employ weapons systems and mass effects to destroy enemy forces or place them at risk of destruction. The speed, range, and accuracy of weapons systems employed by a formation enhance weapons systems' lethality. The demands of large-scale combat rapidly deplete available stockpiles and require forces to retain large reserves of ammunition, weapons, and other warfighting capabilities. Leaders multiply the effects of lethal force by employing combinations of capabilities through multiple domains to create, accrue, and exploit relative advantages—imposing multiple dilemmas on enemy forces and overwhelming their ability to respond effectively.

2-9. Intelligence is inherently multidomain, joint, interagency, intergovernmental, and multinational. The intelligence warfighting function supports lethality directly by providing effective and flexible intelligence support to large-scale combat operations—the Army's modernization focus. However, intelligence support is critical to all Army strategic contexts. The intelligence warfighting function strives to provide commanders and staffs with the timely, relevant, accurate, predictive, and tailored intelligence required to visualize the OE, assess the situation, set the theater, direct military actions, and establish positions of relative advantage across the domains and dimensions of the OE as a part of the joint force.

2-10. Table 2-1 lists several intelligence considerations associated with Army strategic challenges.

Table 2-1. Intelligence considerations for Army strategic challenges

Army strategic challenge	*Intelligence considerations (not all-inclusive)*
Gaining and maintaining support of allies and partners.	• Gaining the proper authorities. • Write to release and intelligence sharing. • Multinational interoperability and using systems such as CENTRIXS and the US BICES. • Security force assistance and engagements. • Language support. • Discrediting disinformation and misinformation.
Maintaining the continuous information collection needed to determine the composition, disposition, strength, and activities of enemy forces.	• Access to the intelligence enterprise and architecture. • Access to experts on the different regional governments and civil components of the operational environment. • Information collection, analysis, and Intelligence reach. • Intelligence processing, exploitation, and dissemination. • Warning intelligence. • Intelligence preparation of the operational environment. • Collection management.

Table 2-1. Intelligence considerations for Army strategic challenges (*continued*)

Army strategic challenge	*Intelligence considerations (not all-inclusive)*
Integrating and synchronizing intelligence at all echelons, distributed across large operational areas with diverse requirements.	• Commander involvement and staff teamwork. • Access to the intelligence enterprise and architecture through intelligence reach. • Intelligence processing, exploitation, and dissemination. • Developing and maintaining the common intelligence picture. • Synchronizing intelligence activities across deep, close, and rear areas.
Preparing forward-stationed forces to fight and win while outnumbered and isolated.	• Military intelligence training and integrating military intelligence forces into formations. • Military intelligence force tailoring. • Pre-mission analysis of the operational environment. • Intelligence preparation of the operational environment. • Intelligence application of the imperatives of operations.
Protecting forward-positioned forces and those moving into a theater.	• Leveraging the intelligence enterprise during force projection through intelligence reach. • Intelligence support to protection. • Counterintelligence primary mission areas. • Continuous information collection.
Minimizing vulnerability to weapons of mass destruction.	• Access to the intelligence enterprise and special collection capabilities. • Warning intelligence. • Intelligence preparation of the operational environment. • Support (including terrain and weather analysis) to unit dispersion across operational environments.
Maintaining command and control and the sustainment of units distributed across vast distances in noncontiguous areas and outside supporting ranges and distances.	• Access to the intelligence enterprise and architecture. • Synchronizing intelligence activities across deep, close, and rear areas. • Support to sustainment.
Maintaining a desirable tempo while defeating fixed and bypassed enemy forces.	• Intelligence activities to consolidate gains. • Coordination with military police and other friendly forces. • Continuous information collection. • Support to targeting. • Synchronizing intelligence activities across deep, close, and rear areas.
Defeating threat information and irregular warfare attacks against the United States and strategic lines of communications.	• Intelligence support to information advantage. • Discrediting disinformation and misinformation. • Integration into joint special operations forces' intelligence efforts.
CENTRIXS Combined Enterprise Regional Information Exchange System US BICES United States Battlefield Information Collection and Exploitation System	

STRATEGIC ENVIRONMENT

2-11. The central challenge to U.S. security is the reemergence of long-term, great power competition with China and Russia as individual actors and as actors collaborating to achieve common goals. China uses its rapidly modernizing military, information warfare, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to its advantage. Additionally, *The Belt and Road Initiative*, a massive China-led infrastructure project, aims to globally create influence. Concurrently, Russia continues to expand influence in its near abroad and adversely affect security through strategic messaging, economic manipulation (energy and trade), and conflicts in Eastern Ukraine and Georgia. Russia's capabilities challenge the security environment in Europe.

2-12. In addition to China and Russia, several other states threaten U.S. security. North Korea seeks to guarantee survival of its regime and increase its leverage. It pursues a combination of CBRN, conventional, and unconventional weapons and a growing ballistic missile capability to gain coercive influence over South Korea, Japan, and the United States. Similarly, Iran seeks dominance over its neighbors by asserting an arc of influence and instability while vying for regional hegemony. Iran uses state-sponsored terrorist activities, a network of proxies, and its missile capabilities to achieve its objectives.

2-13. While states are the principal actors on the global stage, nonstate actors also threaten the strategic environment with increasingly sophisticated capabilities. Terrorists, transnational criminal organizations, threat cyberspace actors, and other malicious nonstate actors have transformed global affairs with increased capabilities of mass disruption. Terrorism remains a persistent tactic driven by ideology and enabled by political and economic structures.

2-14. U.S. intelligence carefully watches the Nation's adversaries. Army intelligence is crucial to DOD efforts to prepare for large-scale combat operations. Additionally, Army intelligence heavily leverages the intelligence enterprise for unique and comprehensive intelligence on the Nation's adversaries. As part of various theater efforts, Army intelligence is heavily involved in setting the theaters to prepare for potential conflicts. In effect, Army intelligence doctrine uses the term set the theater to describe certain doctrinal intelligence concepts. (See chapter 8 for more about intelligence during large-scale combat operations.)

2-15. INSCOM is globally engaged and closely involved in intelligence operations within multiple combatant commands. Some of these INSCOM intelligence units are also involved in several joint force efforts to provide warning intelligence to track adversary actions and changing conditions across the domains and dimensions of the OE in each theater. Simultaneously, intelligence staffs and MI units from corps to maneuver battalions prepare for future operations. (See chapter 7 for more about INSCOM.)

THREATS

2-16. 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 faced by Army forces are, by nature, hybrid. They include individuals, groups of individuals, paramilitary or military forces, criminal elements, nation-states, or national alliances. Generally, a threat can be categorized as an enemy or adversary:

- An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). An enemy is also a combatant under the law of war.
- 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). Adversaries pursue interests that compete with those of the United States and are often called competitors.

Hazards

2-17. While usually not as important as threats, hazards can be a significant part of the OE and can play an important role in the conduct of operations. A *hazard* refers to a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. The threat's use of chemical weapons would be a significant hazard within a unit's AO. The intelligence warfighting function is equipped to provide important intelligence on hazards, as needed, during operations. Access to and collaboration across the intelligence enterprise are especially helpful in conducting intelligence analysis on hazards.

Peer Threats

2-18. Peer threats are adversaries or enemies with capabilities and capacity to oppose U.S. forces across all domains and dimensions of the OE worldwide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power to that of U.S. forces in geographic proximity to a conflict area. Peer threats may also have a cultural affinity to specific regions, providing them relative advantages in the human and information dimensions.

2-19. Peer threats employ strategies that capitalize on their advantages to achieve objectives. When these objectives are at odds with the interests of the United States and its allies, conflict becomes more likely. Peer threats prefer to achieve their goals without directly engaging U.S. forces in combat. They often employ information warfare in combination with conventional and irregular military capabilities to achieve their goals. They exploit friendly sensitivities to world opinions and attempt to exploit the Nation's domestic opinion and sensitivity to friendly casualties. Peer threats believe they have a comparative advantage because of their willingness to endure greater hardships, casualties, and negative public opinion. They also believe their ability to pursue long-term goals is greater than that of the United States.

2-20. Peer threats employ capabilities from and across multiple domains against Army forces, and they seek to exploit vulnerabilities in all strategic contexts. During conflict, peer threats seek to inflict significant damage across multiple domains in a short amount of time. They seek to delay friendly forces long enough to achieve their goals and end hostilities before friendly forces can decisively respond. Peer threats employ many sophisticated and lethal and nonlethal capabilities that create challenges for information collection and

the production of intelligence. These challenges include IADSs; long-range fires; counterreconnaissance; cyberspace and EW operations; space and counterspace operations; and camouflage, concealment, and deception. (See appendix C for more on peer threats.)

THREAT METHODS

2-21. Peer threats use various methods to render U.S. military power irrelevant whenever possible; every intelligence professional should understand these threat methods and how they can apply to future conflicts. The following broad peer threat methods are often used in combination during conventional or irregular conflicts and below the threshold of conflict; FM 3-0 provides more details:

- **Information warfare.** In the context of the threat, *information warfare* refers to a threat's orchestrated use of information activities (such as EW, cyberspace operations, and psychological operations) to achieve objectives. Operating under a different set of ethics and laws than the United States', and under the cloak of anonymity, peer threats conduct information warfare aggressively and continuously to influence populations and decision makers. Peer threats can also use information warfare to create destructive effects during competition below armed conflict and crisis. During armed conflict, peer threats use information warfare in conjunction with other methods to achieve strategic and operational objectives.
- **Systems warfare.** *Systems warfare* refers to the identification and isolation or destruction of critical subsystems or components to degrade or destroy an opponent's overall system. Peer threats view the battlefield, their own instruments of power, and an opponent's instruments of power as a collection of complex, dynamic, and integrated systems composed of subsystems and components. They use systems warfare to attack critical components of a friendly system while protecting their own system.
- **Preclusion.** Peer threats use a variety of actions, activities, and capabilities to preclude a friendly force's ability to shape an OE and mass and sustain combat power. A2 and AD are two strategic and operational approaches to preclusion.
  - *Antiaccess* is action, activity, or capability, usually long-range, designed to prevent an advancing enemy force from entering an operational area (JP 3-0). The employment of A2 capabilities against Army forces begins in CONUS and extends throughout the strategic support area into a theater. Peer threats' A2 means include ballistic missiles, cruise missiles, and space, cyberspace, and information warfare capabilities.
  - *Area denial* is action, activity, or capability, usually short-range, designed to limit an enemy force's freedom of action within an operational area (JP 3-0). Usually, adversaries do not design AD to keep friendly forces out but rather to limit their freedom of action and ability to accomplish their mission in using long-range fires, IADSs, EW, CBRN weapons, man-made obstacles, and conventional ground maneuver forces.
- **Isolation.** *Isolation* refers to the containment of a force so that it cannot accomplish its mission. Peer threats will attempt to isolate U.S. forces in many ways:
  - During competition below armed conflict, peer threats may attempt to isolate friendly forces using disinformation campaigns and the threat of aggression.
  - During crisis, peer threats seek to isolate U.S. forward-positioned forces and prevent their support from the United States or elsewhere in theater.
  - During armed conflict, enemy forces identify isolated friendly forces using a variety of capabilities and rapidly attempt to destroy them through long-range, massed, and precision fires.
- **Sanctuary.** *Sanctuary* refers to the positioning of threat forces beyond the reach of friendly forces. It is a form of protection derived by some combination of political, legal, and physical boundaries that restricts freedom of action by a friendly force commander. Peer threats will use any means necessary, including sanctuary, to protect key capabilities from destruction, particularly by air and missile capabilities. Peer threats will also protect their key interests, whether these interests reside in their homeland or in another country. To create a sanctuary that protects key interests, adversaries employ combinations of both physical and nonphysical means to protect key interests.

EMERGING THREAT CAPABILITIES

2-22. The intelligence enterprise is continuously conducting intelligence collection and analysis on adversary actions, possible intent, and capability developments. Additionally, intelligence analysts watch for trends and the employment of new capabilities and techniques during ongoing conflicts. While the principles and fundamentals of warfare remain relatively unchanged, emerging capabilities—which many of the Nation's adversaries have procured or can procure—may have a disproportionate impact on future conflicts with U.S. and allied forces. Therefore, intelligence collection and analysis are critical in developing countermeasures and contingency plans. Certain Army intelligence units and organizations, primarily INSCOM, the Army Space and Missile Command, and the Army Futures Command, contribute to the Defense Intelligence Agency (DIA) and other DOD and intelligence enterprise organizations in performing these tasks.

2-23. Current and future capability developments—in terms of artificial intelligence, hypersonic weapons, robotics, and fully and semiautonomous weapons system capabilities, among other developments—require continued intelligence collection and analysis. In recent exercises and conflicts, fully and semiautonomous weapons system capabilities and drone swarm technologies have been effectively employed by the Nation's adversaries. The use of semiautonomous weapons systems and drone swarms have occurred during Israel Defense Forces versus Hamas engagements, the 2d Norgorno-Karabakh conflict (2020), the renewed Russian invasion of the Ukraine on 24 February 2022, and subsequent operations. This trend will most likely continue; therefore, the U.S. military must leverage intelligence collection and develop resources to ensure the Nation's adversaries do not capture the strategic advantage.

ARMY STRATEGIC CONTEXTS

2-24. Joint doctrine describes the strategic environment in terms of a competition continuum. Rather than a world either at peace or at war, the competition continuum describes three broad categories of strategic relationships—cooperation, competition below armed conflict, and armed conflict. (See JP 3-0.) Each relationship is defined as between the United States and another strategic actor relative to a specific set of policy aims. Cooperation, competition, and even armed conflict commonly go on simultaneously in different parts of the world.

2-25. Although combatant commands and theater armies campaign across the competition continuum, Army tactical formations typically conduct operations within a context dominated by one strategic relationship at a time. Therefore, Army doctrine describes the strategic situation through three contexts in which Army forces conduct operations: competition below armed conflict, crisis, and armed conflict. Figure 2-2 illustrates the Army strategic contexts and the range of military operations.

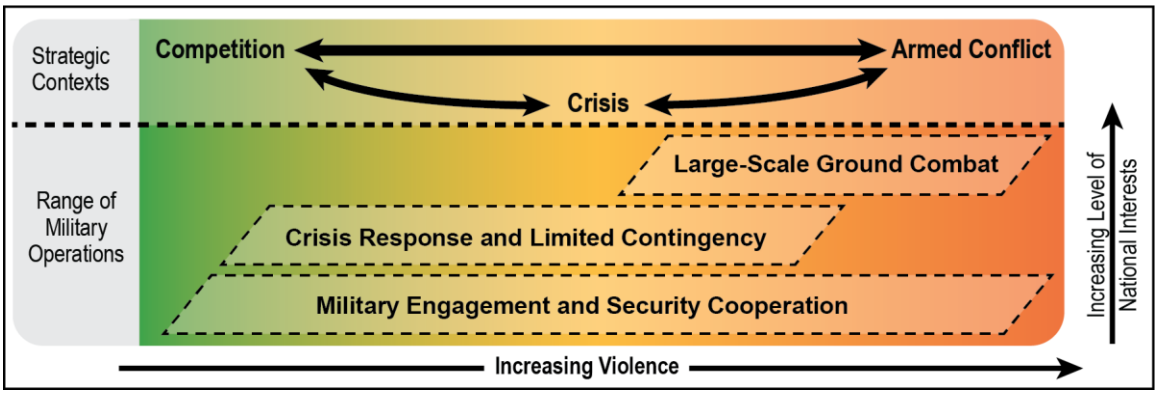


Figure 2-2. Army strategic contexts and operational categories

Note. This publication often uses *competition* to mean *competition below armed conflict*.

2-26. The Army strategic contexts and the range of military operations, which along with consolidating gains, significantly affect intelligence supporting activities. *Consolidate gains* are activities to make enduring any temporary operational success and to set the conditions for a sustainable environment, allowing for a transition of control to other legitimate authorities (ADP 3-0). Army commanders must exploit successful operations by continuously consolidating gains during competition, crisis, and armed conflict. Chapter 4 details intelligence support to each strategic context and the consolidating gains for each context.

UNDERSTANDING AN OPERATIONAL ENVIRONMENT

2-27. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). For Army forces, an OE includes portions of the five domains (land, maritime, air, space, and cyberspace) understood through three dimensions (human, information, and physical). The land, maritime, air, and space domains are defined by their physical characteristics. Cyberspace, a man-made network of networks, transits and connects the other domains as represented by the dots shown in figure 2-3.

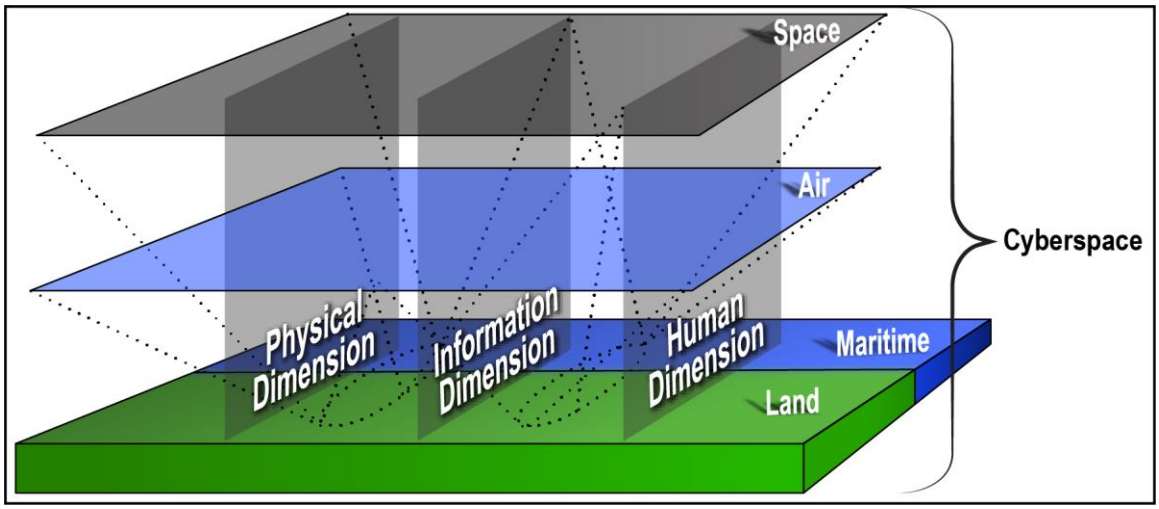


Figure 2-3. Domains and dimensions of an operational environment

Note. Joint doctrine describes the components of an OE as the physical areas of the land, maritime, air, and space domains; the information environment (which includes cyberspace); the EMS; and other factors. (See JP 2-0 and JP 5-0 for doctrine on describing and analyzing an OE from a joint perspective.)

2-28. The OE model assists in accounting for the totality of factors, specific circumstances, and conditions that impact the conduct of operations. This understanding enables commanders and staffs to better identify problems, anticipate potential outcomes, and understand the results of various friendly, enemy, adversary, and neutral actions, including the effects these actions have on achieving the military end state. A description of an OE includes all factors that the commander and staff must capture and understand in order to inform the conduct of operations.

2-29. Knowledge of the OE is the precursor to effective action. Obtaining knowledge about an OE requires aggressive and continuous intelligence operations, surveillance, reconnaissance, and security operations to acquire information. Information collected from multiple sources and analyzed becomes intelligence that answers commanders' intelligence requirements. Using all available relevant information to determine how the OE affects operations is essential to understanding which COAs are the most feasible, suitable, and acceptable. Throughout the course of operations, commanders and staffs rely on an integrated information collection effort to develop an accurate picture of their OE. (See chapter 6 for more on collection.)

2-30. An OE is the totality of factors that affect what occurs in an assigned area. These factors include actors, events, or actions that occur outside the assigned area. How the many entities behave and interact with each other is difficult to discern. No two OEs are the same, and all of them continually change. Changes result, in part, from opposing forces and actors interacting, learning, and adapting.

2-31. The complex and dynamic nature of an OE makes determining the relationship between cause and effect challenging, and they contribute to the uncertain nature of war and human competition. This requires commanders, supported by their staffs, to develop and maintain the best possible understanding of their OE. Several tools and processes assist commanders and staffs in understanding their OE. They include—

- Domains.
- Dimensions.
- Operational and mission variables.
- Running estimates (described in ADP 5-0).
- ADM (described in ATP 5-0.1).
- The MDMP (described in ADP 5-0).
- Pre-mission analysis of the OE (described in chapter 5).
- IPOE (described in chapter 5).
- Sustainment preparation of the OE (described in FM 4-0).

DOMAINS

2-32. Within the context of an OE, a *domain* is a physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills (FM 3-0). Understanding the strengths and dependencies of joint capabilities in each domain is fundamental to a multidomain, combined arms approach to operations. Although each military Service and branch trains and educates its leaders to be experts about operations in a primary domain, each Service has some capability in each of the domains, and each Service develops a shared understanding of how to integrate capabilities from different domains. (See FM 3-0 for doctrine on the domains.)

2-33. Although most domains align with the skills developed in a particular Service, no Service focuses entirely on or exerts total control of that single domain during operations. Joint commanders assign responsibilities and task-organize based on mission requirements. However, the domains present very different conditions of warfare and require the specialized warfighting skills developed by the different Services and subcomponents within each of the Services. The joint force and all Services must collaborate and synchronize to thoroughly understand each domain. When the threat takes actions to significantly counter collection in a particular domain and friendly forces have an incomplete understanding within that domain it challenges operations. In these situations, the intelligence warfighting function must identify all information gaps and depend on collection in the other domains to maintain as complete an understanding of the OE as possible. Army leaders do not need to understand all the technical components of the other domains, but they do need to understand the complementary and reinforcing ways in which they can request and employ joint capabilities and methods to support operations on land. The following occurs across all domains:

- The Army provides forces and capabilities from all domains to the joint force.
- Army forces employ joint capabilities from all domains to complement and reinforce their own capabilities.
- Understanding domain interdependencies assists leaders in better mitigating friendly vulnerabilities while creating and exploiting relative advantages.
- In an environment where the enemy can contest every domain, successful operations require continuous joint integration down to the lowest tactical echelons.
- The intelligence warfighting function must assist commanders and staffs in understanding the threat and other significant aspects of the OE and conducting/leveraging information collection across all domains.

2-34. Table 2-2 lists several operational aspects and intelligence, threat, and other OE considerations associated with the land domain.

Table 2-2. Land domain operational aspects and intelligence and other considerations

Land domain		
The ***land domain*** is the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals (JP 3-31). Variations in climate and terrain and the diversity of populations have a far greater impact on operations in the land domain than in any other domain. The land domain's most distinguishing characteristic is the human dimension. Terrain also significantly impacts the nature of land combat. Land-based domain capabilities can use or alter terrain and operate in most weather conditions and among populations.		
Operational aspects	***Army intelligence considerations***	***Threat and other operational environment considerations***
• Possibility of high lethality, operating in complex terrain, and a CBRNE-degraded environment. • Significantly impacted by long-range precision fires. • Battles and engagements depend on Army forces closing with enemy forces and prevailing in close combat. • Land capabilities extend operational reach and provide options for enabling joint operations. • Joint interdependence: ▪ Operational mobility. ▪ Joint fires. ▪ Other key enabling capabilities. • Army support to other Services, CCMDs, and unified action partners: ▪ Ground-based indirect fires. ▪ Air and missile defense. ▪ EW. ▪ Cyberspace operations. ▪ Communications. ▪ Intelligence. ▪ Rotary-wing aircraft. ▪ Logistics. ▪ Engineering. ▪ Security operations.	• Army intelligence must— ▪ Understand and visualize the interdependencies of the land domain on the other domains and characterize the threat's capabilities and vulnerabilities in each domain relative to operations. ▪ Leverage the intelligence architecture, including intelligence from the intelligence community to get a different perspective and greater insight. ▪ Collaborate, participate in exercises, and build intelligence relationships with the other Services, CCMDs, and unified action partners. • Support other Services, CCMDs, and unified action partners— ▪ In understanding the land domain. ▪ As tasked, by providing significant capabilities across all-source intelligence, the intelligence disciplines, and the complementary capabilities. • Provide Army forces— ▪ An extensive all-source intelligence foundation at and across echelons. ▪ Significant capabilities across the intelligence disciplines and complementary capabilities. ▪ Effective and flexible intelligence support. • The human and information dimensions make the land domain the most complicated domain and the most challenging for the intelligence warfighting function.	**Threat capability examples:** • Morale, doctrine, and effectiveness. • Leaders and their biographic information. • C2. • Long-range fires. • Medium- and short-range fires. • CBRNE. • Information warfare, including EW and cyberspace. • Integrated air defense systems and other A2 and AD capabilities. • Tank and armored. • Infantry and small arms. • Engineering. • Military police. • Logistics and maintenance. **Other operational environment examples:** • Government officials with biographies. • NGOs, PVOs. • Political with biographies. • Economic, commercial, and industrial studies. • Communications infrastructure. • Energy infrastructure. • City infrastructures. • Terrain. • Weather trends, forecasts, and effects. • Weather effects on terrain. • History. • Culture and customs.

A2	antiaccess	EW	electromagnetic warfare
AD	area denial	JP	joint publication
C2	command and control	NGO	nongovernmental organization
CBRNE	chemical, biological, radiological, nuclear, and explosives	PVO	private voluntary organization
CCMD	combatant command		

2-35. Table 2-3 lists several operational aspects and intelligence, threat, and other OE considerations associated with the maritime domain.

Table 2-3. Maritime domain operational aspects and intelligence and other considerations

Maritime domain		
The ***maritime domain*** is the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals (JP 3-32). The maritime domain overlaps with the land domain in the seaward segment of the littoral. Maritime capability may be viewed as global, regional, territorial, coastal, and self-defense forces. Most maritime nations also maintain air forces capable of conducting operations over the maritime domain. This air capability, combined with land-based long-range fires, greatly impacts operations in the maritime domain.		
Operational aspects	***Army intelligence considerations***	***Threat and other operational environment considerations***
• Move strategic fires capabilities, conceal strategic capabilities below the ocean surface, transport personnel and equipment over vast distances, and sustain maritime operations. • Navy functions provide a unique advantage for the joint force: deterrence, operational access, sea control, power projection, and maritime security. • Maritime force joint interdependence: ▪ Protect maritime capabilities and ports. ▪ Secure geographic choke points. ▪ Mitigate long timelines for maritime movement. ▪ Compensate for limited number of platforms. ▪ Mitigate lost ships and platforms. • Army forces rely on maritime forces— ▪ For deployment and sustainment. ▪ Fires and AMD to complement and reinforce land-based systems. • Army forces assist maritime forces— ▪ Sea control. ▪ In controlling littorals by projecting power. ▪ Local and regional maritime superiority through long-range fires, attack aviation, AMD, and cyberspace capabilities. • For intratheater operations, Army watercraft provide a significant capability to move maneuver formations and sustain operations.	• Army intelligence must— ▪ Leverage the intelligence architecture, including intelligence from the intelligence community on the maritime domain. ▪ Collaborate, participate in exercises, and build intelligence relationships with Navy forces, CCMDs, and unified action partners. ▪ Build an understanding of and integrate with unique Navy capabilities such as shipboard signals intelligence and EW and naval aviation. • Support other Services, CCMDs, and unified action partners: ▪ Conduct detailed assessments on key maritime choke points, as appropriate. ▪ Support joint target development on certain threat maritime capabilities, as appropriate. ▪ Support Navy identification of threats to maritime capabilities, as appropriate. ▪ Support port protection activities. • Provide Army forces— ▪ Intelligence on littorals. ▪ Intelligence support to Army watercraft operations. ▪ Effective and flexible intelligence on the maritime domain when required for the mission.	**Threat capability examples:** • Nuclear weapons. • Cruise missiles. • Naval C2. • Naval aviation. • Ship-to-shore fires. • Naval infantry/Marines. • Naval reconnaissance. • Underwater detonation and sabotage capabilities. • Naval air defense systems. • Naval EW and cyberspace capabilities. • Military port and maritime basing agreements. **Other operational environment examples:** • Commercial sea traffic. • Port infrastructure and conditions. • NGOs, PVOs. • Underwater earthquakes and tsunamis. • Current and forecasted oceanographic effects on friendly and threat maritime capabilities. • Littoral studies. • Fishing and other sea-based industries. • Arctic strategic and political considerations.

AMD	air and missile defense	JP	joint publication
C2	command and control	NGO	nongovernmental organization
CCMD	combatant command	PVO	private voluntary organization
EW	electromagnetic warfare		

2-36. Table 2-4 lists several operational aspects and intelligence, threat, and other OE considerations associated with the air domain.

Table 2-4. Air domain operational aspects and intelligence and other considerations

Air domain		
The ***air domain*** is the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible (JP 3-30). The speed, range, and payloads of aircraft, rockets, missiles, and hypersonic glide vehicles in the air domain directly and significantly affect operations on land and sea. Likewise, advances in AMD, EW, directed energy, and cyberspace capabilities increasingly contest freedom of maneuver in the air.		
Operational aspects	***Army intelligence considerations***	***Threat and other operational environment considerations***
• Control of the air and land are often interdependent requirements for successful campaigns and operations. • Allows the attack of strategically valuable targets at long ranges. However, requires land forces to secure airfields and other infrastructure. • Control of the air can vary over time and geography from no control to parity, local superiority, and air supremacy. • While the Army, other Services, and coalitions/host nations have certain air capabilities, Army forces depend on USAF completely or in some instances for— ▪ ISR. ▪ Strategic attack. ▪ Close air support and interdiction. ▪ Personnel recovery (in some instances). ▪ Sustainment and mobility. • Air domain limitations can include weather, enemy collection countermeasures, and proximity of airfields. • Army aviation provides— ▪ ISR. ▪ Fires. ▪ Communications. ▪ Movement. • Commanders establish control measures to enable Army aviation to operate unimpeded. • Army rotary-wing aviation uses terrain to protect it from enemy detection.	• Army intelligence must— ▪ Leverage the intelligence architecture, including intelligence from the intelligence community on the air domain. ▪ Collaborate, participate in exercises, and build intelligence relationships with USAF, Naval, and Marine Corps aviation units; CCMDs; unified action partners. ▪ Understand Army, joint, and other Service aerial ISR and EW capabilities. ▪ Build an understanding of and integrate with unique USAF capabilities such as Rivet Joint and Compass Call. • Support other Services, CCMDs, and unified action partners: ▪ Conduct detailed assessments on likely threat operations against key airfields to support contingency planning, as appropriate. ▪ Support air domain target development on certain threat capabilities, as appropriate. ▪ Support USAF identification of threats to key USAF capabilities, as appropriate. ▪ Support airfield protection activities. ▪ Support SEAD and joint SEAD. • Provide Army forces— ▪ Current and forecasted weather effects through the staff weather officer, staff weather team, or other means. ▪ Effective and flexible support to Army aviation operations. ▪ Effective and flexible intelligence on the air domain across all echelons for every mission. • Conduct signals intelligence surveys.	**Threat capability examples:** • Nuclear weapons. • Theater ballistic missiles. • Cruise missiles. • Air C2 (ground-based). • Airfields and supporting facilities and logistics. • Aircraft specifications and capabilities. • Aerial C2 systems. • Radar systems, capabilities, limitations, and vulnerabilities. • Air ISR. • Close air support tactics, including air controller capabilities. • Air interdiction tactics. • Runway cratering munitions. • Rotary-wing attack, air assault, and air movement capabilities. • UAS and drone tactics and capabilities. • Air and ground EW capabilities. • Military airfield use agreements. **Other operational environment examples:** • Weather trends and forecasts. • Commercial air traffic. • Commercial airfields and infrastructure. • Overflight rights. • Emerging aircraft technology.

AMD	air and missile defense	JP	joint publication
C2	command and control	SEAD	suppression of enemy air defenses
CCMD	combatant command	UAS	unmanned aircraft system
EW	electromagnetic warfare	USAF	United States Air Force
ISR	intelligence, surveillance, and reconnaissance		

2-37. Table 2-5 lists several operational aspects and intelligence, threat, and other OE considerations associated with the space domain.

Table 2-5. Space domain operational aspects and intelligence and other considerations

Space domain		
The ***space domain*** is the area above the altitude where atmospheric effects on airborne objects become negligible (FM 3-0). Like land, maritime, and air domains, space is a physical domain where military, civil, and commercial activities are conducted. The U.S. Space Command is responsible for planning and executing operations, activities, and missions in the space domain. Activities in the space domain enable freedom of action in all other domains, and operations in the other domains can create effects in and through space. (See FM 3-14.)		
Operational aspects	***Army intelligence considerations***	***Threat and other operational environment considerations***
• Commanders and staffs must understand how to employ or coordinate for Army or joint space and counterspace control assets to deny, degrade, disrupt, or deceive adversary space-based and counterspace-based capabilities to achieve relative advantages during operations. • Proliferation of advanced space technology provides access to space-enabled technologies to most of the Nation's threats. • Some adversaries have their own space capabilities, while commercial capabilities allow universal access to space capabilities with military applications. • Specific capabilities provide— ▪ Information collection. ▪ Early warning. ▪ Target acquisition. ▪ EW. ▪ Communications. ▪ Positioning, navigation, and timing. ▪ Environmental monitoring. • Space and counterspace operations depend on cyberspace and the electromagnetic spectrum; space capabilities provide critical portions of cyberspace bandwidth. • Commanders and staffs cannot assume unconstrained use of space-based capabilities, including communications. • Army forces must be prepared to operate under the conditions of a denied, degraded, and disrupted space domain.	• Army intelligence must— ▪ Leverage the intelligence architecture, including intelligence from the intelligence community on the space domain. ▪ Collaborate, participate in exercises, and build intelligence relationships with the Army Space and Missile Command, CCMDs, and unified action partners. ▪ Build an understanding of and integrate with space and counterspace capabilities. • Support other Services, CCMDs, and unified action partners in conducting detailed assessments on threat space-ground stations, communications, and infrastructure, as appropriate. • Provide Army forces, in conjunction with the space operations officer and staff weather officer, considerations for space weather and space weather effects on intelligence activities, information collection, and support to operations security.	**Threat capability examples:** • Space intelligence collection. • Space C2 and communications. • Ground stations, space control, and infrastructure. • Disruption of friendly space capabilities. **Other operational environment examples:** • Dual commercial- and military-space activities. • Space weather trends and forecasts. • Commercial space activities. • Commercial space infrastructure. • Emerging space technology.

C2	command and control	EW	electromagnetic warfare
CCMD	combatant command	FM	field manual

2-38. Table 2-6 lists several operational aspects and intelligence, threat, and other OE considerations associated with the cyberspace domain.

Table 2-6. Cyberspace domain operational aspects and intelligence and other considerations

Cyberspace domain		
The ***cyberspace domain*** is the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum (FM 3-0). Cyberspace is not constrained by geography; it is an extensive and complex global network of wired and wireless links connecting nodes that reach across every domain. Friendly, enemy, adversary, and host-nation networks, communications systems, computers, cellular phone systems, social media, and technical infrastructure are all part of cyberspace. The cyberspace domain is congested, contested, and critical to successful operations. (See FM 3-12.)		
Operational aspects	***Army intelligence considerations***	***Threat and other OE considerations***
• Space domain depends on the land, maritime, air, and space domains. • CO use links and nodes located in these domains and perform functions to gain access and create effects, first in cyberspace and then in other domains. • Space operations depend on cyberspace; space capabilities provide critical portions of cyberspace bandwidth. • Inherently joint, interorganizational, multinational, and often a shared resource with signal and intelligence units and organizations. • Army forces conduct CO and supporting activities as part of both Army and joint operations. • Commanders and staffs use cyberspace and EW capabilities to gain situational awareness and understanding of the enemy. • Cyberspace and EW capabilities enable decision making, protect friendly information, and inform and influence audiences. • To achieve an information advantage, the commander and staff must integrate EW activities and CO: ▪ Ensures command and control and maintains operations security. ▪ Slows or degrades enemy decision making and targeting.	• Army intelligence must— ▪ Leverage the intelligence architecture, including intelligence from the intelligence and cyberspace communities about the cyberspace domain. ▪ Collaborate, participate in exercises, and build intelligence relationships with U.S. Cyber Command, other Services, CCMDs, and UAPs. ▪ Understand USCYBERCOM, Army, joint, and other Service cyberspace and EW capabilities. ▪ Build an understanding of and integrate with unique Army cyberspace capabilities and organizations such as ARCYBER, ARCYBER G-2, and the Cyber Military Intelligence Group. ▪ Build an electromagnetic order of battle in conjunction with the cyberspace community. • Support other Services, CCMDs, and UAPs: ▪ Support all measures to counter threat information warfare, misinformation, and disinformation in the cyberspace domain, as authorized. ▪ Support cyberspace domain target development on certain threat capabilities, as appropriate. ▪ Support the joint identification of threats to key friendly cyberspace capabilities, as appropriate. • Provide Army forces— ▪ Coordinated electromagnetic spectrum actions, in terms of signals intelligence. ▪ Support to EW activities. ▪ Support to CO and cybersecurity. • Team with ARCYBER to exploit cyberspace capabilities as part of intelligence support and information collection. • Team with Army EW units to exploit EW capabilities as a part of intelligence support and information collection. • Conduct signals intelligence surveys. ***Note.*** Challenges in terms of authorities, coordination, and deconfliction between Title 10 and Title 50 statute operations can occur. (See paragraphs B-71 through B-74.)	**Threat capability examples:** • Information warfare intent and objectives in the cyberspace domain. (This can have global effects.) • Offensive CO against friendly forces. • Defensive cyberspace capabilities. • Cyberspace infrastructure with specifications and nodes. • EW capabilities, to include meaconing, jamming, and decoys. • Disruption of friendly space capabilities. **Other OE examples:** • Cyberspace (nonground) communications, including cellular coverage. • Cyberspace providers and ground infrastructure, including power generation and networks. • Computer, information technology, and associated commercial advancements. • Other associated emerging technologies such as nano computers and quantum computing.

ARCYBER	United States Army Cyber Command	FM	field manual
CCMD	combatant command	OE	operational environment
CO	cyberspace operations	UAP	unified action partner
G-2	assistant chief of staff, intelligence	USCYBERCOM	United States Cyber Command
EW	electromagnetic warfare		

DIMENSIONS

2-39. Understanding the human, information, and physical dimensions of each domain assists commanders and staffs in assessing and anticipating the impacts of their operations. Operations reflect the reality that war is an act of force (in the physical dimension) to compel (in the information dimension) the decision making and behavior of enemy forces (in the human dimension). Actions in one dimension influence factors in the other dimensions. Intelligence analysts can categorize information and intelligence related to the human, information, and physical dimensions across all domains by the following elements for each threat entity: intent, capability, access, resources, and expertise. Understanding this interrelationship enables decision making about how to create and exploit advantages in one dimension and achieve objectives in the others without causing undesirable consequences. (See figure 2-4.) (See FM 3-0 for doctrine on the dimensions.)

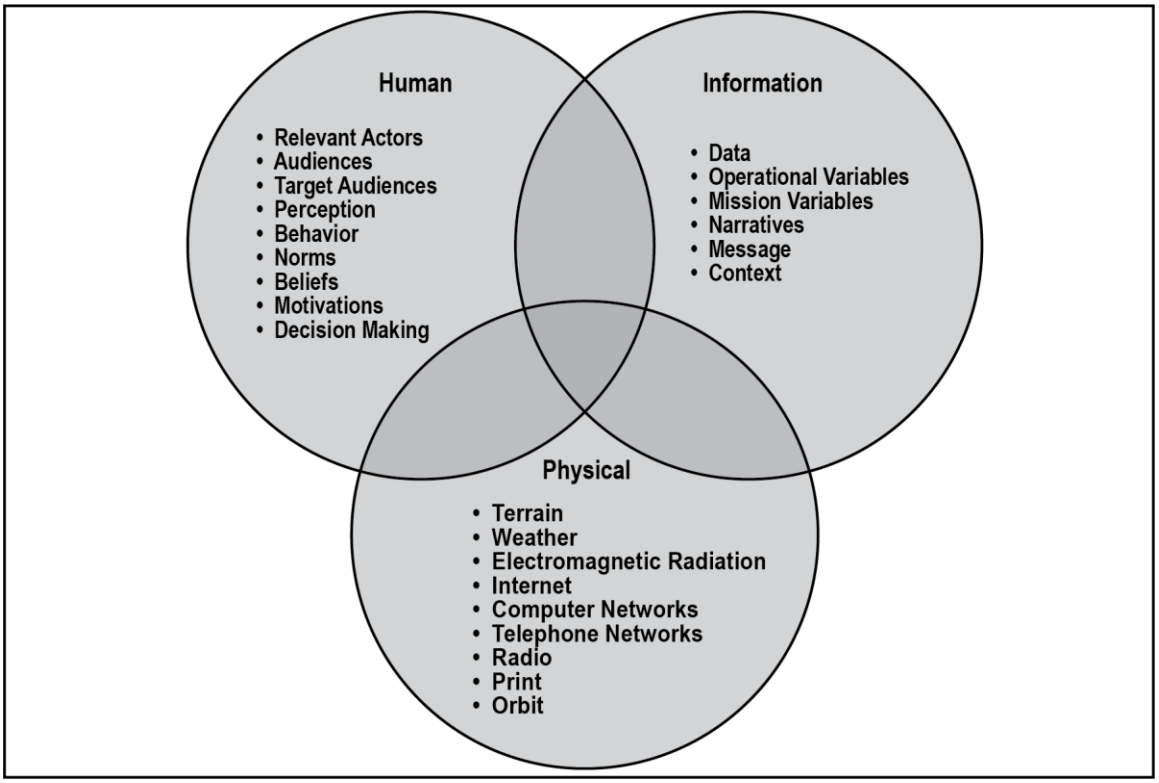


Figure 2-4. Interrelationships between the human, information, and physical dimensions

2-40. Table 2-7 list several operational and intelligence considerations associated with the human dimension.

Table 2-7. Operational and intelligence considerations for the human dimension

The ***human dimension*** encompasses people and the interaction between individuals and groups, how they understand information and events, make decisions, generate will, and act within an operational environment (FM 3-0).	
Operational considerations (not all-inclusive)	***Intelligence considerations (not all-inclusive)***
Discussion: • The will to fight emerges from the complex interrelationship of culture, emotion, and behavior. • Military objectives are achieved by influencing that interrelationship. • Influencing that interrelationship occurs by affecting attitudes, beliefs, motivations, and perceptions. • The commander and staff identify relevant actors and predict their behaviors. • By understanding the operational environment, including relevant actors, the commander and staff attempt to influence relevant actors' behaviors, decision making, and will through physical and informational means. **Human advantage:** • A human advantage occurs when a force holds the initiative in terms of training, morale, perception, and will. • A human advantage enables friendly morale and will, degrades enemy morale and will, and influences popular support. • Examples include— ▪ Soldier competence. ▪ The force's health and physical fitness. ▪ A cultural affinity and good relations with the local population.	• Impossibility of isolating the human dimension from the information and physical dimensions. • Activities and effects within the human dimension. They are challenging, but not impossible, to understand, collect against, make predictions about, and support operational planning. Human thinking, will, intent, and behavior are complex. • Intelligence disciplines and complementary capabilities conducting information collection in and against the human dimension. For example, PAI research, OSINT, HUMINT, and identity activities can make important contributions to understanding important aspects of the human dimension; however, Army forces ultimately use an all-source approach. • IWFTs, including warning intelligence, intelligence preparation of the operational environment, situation development, and intelligence support to targeting. They assist in accounting for aspects within the human dimension. • Center of gravity analysis, functional analysis using critical factors, the outside-in thinking analytic technique, and thorough analysis of relevant actors. They are critical in assisting intelligence analysts in understanding the human dimension. • Operational variables, civil considerations (within the mission variables), and a crosswalk of both operational and mission variables. They assist intelligence analysts in considering the human dimension.
FM field manual HUMINT human intelligence IWFT intelligence warfighting function task	OSINT open-source intelligence PAI publicly available information

2-41. Table 2-8 lists several operational and intelligence considerations associated with physical dimension.

Table 2-8. Operational and intelligence considerations for the physical dimension

The ***physical dimension*** is the material characteristics and capabilities, both natural and manufactured, within an operational environment (FM 3-0).	
Operational considerations (not all-inclusive)	***Intelligence considerations (not all-inclusive)***
Discussion: • War is conducted with physical mechanisms. • Each domain is inherently physical. • The physical dimension includes space orbits, terrain, weather, military formations, electromagnetic radiation, and weapons systems and their ranges. • Physical activities create effects in the human and information dimensions. • The electromagnetic spectrum is one of the physical mechanisms that occurs across all domains. **Physical advantage:** • A physical advantage occurs when a force holds the initiative in terms of the number and combinations of capabilities, quality of capabilities, or geographic positioning. • Finding multiple physical advantages is typically the goal of most tactical operations: occupation of key terrain, physical isolation of the enemy, and destruction of enemy units. • A physical advantage results in superior combat power. • A physical advantage creates human and information advantages.	• Impossibility of isolating the physical dimension from the human and information dimensions. • Existence of most of the threat and other operational environment considerations in table 2-2 on page 2-10 within the physical dimension. • Activities and effects within the physical dimension. They are easier, although not easy, to understand, collect against, and predict compared to threat and other relevant actor aspects of the human and information dimensions. • Proficiency of intelligence disciplines and complementary capabilities in conducting information collection in the physical dimension. • IWFTs, including warning intelligence, IPOE, situation development, and intelligence support to targeting. They must consider the physical dimension. • A relatively complete list of threat and other operational environment aspects. This list within the physical dimension is quite extensive.
FM field manual IPOE intelligence preparation of the operational environment	IWFT intelligence warfighting function task

2-42. Table 2-9 list several operational and intelligence considerations associated with the information dimension.

Table 2-9. Operational and intelligence considerations for the information dimension

The ***information dimension*** is the content and data that individuals, groups, and information systems communicate and exchange, as well as the analytics and technical processes used to exchange information within an operational environment (FM 3-0).	
Operational considerations (not all-inclusive)	***Intelligence considerations (not all-inclusive)***
Discussion: • Connects humans to the physical world. Information transits through all domains. • Information—true, false, or in between—is used by friendly, enemy, adversary, and neutral actors to influence perceptions, decision making, and behaviors. • The effective employment of information depends on the audience, message, and method of delivery. • Social media can enable the swift mobilization of people and resources around ideas and causes. • Disinformation can significantly and negatively affect emotions, perceptions, decision making, and behaviors. • Information enables decision making and combat power. • The information dimension is key to seizing, retaining, and exploiting the initiative and consolidating gains. **Information advantage:** • An information advantage is the operational benefit derived when— ▪ Friendly forces understand and exploit informational considerations to achieve information objectives. ▪ Denying the threat's ability to achieve information objectives. • Army forces employ human and physical aspects to gain information advantages. • Most types of information advantage result from intrinsic human and physical aspects of Army operations. • An information advantage can occur in terms of— ▪ Collecting more and better information. ▪ Using relevant information more effectively. ▪ Effective communications and protecting information. ▪ Disrupting the threat's communications. ▪ Conducting deception. ▪ Influencing relevant actors' behavior.	• Impossibility of isolating the information dimension from the human and physical dimensions. • Activities and effects within the information dimension. They are challenging, but not impossible, to understand, collect against, make predictions about, create intelligence products, conduct intelligence assessments, and support operational planning. • Intelligence disciplines and complementary capabilities conducting information collection in and against the information dimension. For example, PAI research, OSINT, and identity activities can make important contributions to the intelligence effort; however, Army forces ultimately use an all-source approach. • IWFTs, including warning intelligence, IPOE, situation development, and intelligence support to targeting. They must account for aspects within the information dimension. • Support to protecting information and disrupting threat communications. This is not that difficult. • Support to deception. This is more difficult, while support to influencing behaviors and countering misinformation and disinformation are very difficult. • Functional analysis with critical factors, the operational variables, civil considerations (within the mission variables), and a crosswalk of the operational and mission variables. They assist intelligence analysts in considering the information dimension. • Content, data, and processes that individuals, groups, and information systems use to communicate; the technical processes and analytics used to exchange information; and how relevant actors and populations communicate. Intelligence analysts should highlight these. • Importance of analyzing relevant actors, information processes, communications means and nodes, and computer hardware and software—among other aspects.
FM field manual IPOE intelligence preparation of the operational environment IWFT intelligence warfighting function task	OSINT open-source intelligence PAI publicly available information

OPERATIONAL AND MISSION VARIABLES

2-43. The operational and mission variables are tools that assist commanders and staffs in refining their understanding of the domains and dimensions of an OE. Commanders and staffs analyze and describe an OE in terms of eight interrelated operational variables: political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT). The operational variables assist leaders in understanding the land domain and its interrelationships with information, relevant actors, and capabilities in the other domains.

2-44. Commanders analyze information categorized by the operational variables in the context of the missions they are assigned. They use the mission variables, in combination with the operational variables, to refine their understanding of the situation and visualize, describe, and direct operations. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations—each of which has *informational considerations*—those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information (FM 3-0). The mission variables are represented as METT-TC (I). (See FM 5-0 for doctrine on the operational and mission variables.)

Note. METT-TC (I) represents the mission variables that leaders use to analyze and understand a situation in relationship to the unit's mission. The first six variables are not new. However, the pervasiveness of information and its applicability in different military contexts requires leaders to continuously assess various aspects of information during operations. Because of this, **I** has been added to the METT-TC mnemonic. Informational considerations, expressed as a parenthetical variable, is an important component of each variable of METT-TC that leaders must understand in developing an understanding of a situation and the relevant portions of the OE. (See FM 3-0.)

INTELLIGENCE AND UNDERSTANDING AN OPERATIONAL ENVIRONMENT

2-45. Understanding the domains and dimensions of an OE requires aggressive information collection and thorough intelligence analysis across echelons—from the joint level, where there are sophisticated capabilities, to the lowest tactical echelon. However, analyzing and understanding the domains and dimensions of an OE are not an end in and of themselves; information from the domains and dimensions must also feed the operational and mission variables. This ultimately results in the commander and staff reaching adequate situational understanding and visualizing, describing, and directing operations. Figure 2-5 concisely illustrates how to understand an OE and continuously focus and refine information from the domains and dimensions to support operations.

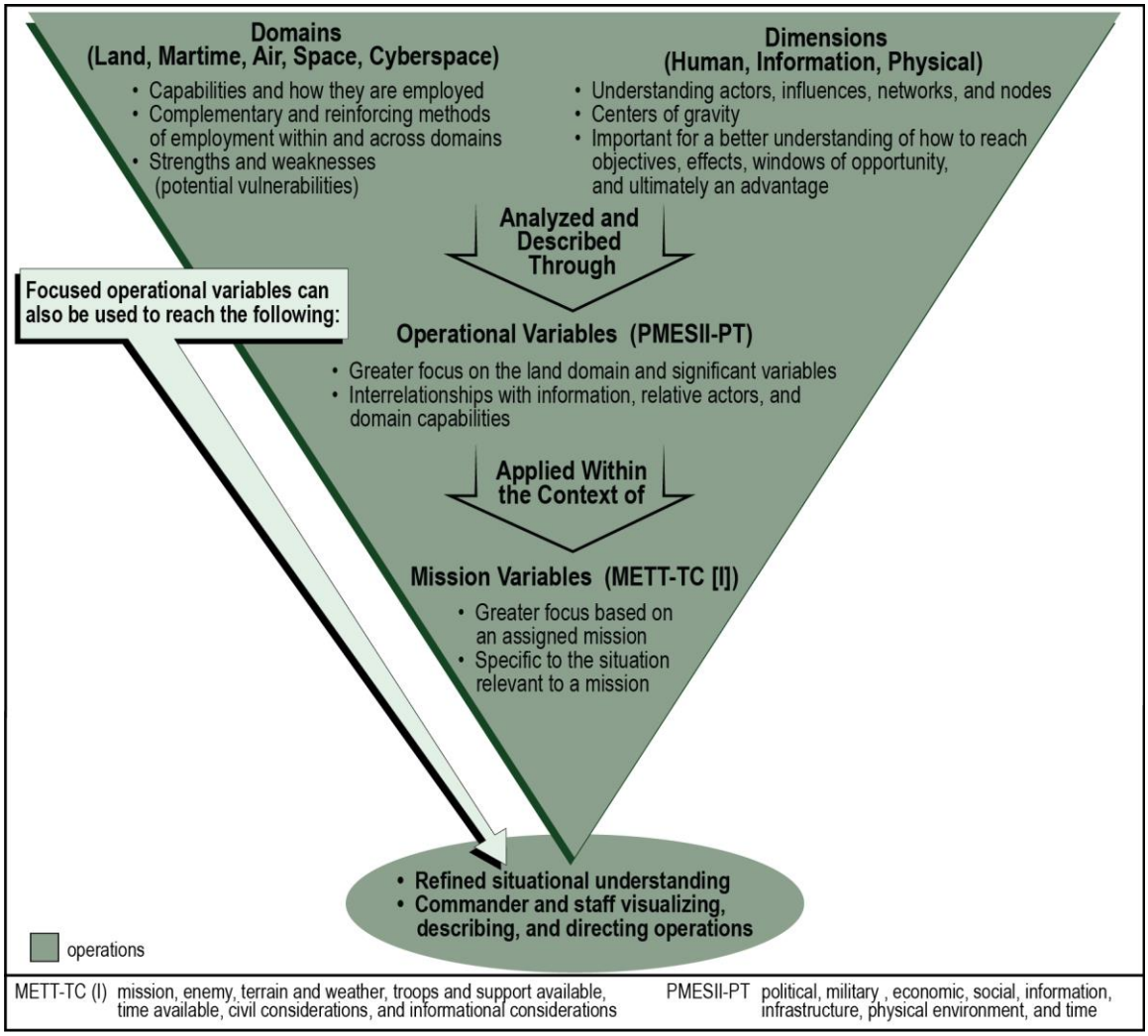


Figure 2-5. Understanding an operational environment

2-46. Understanding an OE is complex. The intelligence staff and intelligence analysis contribute to analyzing and describing the relevant aspects of the domains and dimensions through the operational and mission variables specific to a unit's mission. Through participation with the entire staff, the intelligence staff leads and/or performs an important role in—

- Understanding the domains and dimensions in time and space and identifying OE changes, including their causes and impacts.
- Identifying how human behaviors and beliefs and information impact the physical dimension of operations.
- Identifying one or more centers of gravity, depending on the echelon and situation.
- Functional analysis.
- Developing adversary and enemy threat models and identifying strengths and vulnerabilities across all domains.
- Identifying possible friendly and enemy windows of opportunity across the domains and dimensions to create effects and possibly reach an advantage. ***Note.*** The intelligence staff must view the OE from friendly and enemy perspectives and any significant neutral and other actors.
- Determining how, when, and where to leverage friendly capabilities across the domains to find and exploit friendly windows of opportunity.
- Assisting the commander to visualize operations and impacts on the OE.
- Framing and planning COAs and decisions during the MDMP.

2-47. The intelligence staff, primarily through continuous intelligence analysis and IPOE, assists the commander and staff in focusing on and understanding the relevant aspects of an OE and determining in which domains those relevant aspects reside. This allows the commander and staff to discount irrelevant aspects of the OE. Identifying significant aspects of the OE (a substep to step 1 of IPOE) and describing environmental effects on operations (step 2 of IPOE) are crucial in ensuring the operational and mission variables are properly considered during the MDMP. The following also support the commander and staff's understanding of an OE:

- Understanding domain capabilities and how they are employed and understanding the various aspects of the dimensions are critical in synchronizing intelligence activities, to include modifying the intelligence architecture.
- In turn, intelligence synchronization supports effective collection management and intelligence collection, which result in more focused and relevant information within the operational and mission variables.
- Leveraging specialized and detailed intelligence from the intelligence enterprise is crucial to the effort.
- Collaborating with each staff section and across the intelligence enterprise provides additional depth to understanding each domain and its interdependencies.
- Accessing joint target system analysis (TSA) and joint target development products can be useful when trying to understand domain capabilities and interdependencies.
- Army forces, especially when preparing for armed conflict during competition, must conduct Army analysis of threat systems through a federated target production effort.
- The following IWFTs also support understanding an OE (see appendix B):
  - Conduct pre-mission analysis of the OE.
  - Provide warnings.
  - Provide intelligence support to targeting (including target value analysis).
  - Perform situation development.

2-48. Figure 2-6 illustrates several ways that intelligence supports understanding an OE.

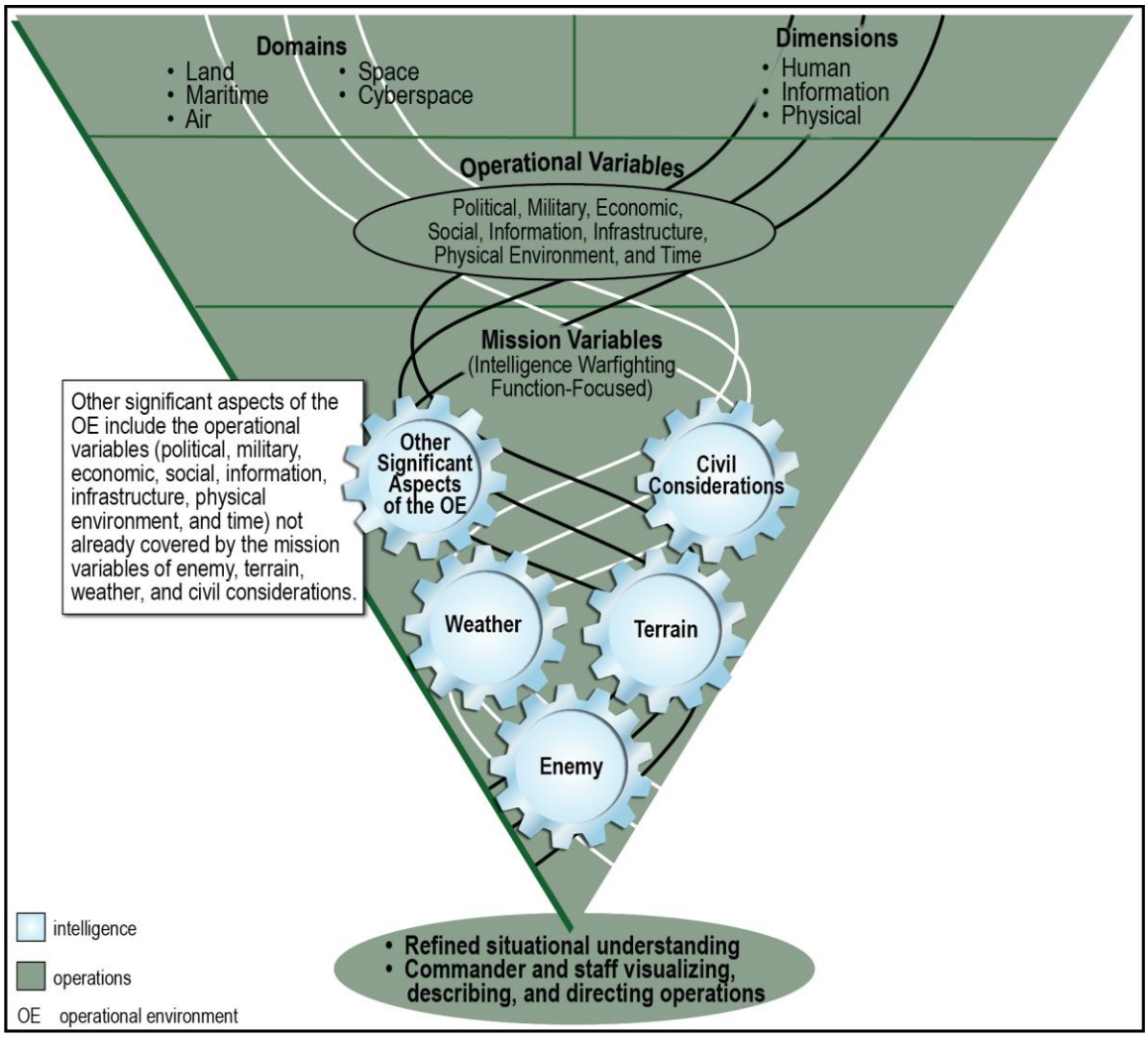


Figure 2-6. How intelligence supports understanding an operational environment

SECTION III – FUNDAMENTALS OF OPERATIONS

2-49. Understanding operational doctrine starts with understanding the higher-level doctrinal concepts in FM 3-0. Intelligence professionals must understand these fundamental concepts as well as how the intelligence warfighting function nests within them. In this manner, intelligence professionals can use the correct terminology and proper concepts in their dealings with the supported commander and staff and fellow intelligence professionals. This ensures the credibility of the professionals and the intelligence warfighting function.

2-50. The primary purpose of intelligence is to effectively support operations. Intelligence professionals must understand intelligence fundamentals and basic Army operational doctrine to provide effective and flexible intelligence support. This also assists intelligence professionals in understanding how commanders and staffs integrate and synchronize intelligence into operations as well as ensuring they are an effective part of the combined arms team.

ARMY OPERATIONS

2-51. 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. It supports four strategic roles for the joint force. Army forces shape OEs, counter aggression on land during crisis, prevail during large-scale combat, and consolidate gains. The Army fulfills its strategic roles by providing forces for joint campaigns that enable the integrated deterrence of adversaries outside of conflict and the defeat of enemies during conflict or war.

2-52. Army forces achieve objectives through the conduct of operations. An *operation* is a sequence of tactical actions with a common purpose or unifying theme (JP 1, Volume 1). Operations vary in many ways. They occur in all types of physical environments, including urban, subterranean, desert, jungle, mountain, maritime, and arctic. Operations vary in scale of forces involved and duration. Operations change various conditions in the human, information, and physical dimensions of an OE and how these dimensions interrelate.

2-53. The complex environment in which operations occur demands leaders who understand both the science and art of operations. Understanding the science of operations—such as combat power ratios, weapons ranges, and movement tables—assists leaders in improving synchronization and reducing risk. However, there is no way to eliminate uncertainty, and leaders must exercise operational art to make decisions and assume risk. Intangible factors, such as the impact of leadership on morale, using shock effect to defeat enemy forces, and supportive populations, are fundamentally human factors that can overcome physical disadvantages and often decide the outcomes of an operation.

2-54. Army forces must be prepared for the most demanding and dangerous types of operations. Army forces contribute to conventional deterrence through their demonstrated capability, capacity, and will to wage war on land in any environment against any opponent. Credible combat forces with lethal capabilities make the other instruments of national power more potent, and they assist in deterring the enemy's escalation of violence during other types of operations. (See FM 3-0 for doctrine on Army operations.)

2-55. Effective and flexible intelligence support assists the Army with the challenges and complexity associated with a broad variety of and significant differences between the types of Army operations and the OE factors that affect those operations. Army commanders, staffs, and the intelligence warfighting function must leverage the intelligence enterprise and fight for intelligence to grapple with these issues. While intelligence is complex and threats, especially peer threats, can counter at least some of the intelligence capabilities and collection assets, Army commanders and staffs can overcome these issues. Every Army echelon can mitigate these challenges through the commander owning the intelligence effort, effective staff integration, and creative and adaptive information collection to overcome existing information collection gaps. Together, these aspects of fighting for intelligence ensure success, whether the operation is a large-scale combat operation, foreign humanitarian operation, counterinsurgency, foreign internal defense, or a noncombatant evacuation.

MULTIDOMAIN OPERATIONS

2-56. *Multidomain operations* is the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders (FM 3-0). Employing Army and joint capabilities makes use of all available combat power from each domain to accomplish missions at the least cost. Multidomain operations are the Army's contribution to joint campaigns, spanning the competition continuum. Below the threshold of armed conflict, multidomain operations are how Army forces accrue advantages and demonstrate readiness for conflict, deterring adversaries while assuring allies and partners. During conflict, they are how Army forces close with and destroy the enemy, defeat enemy formations, seize critical terrain, and control populations and resources to deliver sustainable political outcomes.

2-57. Leaders must understand the interdependencies between their own assigned forces and the forces or capabilities provided by others to generate the complementary and reinforcing effects of combined arms approaches. Army forces employ joint and other unified action partner capabilities to the extent they are available. However, because peer threats can contest the force in all domains, Army forces must be prepared to conduct operations when some or all joint capabilities are unavailable to support mission accomplishment.

2-58. Army forces employ organic capabilities in multiple domains, and they continuously benefit from air and maritime strategic transportation and space and cyberspace capabilities that they do not control, including global positioning, satellite communications, and joint ISR. Lower echelons may not always notice the opportunities created by higher echelons or other forces that operate primarily in other domains; however, leaders must understand how the absence of those opportunities affects their concepts of operations, decision making, and risk assessment. Like all operations, Army intelligence is and has been inherently multidomain in terms of the intelligence process.

RELATIVE ADVANTAGE

2-59. During operations, small advantages can have significant impacts on the outcome of a mission, particularly when they accrue over time. Therefore, creating and exploiting relative advantages are necessary for all operations, and they become even more critical when opposing sides are evenly matched. A *relative advantage* is a location or condition, in any domain, relative to an adversary or enemy that provides an opportunity to progress towards or achieve an objective (FM 3-0). Commanders seek and create relative advantages to exploit through action, and they continually assess the situation to identify ways to expand opportunities. Army forces must accurately see themselves, see the enemy or adversary, and understand their OE before they can identify and exploit windows of opportunity to reach a relative advantage; this is one way that intelligence is critical to operations.

2-60. Army leaders are accustomed to creating and exploiting relative advantages through the combined-arms approach that traditionally focuses on capabilities from the land, maritime, and air domains. The proliferation of space and cyberspace capabilities further requires leaders who understand the advantages those capabilities create in their OE. The ability to integrate space, counterspace, and cyberspace capabilities (which can vary by echelon) expands options for creating advantages to exploit. Multidomain operations fracture the coherence of threat operational approaches by destroying, dislocating, isolating, and disintegrating their interdependent systems and formations, and by exploiting the opportunities these disruptions provide to defeat enemy forces in detail.

2-61. Army forces combine maneuver and targeting methods to defeat enemy formations and systems. Army forces employ maneuver to close with and destroy enemy formations in close operations. Targeting priorities support fires and other key capabilities to disintegrate enemy networks and systems. The commander and staff must consider the various situational understanding-related requirements and targeting-related intelligence requirements and prioritize them accordingly.

Note. Generally, a thorough situational understanding is necessary to conduct effective targeting. Leaders execute the targeting process to create advantages that enable freedom of maneuver and exploit the positional advantages created by maneuver. Targeting is a key means for leaders to integrate the joint capabilities required to create depth in the OE and protect friendly formations.

WINDOWS OF OPPORTUNITY, RELATIVE ADVANTAGES, AND INTELLIGENCE

2-62. Reaching a position of relative advantage across multiple domains does not just happen. Friendly forces must find and exploit a window of opportunity to reach a relative advantage. This effort is closely related to planning and creating desired effects (through lethal and nonlethal means) during operations. These windows of opportunity could be considered subtasks of or a main task to reaching a position of relative advantage. Both a position of relative advantage and a window of opportunity are doctrinal concepts and not concrete graphic planning measures such as named areas of interest (NAIs) or decision points. However, a creative staff should be able to graphically portray a window of opportunity through a series of related existing graphic planning measures like NAIs, decision points, target areas of interest (TAIs), and engagement areas.

2-63. Identifying a possible window of opportunity (in time, location, domains, and possibly dimensions), planning operations, and controlling operations to exploit the window of opportunity requires focused intelligence analysis. Therefore, Army forces require timely, accurate, relevant, and predictive intelligence to understand threat characteristics, capabilities, objectives, and COAs across domains when relevant to the mission. Intelligence initially drives the combinations of defeat mechanisms that commanders and staffs pursue as they employ friendly force capabilities, sometimes precisely in time and space, against enemy forces.

2-64. During IPOE, each staff element provides input, ensuring a sufficiently broad view of the OE. Subsequently, the IPOE effort assists in identifying windows of opportunity to exploit threat vulnerabilities. For example, the air defense artillery staff element's input to IPOE about enemy IADS capabilities and vulnerabilities may present the friendly commander with a possible window of opportunity. The gaps identified during initial IPOE and the requirements developed during the subsequent steps of the MDMP would drive information collection requirements to confirm the window of opportunity, support further planning, and support the exploitation of the window of opportunity. (See ATP 2-01.3 for IPOE doctrine.)

2-65. Besides IPOE, building a relatively complete situational understanding (supported by intelligence situation development) across all domains and dimensions is required to see opportunities, seize the initiative, and exploit enemy vulnerabilities at a window of opportunity. Seeing and understanding when and how to isolate portions of the OE in one or more domains must be supported by the intelligence warfighting function across echelons and include leveraging the intelligence enterprise. (See figure 2-7.) Friendly forces may not be able to continually maintain an adequate level of situational understanding to exploit every window of opportunity. In these situations, friendly forces must either accept a greater degree of risk or wait until they can rebuild an adequate level of situational understanding to exploit a window of opportunity.

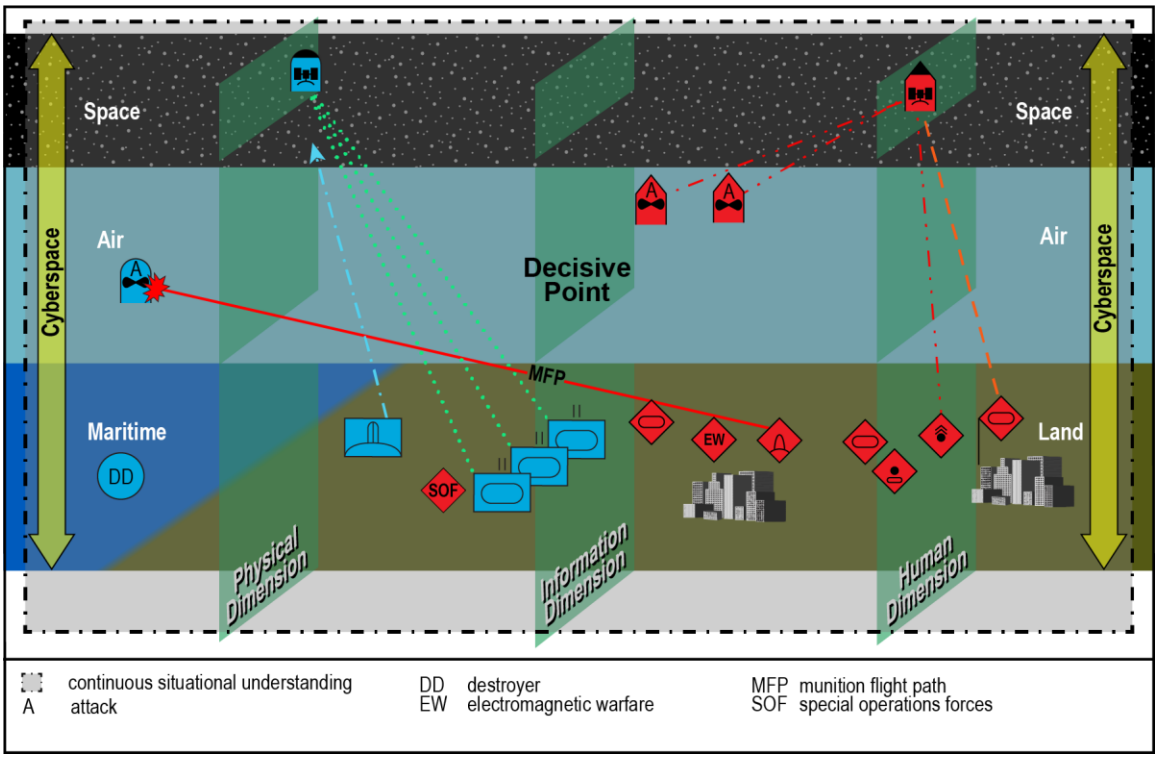


Figure 2-7. Finding windows of opportunity by building situational understanding

2-66. During large-scale combat operations against a peer threat, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to open a window of opportunity for further exploitation by the joint force. For example, the destruction of specific enemy IADSs within a time window and at specific locations may allow friendly joint suppression of enemy air defense operations. This, in turn, may allow a deep strike that could result in the destruction of key enemy capabilities and lead to a relative

advantage. Figure 2-8 depicts a scenario based on this example of a window of opportunity and exploiting the window of opportunity.

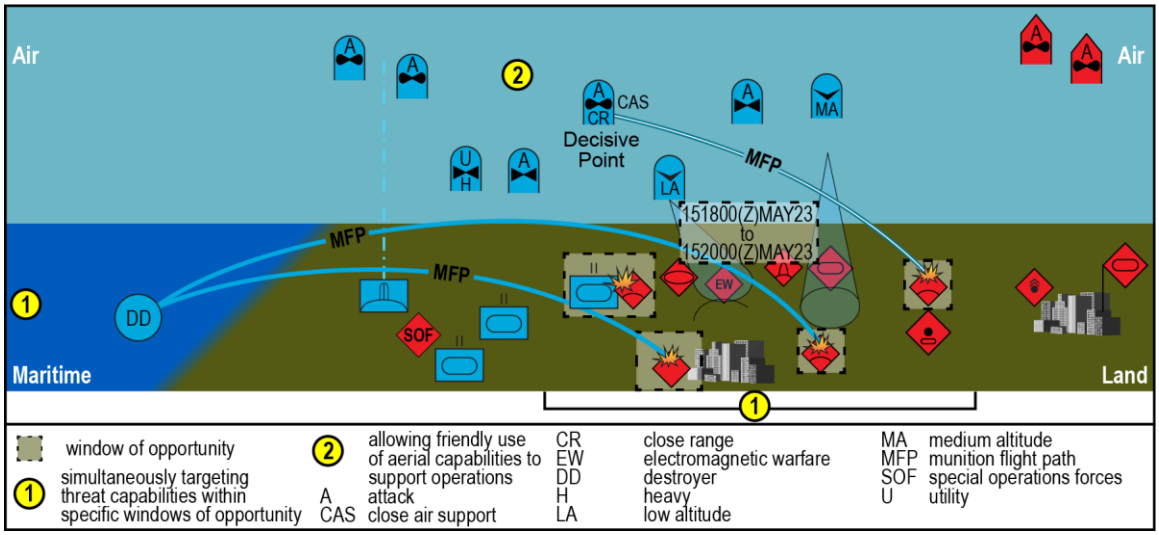


Figure 2-8. Window of opportunity and exploiting the window of opportunity (example)

LARGE-SCALE COMBAT OPERATIONS

2-67. The Army is manned, equipped, and trained to operate in all operational scenarios or categories, starting with the most lethal conditions first—large-scale combat against a peer threat. *Large-scale combat operations* are extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives (ADP 3-0). During ground combat, they typically involve operations by multiple corps and divisions and include substantial forces from the joint and multinational team. Large-scale combat operations often include both conventional and irregular forces on both sides. Chapter 4 discusses large-scale combat operations as part of armed conflict.

2-68. The Army provides the joint force commander (JFC) significant and sustained landpower and intelligence capabilities. *Landpower* is the ability—by threat, force, or occupation—to gain, sustain, and exploit control over land, resources, and people (ADP 3-0). The Army supports the joint force by providing capabilities and capacity to apply sustained combined arms landpower. Those capabilities include maneuver, fires, special operations, intelligence, EW, cyberspace operations, space operations, sustainment, and area security. Army forces assist JFCs in gaining and maintaining the initiative, defeating enemy forces on the ground, controlling territory and populations, and consolidating gains to establish conditions for a political settlement favorable to U.S. interests.

2-69. The JFC applies Army capabilities to neutralize sophisticated enemy forces and capabilities by systematically destroying key nodes and capabilities essential to the enemy's ability to continue fighting and/or legitimizing its messaging. The joint force requires Army special operations forces and conventional Army units that are proficient in combined arms operations and capable of employing capabilities across multiple domains in complementary ways. By aggressively engaging the enemy, Army forces enable joint force freedom of action. Army intelligence capabilities are an integral part of joint ISR across all unified action partners. (See FM 6-05 for doctrine on special operations forces and conventional force integration.)

COMBINED ARMS AND COMBAT POWER

2-70. *Combined arms* is the synchronized and simultaneous application of arms to achieve an effect greater than if each element was used separately or sequentially (ADP 3-0). Leaders combine arms in complementary and reinforcing ways to protect capabilities and amplify their effects. Confronted with a constantly changing situation, leaders create new combinations of capabilities, methods, and effects to pose new dilemmas for

adversaries. The combined arms approach to operations during competition, crisis, and armed conflict is foundational to exploiting capabilities from all domains and dimensions.

2-71. Complementary capabilities compensate for the vulnerabilities of one system or organization with the capabilities of a different one. Infantry protects tanks from enemy infantry and antitank systems, while tanks provide mobile protected firepower for the infantry. Ground maneuver can make enemy forces displace and become vulnerable to joint fires, while joint fires can disrupt enemy reserves and C2 to enable operations on the ground. Cyberspace and space capabilities and EW can prevent enemy forces from detecting and communicating the location of friendly land-based fires capabilities, and Army fires capabilities can destroy enemy ground-based cyberspace nodes and EW platforms to protect friendly communications.

2-72. Reinforcing capabilities combine similar systems or capabilities to amplify the overall effects a formation brings to bear in a particular context. During urban operations, for example, infantry, aviation, and armor units working in close coordination reinforce the protection, maneuver, and direct fire capabilities of each unit type while creating cascading dilemmas for enemy forces. Army artillery can be reinforced by close air support, air interdiction, and naval surface fire support. This greatly increases both the mass and range of fires available to a commander. Space and cyberspace capabilities used to disrupt enemy communications can reinforce a brigade combat team's (BCT's) ground-based jamming effort to increase the disruption to enemy C2. Military information support operations can amplify the effects of physical isolation on an enemy echelon, making it more vulnerable to friendly force exploitation.

2-73. The organic composition, training, and task organization of Army units set conditions for effective combined arms. Throughout operations, commanders assess the OE and adjust priorities, change task organization, and request capabilities to create exploitable advantages, extend operational reach, preserve combat power, and accomplish missions.

2-74. *Combat power* is the total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time (JP 3-0). To generate combat power and apply it against enemy forces, Army forces integrate capabilities and synchronize *warfighting functions*—groups of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives (ADP 3-0). The intelligence warfighting function is synchronized with the other warfighting functions to generate each dynamic—leadership, firepower, information, mobility, and survivability—of combat power (see FM 3-0). (See figure 2-9.)

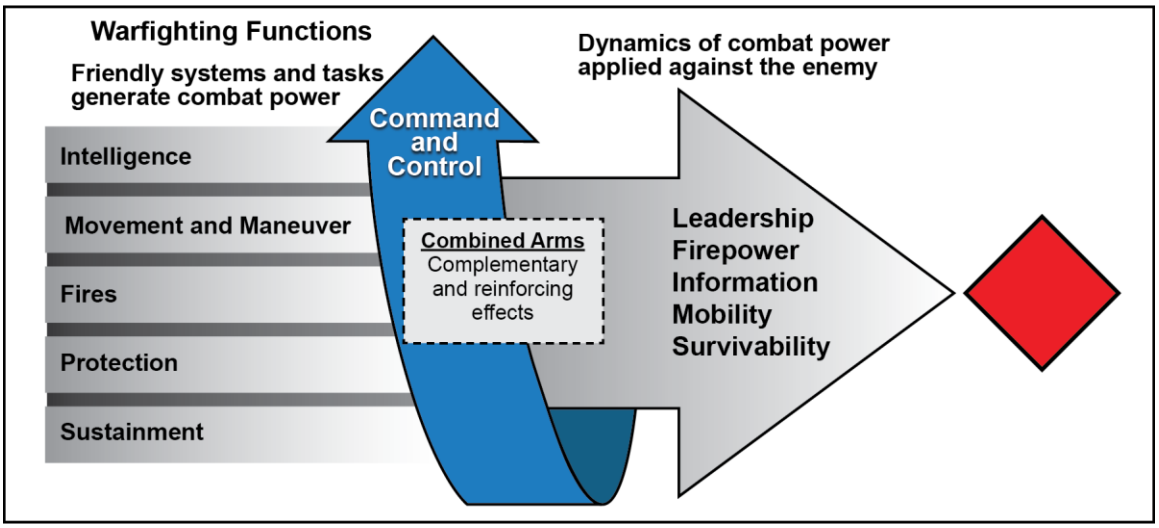


Figure 2-9. Generating combat power

2-75. The warfighting functions provide an intellectual organization for common critical capabilities available to commanders and staffs at all echelons and levels of warfare. Warfighting functions are not confined to a single domain; they typically include capabilities from multiple domains. Warfighting functions are not branch-specific. Although some branches, staff sections, and types of units have a role or purpose that mainly aligns with a warfighting function, each warfighting function is relevant to all types of units.

2-76. Through the warfighting functions, well sustained units can move and maneuver to bring combat power to bear against the enemy. Joint and Army indirect fires complement and reinforce organic firepower in maneuver units. Survivability is a function of protection tasks, the protection inherent to Army platforms, and schemes of maneuver that focus friendly strengths against enemy weaknesses. Intelligence determines how and where to best apply combat power against enemy weaknesses. C2 enables leadership, the most important qualitative aspect of combat power.

2-77. Intelligence professionals must understand the value of their role within the combined arms approach to generating combat power through the dynamics of leadership, firepower, information, mobility, and survivability. The combined arms approach creates complementary and reinforcing effects by employing the warfighting functions, which are primarily synchronized by the C2 warfighting function. In this manner, the intelligence warfighting function plays a key role in combined arms. To a large extent, understanding the OE, planning operations, controlling ongoing operations, and conducting operational assessments begin with intelligence. Effective intelligence staff activities and intelligence operations result from intelligence synchronization, careful planning, and tailoring the use of intelligence capabilities and the intelligence architecture specifically for that unit's operation.

MULTIDOMAIN OPERATIONS: THE ARMY'S OPERATIONAL CONCEPT

2-78. The Army's operational concept is multidomain operations. Multidomain operations are how Army forces contribute to and operate as part of the joint force. Army forces, enabled by joint capabilities, provide the lethal and resilient landpower necessary to defeat threat standoff approaches and achieve joint force objectives.

2-79. The employment of joint and Army capabilities, integrated across echelons and synchronized in a combined arms approach, is essential to defeating threats able to contest the joint force in all domains. Army forces integrate land, maritime, air, space, and cyberspace capabilities that facilitate maneuver to create human, information, and physical advantages that JFCs exploit across the competition continuum. Commanders and staffs require the knowledge, skills, attributes, and intelligence to integrate capabilities rapidly and at the necessary scale appropriate to each echelon.

2-80. During competition, theater armies strengthen landpower networks, set the theater, and demonstrate readiness for armed conflict through the C2 of Army forces supporting the command campaign plan. During crisis, theater armies provide options to combatant commanders (CCDRs) as they facilitate the flow and organization of land forces moving into theater. During armed conflict, theater armies enable and support the joint force land component commander's (JFLCC's) employment of land forces. The JFLCC provides C2 of land forces and allocates joint capabilities to its corps and other subordinate tactical formations.

2-81. Corps integrate joint and Army capabilities at the right tactical echelons and employ divisions to achieve JFLCC objectives. Divisions, enabled and supported by corps, defeat enemy forces, control land areas, and consolidate gains for the joint force. Defeating or destroying enemy capabilities that facilitate the enemy's preferred layered standoff approaches is central to success. For example, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to shape the environment to gain a position of relative advantage for activities, such as joint fires, within the other domains. Ultimately, operations by Army forces both enable and are enabled by the joint force.

2-82. Because uncertainty, degraded communications, and fleeting windows of opportunity characterize OEs during combat, multidomain operations require a disciplined initiative cultivated through a mission command culture. Leaders must have a bias for action and accept that some level of uncertainty is always present. Commanders who empower leaders to make rapid decisions and accept risk within the commander's intent enable formations at echelon to adapt rapidly while maintaining unity of effort. (See ADP 6-0 for doctrine on the mission command approach.)

Multidomain Task Force

The multidomain task force (MDTF) is one way that Army units integrate capabilities across domains to assist in achieving joint force objectives. An MDTF is an Army brigade-sized task force designed to coordinate, integrate, synchronize, and employ cross-domain fires to neutralize enemy A2 and AD strategies. MDTF operations allow more options for the joint force and a greater degree of freedom of maneuver. The MDTF has the following MI capabilities:

- The MDTF S-2 is the principal staff officer for intelligence and synchronizes the intelligence warfighting function.
- The multidomain effects battalion (MDEB) provides sensing and intelligence support, target development, and delivery and synchronization of nonlethal effects to the MDTF. The MDEB provides mission C2, planning, analysis, execution as well as company-level staff support functions.
  - The MDEB S-2 section performs IPOE to assist the commander and staff's visualization, planning, decision making, and nonkinetic effects employment.
  - The MDEB has an organic MI company that answers the commander's intelligence requirements and conducts SIGINT collection and technical analysis, OSINT, intelligence PED, and intelligence analysis to support multidomain operations. The MI company also coordinates with the fires cell for target development across the strategic contexts to create a relative advantage. (See ATP 2-19.1-1 and ATP 3-93.)

Note. All Army units conduct multidomain operations, not just MDTFs.

2-83. Army intelligence supports all aspects of multidomain operations across all echelons—from the CCDR and staff to the Army maneuver battalion commander and staff. Joint intelligence supports critical joint force objectives such as neutralizing enemy integrated air defenses, destroying long-range surface-to-surface fires systems, denying enemy access to a designated area, disrupting enemy C2, protecting friendly networks, conducting military deception, or disrupting an enemy's ability to conduct information warfare. These operations are enabled by precise and detailed joint intelligence on threat capabilities and vulnerabilities across all domains. Seeing and understanding when and how the joint force isolates portions of the OE in one or more domains are important to Army operations.

2-84. Army intelligence is inherently multidomain, joint, interagency, intergovernmental, and multinational through the intelligence enterprise. The Army synchronizes with unified action partners to provide effective and flexible intelligence across multiple domains and to reduce operational uncertainty. Through the Army IWFTs, intelligence professionals across the echelons support how commanders and staffs plan, make decisions, and control operations in and across the various domains and dimensions. Using the various tools and processes discussed under understanding an OE, the intelligence staff strives to support continuous situational understanding to allow Army units to see opportunities, seize the initiative, and exploit enemy vulnerabilities to open windows of opportunity and reach positions of relative advantage.

2-85. The optimal mix of leveraging partner, national, and joint capabilities and conducting aggressive Army information collection are necessary to defeat threat A2 and AD capabilities and support friendly long-range precision fires. Emerging Army deep sensing capabilities will assist in improving Army lethality at a greater depth. ***Deep sensing*** **is the employment of capabilities beyond the division coordinated fire line to collect data and information that supports targeting, situational understanding, or decision making**.

TENETS OF OPERATIONS

2-86. The tenets of operations are desirable attributes that should be built into all plans and operations; they are directly related to how the Army's operational concept should be employed. Commanders use the tenets of operations to inform and assess COAs throughout the operations process. The extent to which an operation exhibits the tenets provides insight into the probability of success. The tenets of operations are agility, convergence, endurance, and depth.

2-87. The Army provides forces capable of transitioning to combat operations, fighting for information, producing intelligence, adapting to unforeseen circumstances, and defeating enemy forces (**agility**). Army forces employ capabilities from multiple domains in a combined arms approach that creates complementary and reinforcing effects through multiple domains, while preserving combat power to maintain options for the JFC (**convergence**). Creating and exploiting relative advantages require Army forces to operate with endurance and in depth. **Endurance** enables the ability to absorb the enemy's attacks and press the fight over the time and space necessary to accomplish the mission. **Depth** applies combat power throughout the OE, securing successive operational objectives and consolidating gains for the joint force. Table 2-10 lists several intelligence considerations for the tenets of operations.

Table 2-10. Intelligence considerations for the tenets of operations

Tenet of operations	*Intelligence considerations (not all-inclusive)*
Agility is the ability to move forces and adjust their dispositions and activities more rapidly than the enemy (FM 3-0). Agility requires sound judgment and rapid decision making, often gained by creating and exploiting information advantages. Agility requires leaders to anticipate needs or opportunities and trained formations to change direction, tasks, or focus as quickly as the situation requires. Change can include a transition between phases of an operation or the requirement to adapt to a new opportunity or hazard.	• Intelligence preparation of the operational environment: ▪ Terrain and weather analysis. ▪ Careful consideration of threat capabilities in conjunction with threat characteristics and threat models. ▪ Situation templates. ▪ Event templates and associated event matrices. • Collection management. • Support to rapid decision making and risk management. • Input to decision support templates and to branches and sequels. • Support to information advantage activities. • Support to identifying windows of opportunity and relative advantages. • Continuous updates to the CIP and intelligence portion of the COP.
Convergence is an outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area (FM 3-0). Its utility derives from understanding the interdependent relationships among capabilities from different domains and combining those capabilities in surprising, effective tactics that accrue advantages over time. When combined, the complementary and reinforcing nature of each friendly capability present multiple dilemmas for enemy forces and produce an overall effect that is greater than the sum of each individual effect. The greater the extent to which forces achieve convergence and sustain it over time, the more favorable the outcome.	• Intelligence preparation of the operational environment: ▪ Significant civil considerations. ▪ Detailed situation templates. For example, templating threat logistics and lines of communications. ▪ Event templates and associated event matrices. ▪ High-value targets. • Understanding the domains and dimensions through pre-mission analysis of the operational environment. • Collection management and effectively using intelligence handover lines. • Input to decision support templates. • Support to functional analysis and center of gravity analysis. • Support to information advantage activities. • Support to identifying windows of opportunity and relative advantages. • Support to targeting: ▪ Analyzing threat systems and conducting target value analysis. ▪ Developing target intelligence folders. ▪ Conducting subsequent target development. • Continuous updates to the CIP and intelligence portion of the COP.
Endurance is the ability to persevere over time throughout the depth of an operational environment (FM 3-0). Endurance enhances the ability to project combat power and extends operational reach; it is about resilience and preserving combat power while continuing operations for as long as is necessary to achieve the desired outcome. During competition, Army forces improve endurance by setting the theater across all warfighting functions and improving interoperability with allies and other unified action partners. Endurance stems from organizing, protecting, and sustaining a force.	• Intelligence preparation of the operational environment: Careful consideration and templating (situation and event templates) of threat activities in the rear area (friendly operational framework). • Collection management. • Counterintelligence primary mission areas (not the same as force protection; see paragraphs 1-66 through 1-68). • Input to protection activities. • Input to security operations. • Input to decision support templates. • Support to targeting. • Continuous updates to the CIP and intelligence portion of the COP.

Table 2-10. Intelligence considerations for the tenets of operations (*continued*)

Tenet of operations	*Intelligence considerations (not all-inclusive)*
Depth is the extension of operations in time, space, or purpose to achieve definitive results (ADP 3-0). While the focus of endurance is friendly combat power, the focus of depth is enemy locations and dispositions across all domains. Commanders achieve depth by understanding the strengths and vulnerabilities of the enemy's echeloned capabilities and then attacking them throughout their dispositions simultaneously and sequentially. Although simultaneous attacks through all domains in depth are not possible in every situation, leaders seek to expand their advantages and limit enemy opportunities for sanctuary and regeneration. Leaders describe the depth they can achieve in terms of operational reach.	• Intelligence preparation of the operational environment: ▪ Terrain and weather analysis. ▪ Detailed situation templates, especially in the deep area (friendly operational framework). ▪ Event templates and associated event matrices. ▪ High-value targets. • Understanding the domains and dimensions through pre-mission analysis of the operational environment. • Collection management and effectively using deep sensing. • Input to decision support templates. • Support to targeting, especially deep operations and long-range precision fires. • Support to information advantage activities. • Continuous updates to the CIP and intelligence portion of the COP.

ADP Army doctrine publication
CIP common intelligence picture
COP common operational picture
FM field manual

IMPERATIVES OF OPERATIONS

2-88. Imperatives are actions Army forces must take to defeat enemy forces and achieve objectives at an acceptable cost. They are informed by the OE and the characteristics of the most capable threats that Army forces can encounter. The imperatives of operations include—

- See yourself, see the enemy, and understand the OE.
- Account for being under constant observation and all forms of enemy contact.
- Create and exploit relative human, information, and physical advantages in pursuit of decision dominance.
- Make initial contact with the smallest element possible.
- Impose multiple dilemmas on the enemy.
- Anticipate, plan, and execute transitions.
- Designate, weight, and sustain the main effort.
- Consolidate gains continuously.
- Understand and manage the effects of operations on units and Soldiers.

2-89. Table 2-11 lists several intelligence considerations for the imperatives of operations.

Table 2-11. Intelligence considerations for the imperatives of operations

Imperative	*Intelligence considerations (not all-inclusive)*
See yourself, see the enemy, and understand the OE. Commanders visualize OEs in terms of factors that are relevant to decision making. OEs are dynamic and contain vast amounts of information that can overload C2 systems and impede decision making. Commanders simplify information collection, analysis, and decision making by focusing on how they see themselves, see the enemy, and understand the OE. These three categories of factors are interrelated, and leaders must understand how each one relates to the others in the current context.	• Applicable to most intelligence warfighting function tasks. • Understanding the domains and dimensions through pre-mission analysis of the OE in conjunction with cultural intelligence and civil information. • Intelligence preparation of the OE: enemy COA development. • Collection management. • Functional analysis and center of gravity analysis (corresponds to defeat mechanisms [see FM 3-0]). • Collaboration with the entire staff to facilitate situational and shared understanding of friendly and threat strengths and vulnerabilities and potential impacts across the OE. • Assisting the commander and staff in understanding friendly combat power in relation to the threat correlation of forces analysis. • Advising the commander on intelligence requirements development. • Developing and maintaining a running estimate and the CIP. • Input to the military decision-making process. • Support to security operations and protection activities.

Table 2-11. Intelligence considerations for the imperatives of operations (*continued*)

Imperative	*Intelligence considerations (not all-inclusive)*
Account for being under constant observation and all forms of enemy contact. Air, space, and cyberspace capabilities increase the likelihood that threat forces can gain and maintain continuous visual and electromagnetic contact with Army forces. Enemy forces possess a wide range of land-, maritime-, air-, and space-based intelligence, surveillance, and reconnaissance capabilities that can detect U.S. forces. Leaders must assume they are under constant observation from one or more domains and continuously ensure they are not providing lucrative targets for the enemy to attack.	• Considering threat collection across all domains and dimensions and integrating that into the planning and execution of operations. • Multidisciplined intelligence threat assessments and associated countermeasure recommendations. • Counterintelligence primary mission areas. • Intelligence preparation of the OE: ▪ Modified combined obstacle overlays. ▪ Observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (OAKOC=military aspects of terrain). ▪ Considering the forms of contact, including influence. (See paragraphs 8-30 and 8-31.) ▪ Terrain analysis. ▪ Terrestrial and space weather analysis, with an emphasis on weather effects, in conjunction with the Air Force staff weather officer. ▪ Line of sight analysis. ▪ Electromagnetic reconnaissance. ▪ Identifying enemy reconnaissance objectives. • Support to counterreconnaissance, including counter-unmanned aircraft system operations. • Input to essential elements of friendly information. • Support to counterspace operations. • Support to deception operations. • Input to obscuration operations. • Input to the various forms of security across all security operations and activities, including electromagnetic emission control measures, unit dispersion techniques, operations security, information security, and physical security.
Create and exploit positions of physical, information, and human advantage in pursuit of decision dominance. The employment of lethal forces is based on the premise that destruction and other physical consequences compel enemy forces to change their decision making and behavior, ultimately accepting defeat. The type, amount, and ways in which lethal forces compel enemy forces varies, and this depends heavily on enemy forces, their capabilities, goals, and the will of relevant populations. Understanding the relationship between physical, information, and human factors enables leaders to take advantage of every opportunity and limit the negative effects of undesirable and unintended consequences.	• Intelligence preparation of the OE: ▪ Situational understanding of domain and dimension interrelationships. ▪ Identifying enemy decision makers (with supporting identity intelligence), C2 networks with capabilities and vulnerabilities, objectives and intent, and possible key decision points. • Collection management. • Support to the military decision-making process. • Support to identifying windows of opportunity and relative advantages. • Support to information advantage activities.
Make initial contact with the smallest element possible. Army forces are extremely vulnerable when they do not sufficiently understand the disposition of enemy forces and become decisively engaged on terms favorable to enemy forces. To avoid being surprised and incurring heavy losses, leaders must set conditions for making enemy contact on terms favorable to the friendly force. Leaders should anticipate when and where to make enemy contact, the probability and impact of making enemy contact, and actions to take on contact. Quickly applying multiple capabilities against enemy forces while preventing the bulk of the friendly force from being engaged itself requires understanding the forms of contact.	• Intelligence preparation of the OE: COA development. • Collection management. • Support to rapid development of situational understanding. • Input to information collection—cueing, redundancy, and mix considerations across domains and dimensions.

Table 2-11. Intelligence considerations for the imperatives of operations (*continued*)

Imperative	*Intelligence considerations (not all-inclusive)*

Impose multiple dilemmas on the enemy. Imposing multiple dilemmas on enemy forces complicates their decision making and forces them to prioritize among competing options. This is a way of seizing the initiative and making enemy forces react to friendly operations. Simultaneous operations encompassing multiple domains—conducted in depth and supported by deception—present enemy forces with multiple dilemmas. Employing capabilities from multiple domains degrades enemy freedom of action, reduces enemy flexibility and endurance, and disrupts enemy plans and coordination. The application of capabilities in complementary and reinforcing ways creates more problems than an enemy commander can solve. This erodes enemy effectiveness and the will to fight.	• Intelligence preparation of the OE:
	  ▪ Situational understanding of domain and dimension interrelationships.
	  ▪ Identifying enemy C2 networks with capabilities and vulnerabilities.
	  ▪ COA development.
	  ▪ Event templates and associated event matrices.
	• Support to the military decision-making process.
	• Support to targeting.
	• Support to deception efforts.

Anticipate, plan, and execute transitions. Transitions mark a change of focus in an operation. Leaders plan transitions as part of the initial plan or parts of a branch or sequel. They can be unplanned and cause the force to react to unforeseen circumstances. Transitions can be part of progress toward mission accomplishment, or they can reflect a temporary setback.	• Input to information collection. • Collection management with emphasis on collection transitions. • Input to the military decision-making process. • Input to consolidating gains, branches, and sequels. • Continuous updates to the CIP and intelligence portion of the COP. • Support to assessments, including measures of performance and effectiveness.
Designate, weight, and sustain the main effort. Commanders frequently face competing demands for limited resources. They establish priorities to resolve these demands by designating, weighting, and sustaining the main effort. They provide the main effort with the appropriate resources and support necessary for its success. When designating a main effort, commanders consider augmenting a unit's task organization and giving it priority of resources and support. The commander designates various priorities of support, such as for air and missile defense, close air support and other fires, information collection, mobility and countermobility, and sustainment.	• Intelligence preparation of the OE with emphasis on terrain analysis. • Assisting the commander and staff in understanding friendly combat power in relation to the threat correlation of forces analysis. • Support to identifying defeat mechanisms. • Collection management. • Support to information collection. • Input to the military decision-making process. • Support to targeting. • Continuous updates to the CIP and intelligence portion of the COP.
Consolidate gains continuously. Leaders add depth to their operations in time and purpose when they consolidate gains. Commanders consolidate gains at the operational and tactical levels as a strategically informed approach to current operations, considering the desired political outcome of the conflict. During competition and crisis, commanders expand opportunities created from previous conflicts and activities to sustain enduring U.S. interests, while improving the credibility, readiness, and deterrent effect of Army forces. During large-scale combat operations, commanders consolidate gains continuously or as soon as possible, deciding whether to accept risk with a more moderate tempo during the present mission or in the future as large-scale combat operations conclude.	• Collection management. • Counterintelligence primary mission areas. • Support to security operations and protection activities. • Evaluating time windows for effects to appear within the OE. • Support to stability activities or operations. • Continuous updates to the CIP and intelligence portion of the COP.
Understand and manage the effects of operations on units and leaders. Continuous operations rapidly degrade the performance of people and the equipment employed, particularly during combat. In battle, Soldiers and units are more likely to fail catastrophically than gradually. Commanders and staffs must be alert to small indicators of fatigue, fear, indiscipline, and reduced morale; they must take measures to deal with these indicators before their cumulative effects drive a unit to the threshold of collapse. Staffs and commanders at higher echelons must consider the impact of prolonged combat on subordinate units. This causes efficiency to drop, even when physical losses are not great.	• Engagement with intelligence staff members. • Focusing on training to improve combat effectiveness. • Staff member recuperation. • Military intelligence unit engaged leadership.

C2 command and control
CIP common intelligence picture
COA course of action
COP common operational picture
FM field manual
OE operational environment
U.S. United States

OPERATIONAL APPROACH AND OPERATIONAL FRAMEWORK

2-90. An operational approach provides the logic for how tactical tasks ultimately achieve the desired end state. It provides a unifying purpose and focus to all operations. Sound operational approaches balance risk and uncertainty with friction and chance. The operational approach provides the basis for detailed planning, allows leaders to establish a logical operational framework, and assists in producing an executable order. (See ADP 3-0 and ADP 5-0 for doctrine on operational art and planning, respectively.)

2-91. An operational framework organizes an area of geographic and operational responsibility for the commander and provides a way to describe the employment of forces. The framework illustrates the relationship between close operations, operations in depth, and other operations in time and space across domains. As a visualization tool, the operational framework bridges the gap between a unit's conceptual understanding of the environment and its need to generate detailed orders that direct operations.

OPERATIONAL APPROACH

2-92. Through operational art, commanders develop their *operational approach*—a broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission (JP 5-0). An operational approach is the result of the commander's visualization of what needs to be done in broad terms to solve identified problems. It is the main idea that informs detailed planning. When describing an operational approach, commanders—

- Consider ways to defeat enemy forces in detail and potential decisive points. *Defeat in detail* is concentrating overwhelming combat power against separate parts of a force rather than defeating the entire force at once (ADP 3-90).
- Employ combinations of defeat mechanisms to isolate and defeat enemy forces, functions, and capabilities.
- Assess options for assuming risk.

2-93. Table 2-12 lists several operational and intelligence considerations for operational approach.

Table 2-12. Operational and intelligence considerations for operational approach

Operational approach	*Operational and intelligence considerations (not all-inclusive)*
Defeating enemy forces in detail Armed conflict implies the need to defeat enemy forces. *Defeat* is to render a force incapable of achieving its objectives (ADP 3-0). When used as a task or effect in operations, defeat provides the commander maximum flexibility to accomplish the mission. Senior leaders assign defeat as a task when the situation is still developing, or when the commander on the ground, by virtue of experience and proximity to the problem, is uniquely capable of deciding how to employ lethal force to accomplish objectives.	• Understanding the commander's intent. • Evaluating enemy forces in the context of all the relevant domains and dimensions of an operational environment. • Understanding threat functions, capabilities, and echelonment. • Understanding how the enemy may employ capabilities. • Identifying enemy strengths and vulnerabilities. • Comparing enemy vulnerabilities to friendly advantages to identify decisive points (key terrain, key events, critical factors or functions) to achieve convergence.
Defeat mechanisms *Defeat mechanism* is a method through which friendly forces accomplish their mission against enemy opposition (ADP 3-0). Army forces at all echelons commonly use combinations of the four defeat mechanisms. Applying more than one defeat mechanism simultaneously creates multiple dilemmas for enemy forces and complementary and reinforcing effects not attainable with a single mechanism. Commanders may have an overarching defeat mechanism or combination of mechanisms that accomplish the mission, with supporting defeat mechanisms for components of an enemy formation or warfighting system. Defeat mechanisms can guide the subordinate development of tactical tasks, purposes, and effects in operations, facilitating control and initiative.	• **Defeat mechanisms:** ▪ ***Destroy*** is a tactical mission task that physically renders an enemy force combat-ineffective until reconstituted (FM 3-90). ▪ ***Dislocate*** is to employ forces to obtain significant positional advantage in one or more domains, rendering the enemy's dispositions less valuable, perhaps even irrelevant (FM 3-0). ▪ ***Isolate*** is to separate a force from its sources of support in order to reduce its effectiveness and increase its vulnerability to defeat (ADP 3-0). ▪ ***Disintegrate*** is to disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations (FM 3-0). • Providing information to confirm/deny if friendly actions created the desired effects and met the commander's requirement. • Conducting functional analysis and center of gravity analysis. • Providing intelligence support to targeting. • Providing intelligence support to combat assessment: battle damage assessment, physical damage assessment, and functional damage assessment.

Table 2-12. Operational and intelligence considerations for operational approach (*continued*)

Operational approach	*Operational and intelligence considerations (not all-inclusive)*
Stability mechanisms A *stability mechanism* is the primary method through which friendly forces affect civilians in order to attain conditions that support establishing a lasting, stable peace (ADP 3-0). As with defeat mechanisms, combinations of stability mechanisms produce complementary and reinforcing effects that accomplish the mission more effectively than single mechanisms.	• **Stability mechanisms:** ▪ **Compel** refers to using, or threatening to use, lethal force to establish control and dominance, affect behavioral change, or enforce compliance with mandates, agreements, or civil authority. ▪ **Control** involves imposing civil order. ▪ **Influence** refers to altering the opinions, attitudes, and ultimately the behavior of foreign, friendly, neutral, and threat audiences through messages, presence, and actions. ▪ **Support** establishes, reinforces, or sets the conditions necessary for the instruments of national power to function effectively. • Conducting pre-mission analysis of the operational environment in conjunction with cultural intelligence and civil information. • Performing intelligence preparation of the operational environment. • Using measures of performance and effectiveness to assess operations. • Considering the instruments of national power. • Considering the operational variables and civil considerations.
Risk Commanders accept risk on their own terms to create opportunities and apply judgment to manage those hazards they do not control. Risk is an inherent part of every operation and cannot be avoided. Commanders analyze risk in collaboration with subordinates to assist in determining the risk level and type and how to mitigate the risk. When considering how much risk to accept with a course of action, commanders consider risk to the force against the probability of mission success during current and future operations. They assess options in terms of weighting the main effort, economy of force, and physical loss based on what they have been tasked to do.	• Leaders considering risk across the domains. Accepting risk in one domain may create opportunities in other domains. • G-2/S-2s recommending risk assumptions to friendly forces based on threat forces. • Commanders determining how to impose risk on enemy forces. • Presenting multiple dilemmas and increasing the number and severity of hazards with which enemy forces must contend. • Providing commanders data to assess risk. Intelligence is necessary to assess and assume risk. • Continuous situation development. • Providing intelligence support to protection. • Considering human and information factors that govern how friendly and enemy forces and other relevant actors assess costs and benefits and calculate risk. • Waiting for near-perfect intelligence and synchronization. This may increase risk or close a window of opportunity.

ADP Army doctrine publication FM field manual

STRATEGIC FRAMEWORK

2-94. The strategic framework accounts for factors in the strategic environment and the connection of strategic capabilities to operational- and tactical-level operations. It includes the strategic support area, joint security area, extended deep area, and assigned operational area.

2-95. The strategic framework has importance in terms of joint operations and Army operational-level operations. For most Army operations, understanding the Army operational framework in the context of the strategic framework, is important. (See figure 2-10 on page 2-34). (See FM 3-0, JP 3-0, and JP 3-10.)

OPERATIONAL FRAMEWORK

2-96. An *operational framework* is a cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations (ADP 1-01). Commanders build their operational framework on their assessment of the OE, including all domains and dimensions. They may create new models to fit the circumstances, but they generally apply a combination of common models according to doctrine. The three models commonly used to build an operational framework are—

- Assigned areas.
- Deep, close, and rear operations.
- Main effort, supporting effort, and reserve.

Note. Commanders may use any operational framework model they find useful, but they must remain synchronized with their higher-echelon headquarters' operational framework. (FM 3-0 provides a detailed discussion on each model.)

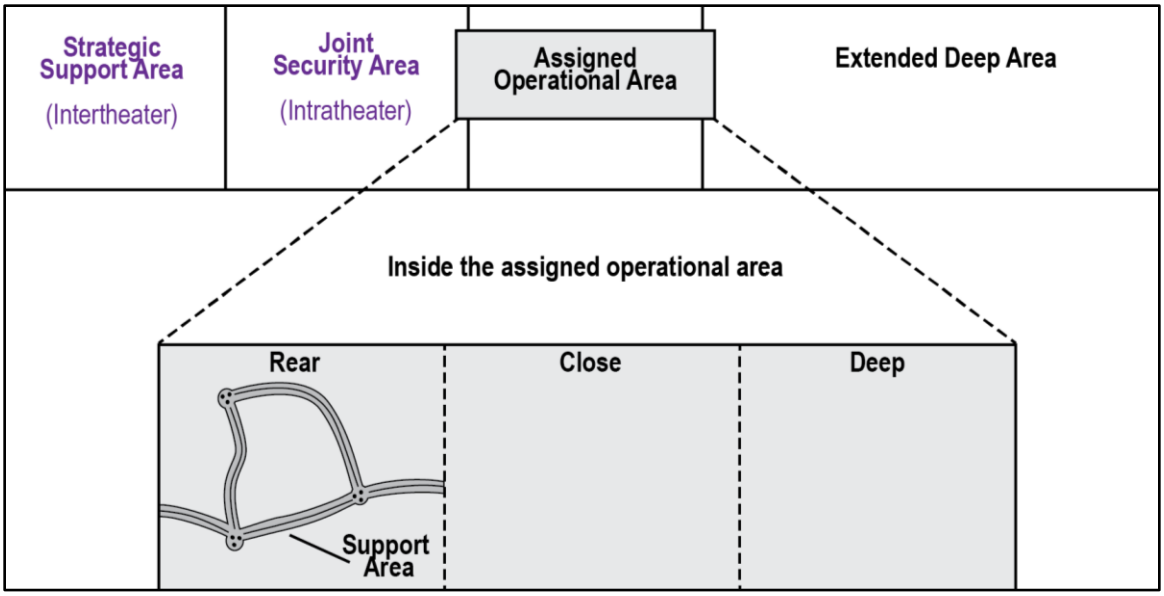


Figure 2-10. The Army operational framework in the context of the strategic framework

2-97. Intelligence professionals must understand and properly use the doctrinal terminology, concepts, and considerations for the operational framework. Table 2-13 lists several intelligence considerations for the three operational framework models.

Table 2-13. Intelligence considerations for operational framework

Operational framework models		*Intelligence considerations (not all-inclusive)*
Assigned areas	An ***area of operations*** is an operational area defined by a commander for the land or maritime force commander to accomplish their missions and protect their forces (JP 3-0).	• Interrelationships of domains and dimensions and associated impacts. • Enemy capabilities in each domain. • Higher-echelon and adjacent-unit information collection capabilities. • Evaluation of time windows for effects to appear within the area of operations. • Intelligence handover lines, as appropriate.
	A ***zone*** is an operational area assigned to a unit in the offense that only has rear and lateral boundaries (FM 3-0).	• Location of NAIs, EAs, and TAIs.
	A ***sector*** is an operational area assigned to a unit in the defense that has read and lateral boundaries and interlocking fires (FM 3-0).	• Location of NAIs, EAs, and TAIs. • Location of friendly battle positions supported by information collection capabilities.
Within assigned areas, commanders organize their operations in time, space, and purpose by synchronizing deep, close, and rear operations. Across all operations, the G-2/S-2 must determine how to support consolidating gains optimally to capitalize on tactical successes.		
Deep operations	***Deep operations*** are tactical actions against enemy forces, typically out of direct contact with friendly forces, intended to shape future close operations and protect rear operations (FM 3-0).	• Synchronizing the intelligence effort with close and rear areas, including the use of intelligence handover lines. • Setting conditions for future close operations. • Targeting and disintegrating enemy structures and systems, including the high-value targets needed for the close fight. • Disrupting enemy freedom of action, coherence, and tempo. • Support to deception. • Support to electromagnetic warfare. • Integrating intelligence between special operations forces and conventional forces.

Table 2-13. Intelligence considerations for operational framework (*continued*)

Operational framework models		*Intelligence considerations (not all-inclusive)*
Close operations	***Close operations*** are tactical actions of subordinate maneuver forces and the forces providing immediate support to them, whose purpose is to employ maneuver and fires to close with and destroy enemy forces (FM 3-0).	• Information collection supporting the maneuver of subordinate formations. • Identifying enemy reserve assets.
Rear operations	***Rear operations*** are tactical actions behind major subordinate maneuver forces that facilitate movement, extend operational reach, and maintain desired tempo (FM 3-0).	• Support to security operations and protection activities. • Identifying bypassed forces. • IPOE, support to protection, and situation development in order to support possible threats to the rear area, for example, enemy special operations forces, air assaults, terrorists, partisan forces, stay-behind forces, air attacks, cyberspace attacks, long-range fires, and chemical attacks.
When supporting the main effort, supporting effort, and the reserve, intelligence synchronization across echelons is critical. The information collection effort must be synchronized across all operations to reduce the possibility of collection gaps.		
Main effort	A ***main effort*** is a designated subordinate unit whose mission at a given point in time is most critical to overall mission success (ADP 3-0).	• Terrain analysis. • Collection assets available. • Threat use of denial and deception. • Location of EAs, NAIs, and TAIs. • Location of enemy counterattack forces and reserve.
Supporting effort	A ***supporting effort*** is a designated subordinate unit with a mission that supports the success of the main effort (ADP 3-0).	• Collection assets available. • Location of enemy counterattack forces and reserve.
Reserve	A ***reserve*** is that portion of a body of troops that is withheld from action at the beginning of an engagement to be available for a decisive movement (ADP 3-90).	• Terrain analysis to determine optimal location for the placement of the reserve to support main and supporting efforts. • Collection assets available before and during commitment. • Location of enemy counterattack forces and reserve. • Positioning of collection assets to exploit main and supporting effort successes.

ADP Army doctrine publication
EA engagement area
FM field manual
IPOE intelligence preparation of the operational environment
JP joint publication
NAI named area of interest
TAI target area of interest

This page intentionally left blank.

Chapter 3
Integrating the Intelligence Warfighting Function

SECTION I – INTEGRATING AND SYNCHRONIZING INTELLIGENCE

3-1. Leadership is the most essential dynamic of combat power, and it is the commander who provides purpose, direction, and motivation to accomplish the mission and improve the unit or organization. Leaders must be able to thoroughly understand the given mission, current situation, and how the OE may impact the mission. Therefore, leaders must integrate and synchronize intelligence into operations. This facilitates understanding an OE and assists in determining when and where to employ capabilities against adversaries and enemies.

3-2. Leaders must provide their formations, including the intelligence warfighting function, direction, guidance, and a sense of purpose. To do this, leaders must be knowledgeable of intelligence fundamentals, the intelligence process, the intelligence warfighting function, intelligence capabilities, the intelligence architecture, and how they can be leveraged to support the operations process.

3-3. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to simultaneously visualize the OE and accomplish the required tasks and activities. The effective use of intelligence capabilities enhances the capability of the combined arms team to create and concentrate combat power and minimize risk.

3-4. The integration and synchronization of the warfighting functions, including the intelligence warfighting function, are important for mission success. While the intelligence warfighting function is somewhat complex, its integration is doctrinally no different than the integration of the other warfighting functions and no less important. Figure 3-1 illustrates the integration of the intelligence warfighting function, accomplished through planning methodologies, integrating processes, and a unit's battle rhythm.

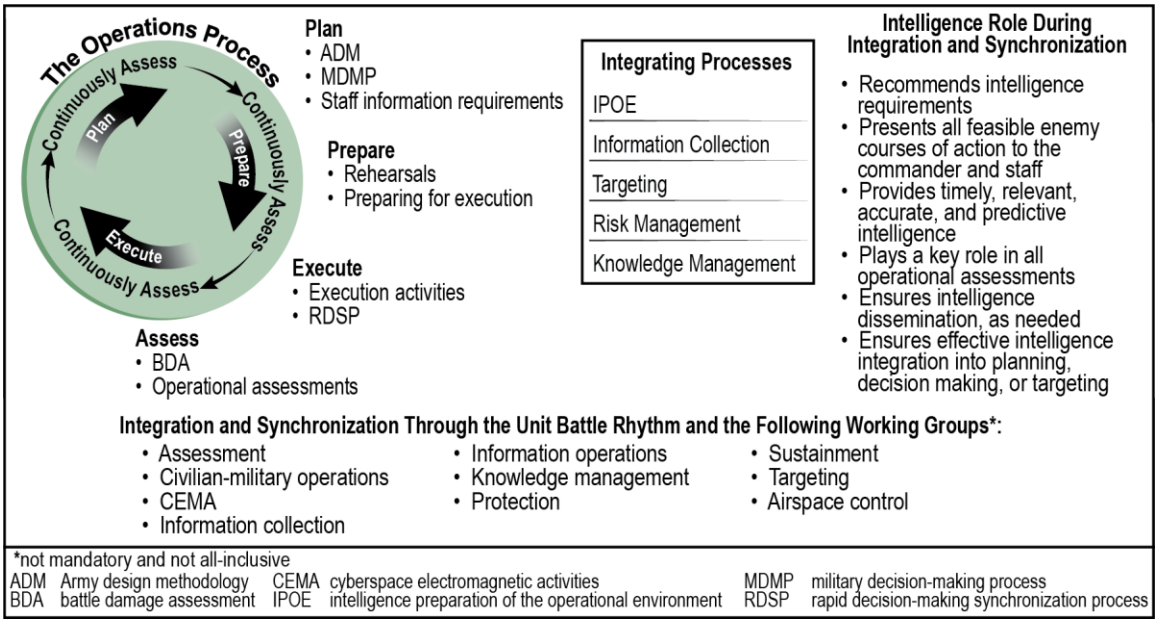


Figure 3-1. Integrating and synchronizing the intelligence warfighting function

SECTION II – THE ROLE OF THE COMMANDER AND STAFF

3-5. *Command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission (JP 1, Volume 2). C2 is fundamental to the art and science of warfare. (See FM 6-0.) No single specialized military function, either by itself or combined with others, has a purpose without it. Commanders are responsible for C2. Through C2, commanders provide purpose and direction to integrate all military activities toward a common goal—mission accomplishment. Staffs support commanders in making and implementing decisions and in integrating and synchronizing combat power. Competent staffs multiply a unit's effectiveness. (See figure 3-2.)

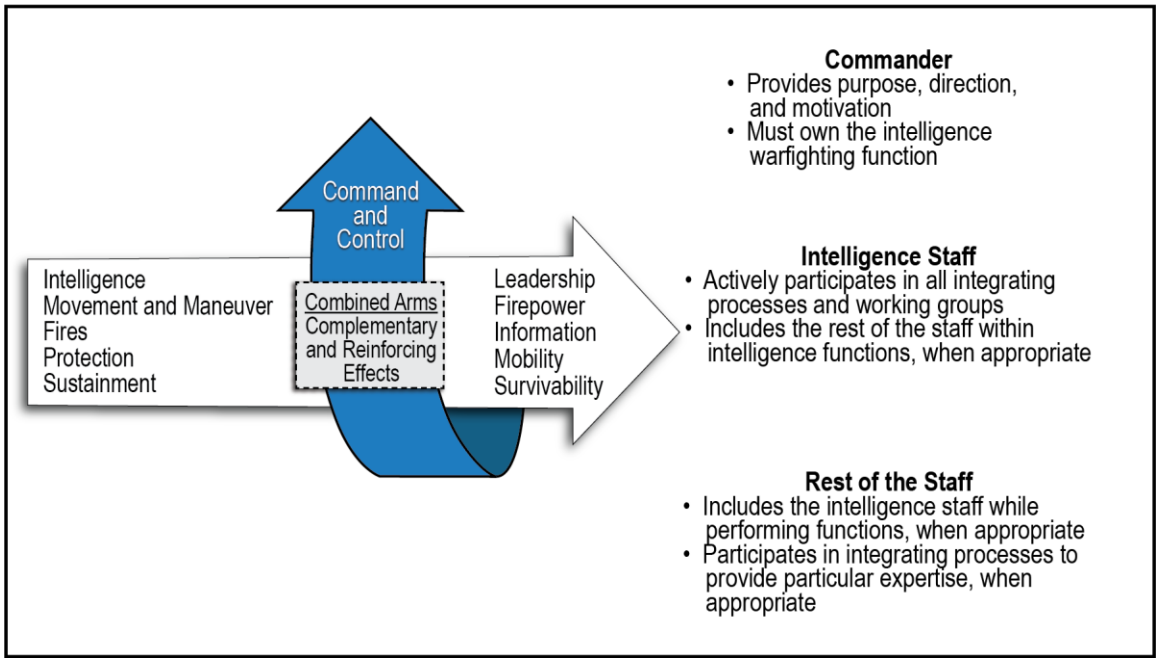


Figure 3-2. Exercising command and control to accomplish the mission

THE COMMANDER

3-6. The commander drives intelligence, intelligence drives operations, and operations must support information collection; this relationship is continuous. Due to the fog and friction of war, including the efforts of determined and adaptive threat forces, commanders must fight for intelligence and then share it across echelons and with adjacent units. The commander, based on recommendations from the intelligence staff, tailors intelligence capabilities and intelligence operations to support the mission. The force-tailoring and specific task organization establish an ordered command and support structure with technical channels for intelligence operations.

3-7. Similar to the relationship with subordinate units and the rest of the staff, commanders provide the intelligence staff guidance and continuous feedback throughout operations (see also figure 3-2) by—

- Providing direction.
- Providing their understanding, visualization, and description of the problem.
- Directing through clearly stated intelligence requirements and priorities.
- Leading and making decisions.
- Continuously assessing the operation through collaboration with the G-2/S-2 during the execution of operations.
- Emphasizing the importance or close cross-staff collaboration, especially with the G-3/S-3, fire support coordinator/chief of fires, and G-6/S-6.

Commander's Critical Information Requirements

A *commander's critical information requirement* is specific information identified by the commander as being essential to facilitate timely decision making (JP 3-0). There are two CCIR categories: PIRs and friendly force information requirements (also called FFIRs). CCIRs directly influence decision making and facilitate the successful execution of operations. As discussed in paragraph 1-34, the intelligence warfighting function focuses on answering intelligence requirements comprising PIRs, targeting intelligence requirements, and other intelligence requirements. The commander approves and prioritizes all intelligence requirements, which drive every aspect of the intelligence process—information collection, including collection management; intelligence PED; intelligence analysis; intelligence production; and dissemination and integration.

3-8. The commander's involvement and interaction enable the intelligence staff to assess how to more effectively produce intelligence to meet the commander's requirements. The commander's involvement also assists the staff in synchronizing the unit's information collection effort with the operation. The commander and staff should also consider some unique aspects of the intelligence warfighting function:

- **Operational uncertainty.** Intelligence does not eliminate uncertainty entirely; to succeed, commanders must take risks.
- **Driving IPOE.** Make it a full staff effort. Focus the staff on those aspects of the OE that are important to the mission (commander's focus and priorities for analysis).
- **Resourcing.** Resource and prioritize the intelligence warfighting function appropriately. For example, adequate network capability and access are critical in meeting the commander's needs.
- **Prioritization.** Prioritize finite resources and capabilities by focusing collection and analysis on key decisions and targeting through intelligence requirements and other means.
- **Continuous collection.** Information collection must be continuous. Start as early in the operations process, as feasible, and effectively transition to the next operation.
- **Tailoring intelligence.** Clearly state what (in terms of priorities, format, and style) is needed across the various intelligence products, especially IPOE products, the intelligence running estimate, and the intelligence portion of the common operational picture (COP).

3-9. Building from this list, table 3-1 provides an extensive list of considerations to assist commanders and staffs in ensuring the intelligence warfighting function is effectively integrated into operations.

Note. Table 3-1 is not intended as a checklist, a set of mandatory actions, or an all-encompassing list of considerations.

Table 3-1. Commander and staff considerations

An effective staff team. Build the team and foster a collaborative environment that encourages critical thinking, candor, and cooperation.
Risk. Accept necessary risks and some operational uncertainty. Intelligence cannot eliminate uncertainty. Commanders determine the necessary risks inherent in any operation.
Guidance. Broadly and clearly share the commander's guidance and visualization of the operation and the OE. Ensure the right aspects of the domains and dimensions are accounted for in the operational variables and the mission variables.
Driving IPOE. Initial guidance, key participation, and periodic oversight are extremely valuable in ensuring a thorough IPOE.
Owning intelligence requirements. Personally engage in developing and approving intelligence requirements that drive operations and targeting.
Enabling information collection. In nondoctrinal terms, information collection is the *fight before the fight*. Demand effective collaboration between the G-3/S-3, G-2/S-2, and rest of the staff to plan and control information collection. Allocate maneuver, fires, and other capabilities to enable information collection and intelligence analysis and production, when necessary. Resource the reconnaissance and surveillance network and intelligence operations sufficiently, to include providing adequate network capability (for example, relays, bandwidth, and access).
Maximizing collection. Facilitate detailed planning on the use of organic, assigned, and attached collection, PED, and processing capabilities such that they can be thought of as information collection pacing items. It is also important to fully leverage supporting collection assets, external PED and analysis, and intelligence from national-level and allied and partner intelligence organizations.

Table 3-1. Commander and staff considerations (*continued*)

Allocating adequate time for information collection and intelligence analysis. Sometimes, operational necessity dictates timelines. However, sometimes, it is worth the time (tactical patience) to allow for thorough information collection, analysis, and the production of effective intelligence products.
Owning the intelligence architecture. Emphasize its importance and facilitate teamwork between the G-3/S-3, G-2/S-2, G-6/S-6, G-9/S-9, CEMA officer, space operations officer, and other staff members. An effective intelligence architecture is crucial. The architecture connects *each intelligence capability* from national and multinational partner, joint, and higher-level Army echelons as well as from organic and supporting intelligence collection, intelligence PED, and all-source capabilities across the area of operations, including all command posts.
The common operational picture and intelligence products. Provide clear guidance to the G-2/S-2 on the intent and standard for maintaining the threat portion of the common operational picture and the expectation for answering intelligence requirements.
Sharing with allied and partner forces. Ensure the intelligence staff completes information sharing coordination before the operation and shares appropriately throughout the entire operation.
Prioritizing battle damage assessment. Prioritize the battle damage assessment effort and ensure a thorough staff analysis is completed for battle damage assessment.
Guiding transitions. Transitions can be very tricky for the intelligence warfighting function. Early and clear guidance is integral to effectively transitioning the intelligence warfighting function.

CEMA	cyberspace electromagnetic activities	IPOE	intelligence preparation of the operational environment
G-2/S-2	division or corps/battalion or brigade intelligence staff officer	PED	processing, exploitation, and dissemination
G-3/S-3	division or corps/battalion or brigade operations staff officer	OE	operational environment
G-6/S-6	division or corps/battalion or brigade signal staff officer		
G-9/S-9	division or corps/battalion or brigade civil affairs operations staff officer		

THE STAFF

3-10. This general discussion focuses on the staff and its participation in the intelligence warfighting function. Chapter 5 discusses intelligence staff activities. The staff is a key component of the C2 warfighting function. In addition to executing its specialized staff tasks, the staff's primary responsibilities include supporting the commander; assisting subordinate commanders, staffs, and units; and informing units and organizations outside the headquarters.

SUPPORTING THE COMMANDER

3-11. Staffs support the commander in understanding, visualizing, and describing the OE; making and articulating decisions; and directing, leading, and assessing military operations. Staffs also support the commander by—

- Making recommendations and preparing plans and orders for the commander.
- Producing timely and relevant information and analysis and using knowledge management to extract that information from the vast amount of available information.
- Battle tracking the ongoing operation to ensure information collection tasks are executed or adjusted as the situation dictates.
- Seeing and understanding when windows of opportunity to achieve a relative advantage open and close, and by alerting and providing recommendations to the commander when decision criteria are met.
- Monitoring and providing recommendations to adjust the plan or tasks when the situation changes and the anticipated decisions are no longer relevant.

PARTICIPATING IN THE INTELLIGENCE WARFIGHTING FUNCTION

3-12. The entire staff is part of the intelligence warfighting function. The rest of the staff (other than the intelligence staff) has the same obligation to participate in key intelligence processes, meetings, and working groups just as the intelligence staff is obligated to fully engage in other warfighting function processes, meetings, and working groups.

3-13. The intelligence staff cannot be experts in all aspects of the OE and threat capabilities. Staff members must know certain aspects of the OE and threat capabilities related to their warfighting function or specialty. Important activities require the entire staff to participate; this ensures the intelligence warfighting function—

- Facilitates a real understanding of the many important aspects of the OE (especially when, where, and how the threat will employ capabilities).
- Assists the commander and staff's visualization.
- Supports in developing friendly COAs and recommending the best COA to the commander.
- Assists in synchronizing combat power within the operation.
- Supports targeting (through lethal and nonlethal means).

3-14. Some of the most important intelligence processes and activities requiring the rest of the staff's participation, discussed in section III, includes—

- IPOE, led by the intelligence staff, especially initial IPOE during step 2 (mission analysis) of the MDMP.
- Collection management (the basis for information collection planning), led by the intelligence staff, and information collection processes.
- Any intelligence working groups, if held.
- The information collection working group, if held.

SECTION III – STAFF TEAMWORK

3-15. Teamwork within a staff and between staffs produces the staff integration necessary to synchronize operations. A staff works efficiently with complete cooperation from all staff sections. In addition to being highly knowledgeable in their own fields, operations processes, and procedures, all staff members must be familiar with the duties and responsibilities of other staff sections to coordinate and achieve results for the commander. A force operates effectively in cooperation with all headquarters. Commanders and staffs contribute to foster this positive climate during training and sustain it during operations. However, frequent personnel changes and augmentations to their headquarters add challenges to building and maintaining a team. While all staff sections have clearly defined functional responsibilities, none can operate effectively in isolation; therefore, coordination is critical. Commanders ensure staff sections are properly equipped and manned. This allows staffs to efficiently work within their headquarters and with their counterparts in other headquarters. Commanders ensure staff integration by developing the unit's battle rhythm, to include synchronizing various meetings, working groups, and boards.

3-16. Staff teamwork works in both directions. The intelligence staff must fully participate in and bring its unique perspectives, knowledge, and expertise to support the rest of the staff across the planning methodologies, integrating processes, working groups, and other staff functions. Conversely, the same is true of the rest of the staff supporting intelligence processes; tasks; working groups, if established; and functions. It is important to remember that the commander and staff are part of the intelligence warfighting function. Some of the support provided by the rest of the staff to the intelligence staff includes—

- Sharing unique perspectives, knowledge, and expertise with the intelligence staff at key times within certain intelligence tasks.
- Supporting ancillary and specialized information collection capabilities (see paragraph 3-35) and intelligence-related missions and operations (see paragraph 3-41).

3-17. Certain intelligence tasks are far more effective when the rest of staff, especially key members, participates with the intelligence staff at key times in certain intelligence tasks. The value of staff participation applies primarily to IPOE and collection management; it also applies to a lesser extent to pre-mission analysis of the OE, situation development, intelligence support to targeting, and support to operational assessments. Staff members contribute warfighting function/specialty knowledge and expertise as well as perspectives that differ from the intelligence staff's—all of which are invaluable. This comprehensive staff participation is similar to the staff participation necessary to adequately conduct targeting, support protection, or any number of other staff tasks. Despite pervasive time constraints that hinder participation in key intelligence tasks, the lack of staff participation during initial IPOE, mission analysis, or collection management puts a unit's mission at risk.

3-18. Table 3-2 lists those staff members whose contributions to key intelligence tasks enable the effectiveness of the intelligence warfighting function. The list is not all-inclusive; staff members vary based on the echelon and specific unit.

Table 3-2. Staff support to the intelligence warfighting function

Staff section	*IPOE, situation development, and intelligence support to targeting input*	*Collection management participation*
All staff sections: Provide subject matter expertise to assist the intelligence staff in the following tasks.	• Based on staff expertise, assist the intelligence staff in analyzing and developing— ▪ Modified combined obstacle overlays. ▪ Civil considerations products. ▪ Threat objectives and the desired end state. ▪ NAIs. ▪ High-value targets, which become high-payoff targets. ▪ Possible threat decision points. • Assist the intelligence staff in deciding what key aspects to add to the intelligence portion of the common operational picture and intelligence running estimate.	• Based on staff expertise, develop information requirements, as needed; assist the collection management team in— ▪ Developing or refining indicators and SIRs. ▪ Matching collection assets to SIRs. ▪ Developing NAIs and active time. ▪ Planning the use of technical collection, biometric, forensic, and document and media exploitation capabilities. ▪ Planning the use of ancillary collection assets from associated warfighting function or specialty knowledge. • Assist the G-3/S-3 in developing the final Annex L (Information Collection).
G-3/S-3: Provides subject matter expertise on the art and science of military operations, including reconnaissance, surveillance, and security operations. Evaluates IPOE products to ensure they support friendly COA development and analysis. Plans and directs information collection based on collection management.	• Provides operational experience. • Assists in determining— ▪ Friendly and enemy TAIs. ▪ Friendly and enemy engagement areas. ▪ Enemy time phase lines. • Assists the entire staff in determining how the threat might integrate and synchronize its operations. • Develops threat C2 models, intent, vulnerabilities, and templating. • Provides threat reconnaissance, surveillance, and security operations models; intent; vulnerabilities; and templating. • Provides threat maneuver unit models, intent, vulnerabilities, and templating. • Assists the staff in developing relative combat power matrices for friendly and enemy forces.	• Develops threat C2 indicators, SIRs, and NAIs. • Develops threat reconnaissance, surveillance, and security operations indicators, SIRs, and NAIs. • Develops threat maneuver unit indicators, SIRs, and NAIs. • Refines— ▪ Friendly TAIs. ▪ Friendly engagement areas. ▪ Enemy time phase lines. • Effectively integrates and synchronizes (feasible and supported) reconnaissance, surveillance, and security operations into the collection management plan.
G-4/S-4: Provides subject matter expertise on sustainment operations.	• Provides threat logistics models, intent, vulnerabilities, and templating. • Templates threat supply/resupply routes/points. ***Note.*** Threat logistic activities and lack of activities can be a good indicator of threat intent and future threat operations/COAs.	• Develops threat logistics and supply/resupply indicators, SIRs, and NAIs. • Conducts logistics planning for technical collection and document and media exploitation.
G-6/S-6: Provides subject matter expertise on friendly communications systems and assists the G-2/S-2 in identifying and evaluating friendly communications systems' vulnerabilities to cyberspace and electromagnetic attack.	• Provides threat communications systems models, intent, vulnerabilities, and templating, including networks and nodes. • Conducts line-of-sight analysis.	Develops threat communications systems indicators, SIRs, and NAIs.

Table 3-2. Staff support to the intelligence warfighting function (*continued*)

Staff section	*IPOE, situation development, and intelligence support to targeting input*	*Collection management participation*
G-9/S-9: Provides subject matter expertise on civil affairs operations.	• Integrates civil knowledge gained from unified action partners working with indigenous populations and institutions. • Conducts ASCOPE (areas, structures, capabilities, organizations, people, and events) analysis. • Conducts PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time) analysis. • Provides civil considerations overlays with critical civilian infrastructure status and capabilities, and areas of cultural significance (protected targets). • In collaboration with unified action partners and the staff judge advocate, identifies restricted fires requirements (persons and places) for the commander. ***Note.*** Refugees, displaced persons, and evacuees can have a major impact on friendly and threat operations.	• Develops civil considerations and local population attitudes, "atmospherics," indicators, SIRs, and NAIs. • Determines the local population's impact on information collection. • Recommends the use of developed and engaged civil network as part of collection. • Manages the civil information collection plan. • Directs civil reconnaissance, civil engagement, and civil network development within the operational area.
Chief of fires/Deputy fires support coordinator/Fires support officer: Provides subject matter expertise on fires.	• Provides threat fires capabilities, models, intent, vulnerabilities, and templating. • Assists in determining— ▪ Friendly TAIs. ▪ Friendly electromagnetic attack. ▪ Enemy time phase lines.	• Develops threat fires indicators, SIRs, and NAIs. • Shares the high-payoff target list, target synchronization matrix, attack guidance matrix, and target selection standards. • Ensures incorporation of counterfire/counterbattery radar systems in the collection management plan. • Refines friendly TAIs.
Chief of protection: Provides subject matter expertise on all aspects of the protection warfighting function.	• Performs checks and balances between IPOE, subsequent operational planning, and collection management to account for all aspects of protection. • Provides threat rear-area capabilities, models, intent, vulnerabilities, and templating. In this situation, threat rear-area capabilities are threat capabilities, units, and systems that could be used in the friendly rear area to disrupt friendly operations. These threat capabilities can include terrorists, bypassed forces, stay-behind forces, special purpose forces, or many other threats to the friendly rear area.	• Develops threat rear-area capabilities indicators, SIRs, and NAIs. • Plans biometric and forensic capabilities and identity activities as part of collection management. • Shares the friendly critical and defended asset lists.
Air and missile defense officer: Provides subject matter expertise on ADA and assists the G-2/S-2 in determining the locations of ADA assets and potential areas of employment.	• Provides threat ADA models, intent, vulnerabilities, and templating. • Determines threat air avenues of approach. • Identifies threat missile capabilities and flight characteristics.	Develops threat ADA indicators, SIRs, and NAIs.
Air LNO (senior member of the tactical air control party): Provides subject matter expertise on air and space capabilities and limitations as well as applies and integrates joint capabilities to generate multidomain effects throughout an OE in direct support of the ground commander's intent and guidance.	• Provides threat close air support capabilities models, intent, vulnerabilities, and templating. • Provides access to Air Force intelligence products.	• Develops threat close air support indicators, SIRs, and NAIs. • Shares airspace control orders, restricted operations zones, and aerial ISR taskings. • Operates and maintains the joint air request net. • Advises the staff on preparing air support requests. • Transmits requests for ISR support.

Table 3-2. Staff support to the intelligence warfighting function (*continued*)

Staff section	*IPOE, situation development and intelligence support to targeting input*	*Collection management participation*
Aviation officer: Provides subject matter expertise on Army aviation assets and operations, ranging from attack aviation, lift, UASs, and fixed-wing assets at the theater army, corps, division, and brigade levels.	Provides threat attack helicopter, air assault, and UAS (including UAS *swarms*) capabilities, models, intent, vulnerabilities, and templating.	Develops threat attack helicopter, air assault, and UAS (including UAS *swarms*) indicators, SIRs, and NAIs.
Engineer officer: Provides subject matter expertise on mobility/countermobility and assists the G-2/S-2 in developing enemy obstacle plans for the enemy situation template.	• Provides threat engineer models, intent, vulnerabilities, and templating, including obstacle locations and mobility systems. • Conducts terrain analysis and assists in determining— ▪ Mobility corridors. ▪ Military aspects of terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment [also called OAKOC]) factors.	Develops threat engineer indicators, SIRs, and NAIs.
CBRN officer: Provides subject matter expertise on CBRN and assists the G-2/S-2 in determining the locations of CBRN assets and potential areas of employment.	• Provides threat CBRN capabilities, models, intent, vulnerabilities, and templating. • Provides threat triggers for using CBRN. • Provides threat CBRN terrain and weather considerations.	Develops threat CBRN indicators, SIRs, and NAIs.
CEMA section: Provides subject matter expertise on information pertaining to doctrine, tactics, and equipment of enemy cyberspace and EW forces, and access to cyberspace and EW capabilities for information collection.	• Provides threat cyberspace and EW models, intent, vulnerabilities, and templating. • Copartners to develop and maintain the enemy electromagnetic order of battle.	• Develops threat cyberspace and EW indicators, SIRs, and NAIs. • Plans friendly cyberspace and EW operations collection requirements.
CEMA officer: Provides subject matter expertise on ground-based, airborne, and functional EW employment considerations.	• Provides threat EW models, intent, vulnerabilities, and templating. • Conducts line-of-sight analysis.	• Develops threat EW indicators, SIRs, and NAIs. • Plans friendly EW capabilities collection.
Explosive ordnance disposal officer: Provides subject matter expertise on the detection, identification, recovery, evaluation, rendering safe, and final disposal of explosive ordnance.	Provides threat explosive ordnance (including improvised explosive devices) models, intent, vulnerabilities, and templating.	• Develops threat explosive ordnance (including improvised explosive devices) indicators, SIRs, and NAIs. • Plans foreign ordnance and weapons technical intelligence collection, when needed.
Information operations officer: Provides subject matter expertise on shaping operational activities in and through the information dimension.	• Provides threat information warfare models, intent, vulnerabilities, and templating. • Predicts threat themes and messaging in conjunction with the intelligence staff. • Provides information overlays.	• Develops threat information warfare indicators, SIRs, and NAIs. • Assists the collection management team in accounting for the information dimension, when needed.
Military deception officer: Provides subject matter expertise on coordinating military deception assets and operations and influencing enemy decision makers.	Provides threat deception models, intent, vulnerabilities, and templating.	• Develops threat deception indicators, SIRs, and NAIs. • Assists the collection management team in accounting for the information dimension, when needed.
Operations security officer: Provides subject matter expertise on the development, organization, and administration of an operations security program.	Provides threat collection models, intent, vulnerabilities, and templating, in coordination with counterintelligence personnel.	• Develops threat collection indicators, SIRs, and NAIs, in coordination with counterintelligence personnel. • Assists the collection management team in accounting for the information dimension, when needed. • Shares essential elements of friendly information.
Psychological operations officer: Provides subject matter expertise on synchronizing MISO support to operations.	Provides threat psychological operations models, intent, vulnerabilities, and templating.	• Develops threat psychological operations indicators, SIRs, and NAIs. • Assists the collection management team in accounting for the information dimension, when needed.

Table 3-2. Staff support to the intelligence warfighting function (*continued*)

Staff section	*IPOE, situation development and intelligence support to targeting input*	*Collection management participation*
Space operations officer: Provides subject matter expertise on the space domain and adversary space/counterspace capabilities and effects within the OE.	• Provides threat space models, intent, vulnerabilities, and templating. • Provides space weather effects on operations. • Provides threat counterspace capabilities, characteristics, and employment.	• Develops threat space indicators, SIRs, and NAIs. • Provides space weather effects on operations.
Staff judge advocate: Provides subject matter expertise on all types of legal matters and provides support and advice to the commander and staff.	Provides legal considerations to minimize unnecessary collateral damage or injury to the civilian population.	Provides legal considerations to minimize unnecessary collateral damage or injury to the civilian population.
Command surgeon or medical support officer: Provides subject matter expertise on all medical or medical-related matters and provides support and advice to the commander and staff.	• Identifies health threats faced by friendly and enemy forces (injuries, diseases, environmental, weapons effects, physiologic and psychological stressors). • Provides details on the local population's medical care and health factors, including— ▪ Changes to access for medical care. ▪ Sanitation issue. ▪ Portable water supply. ▪ Effects of significant health factors, for example, insects, diseases, and other issues.	• Develops SIRs, NAIs, and indicators related to host nation medical facilities. • Develops SIRs, NAIs, and indicators related to medical-health threats. • Provides medical evacuation procedures and methods.
Chaplain: Provides religious, moral, and ethical advisement to the commander and staff in areas that potentially impact the unit both externally and internally. ***Note.*** Chaplains and unit ministry teams do not collect information that would violate their status as noncombatants.	• Produces a religious area analysis and subsequently a religious impact assessment. • Provides religious demographics, time (specific holidays or time of day), and practices. • Conducts *sacred sites* analysis (with the staff judge advocate) and determine religious impact on operations.	Develops SIRs, NAIs, and indicators related to religious factors (religious, human, and ideological) of the OE.
LNO: Provides subject matter expertise from its assigned headquarters. ***Note.*** This only occurs when the LNO is authorized security access to the IPOE and collection management processes.	• Promotes coordination, synchronization, and cooperation among its parent unit and higher-echelon headquarters and interagency, coalition, host-nation, adjacent, and subordinate organizations, as required. • Coordinates face-to-face, which is invaluable to sharing a different perspective on IPOE and IPOE products.	Coordinates face-to-face, which is invaluable to sharing various collection details.

ADA	air defense artillery	IPOE	intelligence preparation of the operational environment
C2	command and control	ISR	intelligence, surveillance, and reconnaissance
CBRN	chemical, biological, radiological, and nuclear	LNO	liaison officer
CEMA	cyberspace electromagnetic activities	MISO	military information support operations
COA	course of action	NAI	named area of interest
EW	electromagnetic warfare	OE	operational environment
G-2/S-2	division or corps/battalion or brigade intelligence staff officer	SIR	specific information requirement
G-3/S-3	division or corps/battalion or brigade operations staff officer	TAI	target area of interest
G-4/S-4	division or corps/battalion or brigade logistics staff officer	UAS	unmanned aircraft system
G-6/S-6	division or corps/battalion or brigade signal staff officer		
G-9/S-9	division or corps/battalion or brigade civil affairs operations staff officer		

SECTION IV – THE OPERATIONS PROCESS AND INTELLIGENCE

3-19. Commanders employ the operations process to incorporate coalition and joint partners, empower subordinate initiative, and ensure authorities and risk acceptance are delegated to the appropriate echelon for the situation. Staffs and subordinate headquarters earn the commander's trust by providing relevant information, anticipating needs, and directing supporting actions. Close interaction between the commander and the G-2/S-2 and the other staff is essential as the staff supports unit planning and preparation. Commanders direct the intelligence warfighting function through their relationship with the G-2/S-2, the rest of the intelligence staff, and the MI unit commander.

3-20. As shown in figure 3-3, the major activities of the operations process are—

- **Plan.** Planning normally begins upon receipt of orders from a higher-echelon headquarters and continues through the execution of the operation.
- **Prepare.** Commanders, assisted by their chiefs of staff or executive officers, drive the preparation for an operation by allocating time, prioritizing resources, and supervising preparation activities, such as rehearsals, to ensure their forces are ready to execute operations.
- **Execute.** During execution, commanders and staffs focus their efforts on translating plans into direct action to achieve objectives in accordance with the higher commander's intent.
- **Continuously assess.** The commander and staff continually assess operations and revise the plan through fragmentary orders (FRAGORDs).

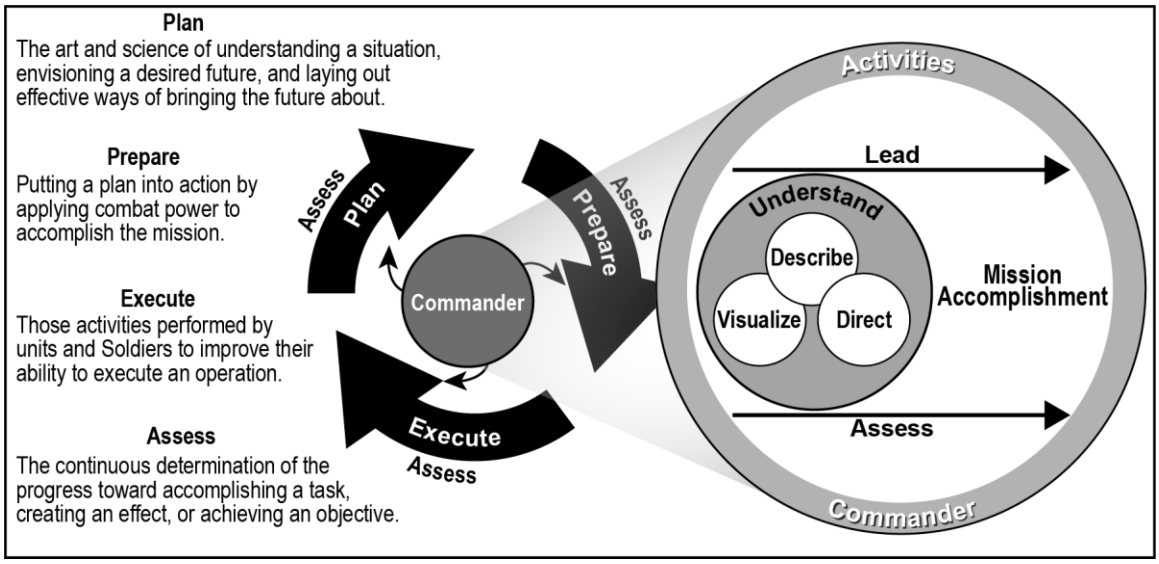


Figure 3-3. The operations process

ARMY PLANNING METHODOLOGIES

3-21. Integrated planning—from conceptual to detailed planning—is critical to Army operations. Planning requires the integration of both conceptual thinking and detailed analysis. Army leaders employ several methodologies for planning, determining the appropriate mix based on the scope and understanding of the problem, time available, and availability of a staff. The Army planning methodologies, detailed in FM 5-0, include—

- Army problem solving.
- ADM.
- The MDMP.
- Rapid decision-making and synchronization process (RDSP).
- Troop leading procedures (TLP).

3-22. Perfect knowledge and assumptions about the future do not occur. The commander and staff cannot predict with precision how enemies will react or how other actors will respond during operations. Nonetheless, the understanding and learning that occur during planning are valuable. Even if units do not execute the plan exactly as envisioned, planning results in an improved understanding of the situation that facilitates future decision making. Planning and plans assist leaders in—

- Building situational understanding.
- Identifying and developing solutions to problems.
- Understanding, describing, and accepting risk.
- Directing, coordinating, and synchronizing action.
- Task-organizing the force and prioritizing efforts.
- Anticipating events.

3-23. The intelligence staff has a critical role in all activities of the operations process, especially in planning and the integrating processes (see section V). The G-2/S-2 supports the commander's ability to understand the OE and visualize operations by—

- Leading the IPOE process and portraying the enemy and other relevant aspects of the OE throughout the MDMP.
- Developing the information collection plan (in coordination with the G-3/S-3).
- Producing the intelligence portion of the COP.
- Updating the intelligence running estimate.
- Developing other intelligence products and reports.

INTELLIGENCE SUPPORT TO THE MILITARY DECISION-MAKING PROCESS

3-24. Although the five Army planning methodologies are important, the MDMP is the one most often applied from theater army to BCT levels during armed conflict. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The MDMP begins with the receipt of the mission and combines the conceptual and detailed components of planning. Commanders use the MDMP to visualize the OE and the threat, build plans and orders for extended operations, and develop orders for short-term operations within the framework of a long-range plan. (See FM 5-0.)

3-25. During the MDMP, the intelligence staff leads the IPOE effort and provides all-source intelligence products and tools. Besides IPOE, the intelligence staff uses products developed during pre-mission analysis of the OE and begins to develop some of the early intelligence support to targeting and collection management products and tools. The staff tailors the all-source intelligence products and tools to the commander's requirements, the situation, and the mission. The commander and staff require the following products throughout planning:

- Line of communications overlays.
- Broadcast and communications networks.
- Combined information overlays.
- Electromagnetic orders of battle.
- Hazards overlays (that accurately depict the affected areas).
- Modified combined obstacle overlays (also called MCOOs) and terrain effects matrices.
- Weather trends and current and forecasted weather effects on friendly and enemy capabilities.
- Weather effects matrices and other weather tactical decision aids.
- Civil considerations overlays (addressing factors such as demographics, political alignments, religions and sects, network diagrams, and link and node overlays).
- Threat characteristics.
- Threat models.
- Broad set of possible threat COAs.

- Threat situation templates (covering at least the most likely and most dangerous threat COAs).
- Event templates and matrices.
- Other relevant threat and civil consideration templates.
- Analysis of threat systems products.
- High-value target (HVT) lists, which facilitate or are used to develop high-payoff target lists (HPTLs).
- Target value analysis and other intelligence support to targeting products.

Note. Possible products are limited only by the intelligence staff's initiative and creativity as balanced against time available.

3-26. Table 3-3 outlines intelligence support to the MDMP.

Table 3-3. Intelligence support to the military decision-making process

Step 1—Receipt of mission	*Intelligence support to step 1*
• Alert the staff and other key participants. • Gather the tools. • Update running estimates. • Conduct the initial assessment. • Issue the commander's initial guidance. • Issue the initial WARNORD.	• Begin parallel planning and collaborate with higher, lower, and adjacent intelligence organizations to facilitate the IPOE process. • Focus activities on the mission variables. • Identify gaps in intelligence holdings. • Use intelligence reach to collect updated or additional enemy, terrain and weather, and civil considerations data. • In coordination with the Air Force staff weather officer, update the weather estimate. • In coordination with the cyberspace electromagnetic warfare officer and CEMA section, update the effects of the EMS and cyberspace domain, including information from products that portray the physical network and logical network layers. • Coordinate with the G-3/S-3, G-6/S-6, and the CEMA section to address the information dimension and cyberspace domain. When feasible, coordinate with the JFC information planning cell. • Develop and submit initial requests for information based on intelligence gaps. • Work with the operations staff to initiate the movement of collection assets, as needed, to position them for future collection. • If needed, work with the operations staff to revise ongoing information collection or initiate limited preliminary information collection, which is published as Annex L (Information Collection) to WARNORD #1. • Continually update target packets and the enemy situation. • Update the intelligence running estimate.
Step 2—Mission analysis	***Intelligence support to step 2***
• Analyze the higher headquarters' plan or order. • Perform initial IPOE. • Determine specified, implied, and essential tasks. • Review available assets and identify resource shortfalls. • Determine constraints. • Identify critical facts and develop assumptions. • Begin a risk assessment. • Develop initial CCIRs and EEFIs. • Develop the initial information collection plan. • Update plan for the use of available time. • Develop initial themes and messages. • Develop a proposed problem statement. • Develop a proposed mission statement. • Present the mission analysis briefing. • Develop and issue the initial commander's intent. • Develop and issue initial planning guidance. • Develop COA evaluation criteria. • Issue a WARNORD.	• Identify gaps in the higher headquarters information collection plan and IPOE. • Lead the staff through the IPOE process. Consolidate the staff's IPOE products into a set of coherent and holistic IPOE products. • Begin collection management by identifying specified and implied intelligence tasks from the higher headquarters order. • Develop the initial collection management plan and support the initial information collection plan (WARNORD, fragmentary order, or OPORD). • Use pertinent intelligence from higher echelons. • Assist in determining the area of operations and area of interest. • Develop initial information requirements (with staff). • In coordination with the G-3/S-3, recommend initial PIRs to the commander. • Assist in developing initial operations security vulnerabilities and EEFIs. • Include weather (which includes space) and EMS effects on the enemy's warfighting function capabilities. • Include key considerations for threat cyberspace operations, including the identification of key aspects of the cyberspace domain.

Table 3-3. Intelligence support to the military decision-making process (*continued*)

Step 2—Mission analysis	*Intelligence support to step 2 (continued)*
• Analyze the higher headquarters' plan or order. • Perform initial IPOE. • Determine specified, implied, and essential tasks. • Review available assets and identify resource shortfalls. • Determine constraints. • Identify critical facts and develop assumptions. • Begin a risk assessment. • Develop initial CCIRs and EEFIs. • Develop the initial information collection plan. • Update plan for the use of available time. • Develop initial themes and messages. • Develop a proposed problem statement. • Develop a proposed mission statement. • Present the mission analysis briefing. • Develop and issue the initial commander's intent. • Develop and issue initial planning guidance. • Develop COA evaluation criteria. • Issue a WARNORD.	**MCOO and terrain (with engineer officer):** Does the overlay— • Identify restricted or severely restricted terrain? • Identify mobility corridors (air and ground)? • Identify infiltration lanes and landing and pickup zones? • Identify key or decisive terrain? • Define defensible terrain? • Identify terrain that supports survival and evasion of personnel executing their isolated Soldier guidance? • Identify aspects within the information dimension (and their interrelationship with the human dimension), such as communications means and networks (telephone networks [landline, cellular, satellite, and voice over internet protocol]; internet; radio; television; newspapers and other printed material; social media; cyber cafes; threat and neutral narratives; threat and neutral actor vulnerabilities to information advantage activities; and friendly vulnerabilities to threat information warfare activities). **Situation templates:** Do the situation templates— • Include all committed and reinforcing forces as well as combat multipliers? • Focus at least two levels down in detail (or as command dictates), including all threat warfighting functions? • Graphically portray threat characteristics, vulnerabilities and peculiarities, activities, and capabilities for each COA? • **Event templates and matrices (unrefined):** Do the event templates identify and focus on NAIs, time phase lines, time distance analysis, critical actions, or threat DPs?
Step 3—COA development	***Intelligence support to step 3***
• Assess relative combat power. • Generate options. • Array forces. • Develop a broad concept. • Assign headquarters. • Develop COA statements and sketches. • Conduct COA briefing. • Select or modify COAs for continued analysis.	• Ensure IPOE products are deliberately integrated into COA development. Critical products include the MCOO, civil considerations products, threat objectives, threat models (including HVTs), situation templates, and event templates. • Integrate information and intelligence received from the initial information collection effort. • Ensure weather and EMS effects on the warfighting function capabilities are deliberately integrated into COA development. • Refine and prioritize situation templates, event templates, and matrices. • Update HVTs for targeting by lethal and nonlethal methods. • Take an active part in analyzing combat power by providing all available information on current threat forces and the situation. • Provide information on threat vulnerabilities while analyzing relative combat power. • Consider as many possible COAs as time permits, starting with the most likely and including the worst case (most dangerous).
Step 4—COA analysis (war game)	***Intelligence support to step 4***
• Gather the tools. • List all friendly forces. • List assumptions. • List known critical events and DPs. • Select the war-gaming method. • Select a technique to record and display results. • War-game the operations and assess the results. • Conduct a war-game briefing (optional).	**As the enemy commander—** • Use the enemy situation template as a starting point and the event template and matrix as guides to develop critical enemy DPs in relation to friendly COAs. • Project enemy reactions to friendly actions and project enemy losses. • Capture the results of each enemy action and counteraction as well as corresponding friendly and enemy strengths and vulnerabilities. **As the command's senior intelligence officer—** • Identify new information requirements. • Recommend PIRs that correspond to DPs and refine PIRs with the LTIOV. • Redefine enemy COAs based on developed DPs and the situation template. • Develop critical enemy DPs in relation to friendly COAs. • Fight as an uncooperative enemy to develop DPs and project enemy losses. • Address all relevant enemy activities. • Assist in developing target selection standards and the attack guidance matrix from war-gamed COAs. • Recommend changes to the information collection plan. • Based on the war game, refine the situation and event templates with corresponding DPs, TAIs, and HVTs, including NAIs. • Refine the event matrix with TAIs and HVTs. • Participate in the targeting process. • Link NAIs to TAIs. • Display the scheme of information collection during the war game. • Assists the G-3/S-3 in developing the decision support template. • Consider the effects of enemy and friendly COAs on local population attitudes and behaviors.

Table 3-3. Intelligence support to the military decision-making process (*continued*)

Step 5—COA comparison	*Intelligence support to step 5*
• Conduct analysis of advantages and disadvantages. • Compare COAs. • Conduct a COA decision briefing.	• Ensure incorporation of the recommended PIRs in the tasking of subordinate units and the requests to higher and lateral echelons. • Coordinate with supporting information collection organizations and G-2/S-2s to ensure the information collection plan is understandable and executable. When executed, the plan should enable a rapid and seamless transition between current and future operations. • Modify the initial set of intelligence requirements developed during mission analysis to reflect war-gaming results. • Include weather and EMS effects on specific warfighting function capabilities' analysis of advantages and disadvantages for each COA. • Clearly delineate intelligence requirements. • Ensure the synchronization of all available collection assets.
Step 6—COA approval	*Intelligence support to step 6*
Commander approves a COA.	• Recommend PIRs (including the LTIOV) and the supporting information collection plan. • Implement, refine, or rework the intelligence running estimate, Annex B (Intelligence), and the information collection plan based on the commander's acceptance, modification, or rejection of the staff's recommendation. • Upon COA approval, the G-2/S-2 and G-3/S-3 coordinate with supporting information collection resources to ensure the scheme of information collection supports the approved COA. • Refine the weather estimate. • Collaborate with the G-3/S-3 to ensure staffs at all levels understand the following: ▪ Scheme of information collection. ▪ EEFIs. ▪ Collection tasks. ▪ Analysis and production priorities. ▪ Intelligence control measures: target handover, reconnaissance handover, and reporting responsibilities. ▪ Procedures for tasking and reporting.
Step 7—Orders production, dissemination, and transition	*Intelligence support to step 7*
• Produce and disseminate orders. • Transition from planning to operations.	• The G-2/S-2 plans cell, assisted by the intelligence cell, develops Annex B (Intelligence) to the OPORD and assists the G-3/S-3 in producing Annex L (Information Collection). • The G-2/S-2 plans cell assists other staff members in preparing the enemy or information collection aspects of their annexes. Paragraph 3 (Coordinating Instructions) of Annex B (Intelligence) explains measures for handling captured personnel, documents, and materiel. • The G-2/S-2 reviews the OPORD and Annex B (Intelligence) for accuracy and completeness as well as compatibility with foreign disclosure policy or guidelines. • The G-2/S-2 forwards Annex B (Intelligence) to the G-3/S-3 for incorporation and dissemination into the OPORD. • The collection manager, supported by the intelligence cell, develops requests for information (intelligence production); with G-2/S-2 approval, the manager forwards the requests to the next higher echelon and adjacent units.

CCIR	commander's critical information requirement	IPOE	intelligence preparation of the operational environment
CEMA	cyberspace electromagnetic activities	JFC	joint force commander
COA	course of action	LTIOV	latest time information is of value
DP	decision point	MCOO	modified combined obstacle overlay
EEFI	essential element of friendly information	NAI	named area of interest
EMS	electromagnetic spectrum	OPORD	operation order
G-2/S-2	division or corps/battalion or brigade intelligence staff officer	PIR	priority intelligence requirement
G-3/S-3	division or corps/battalion or brigade operations staff officer	TAI	target area of interest
G-6/S-6	division or corps/battalion or brigade signal staff officer	WARNORD	warning order
HVT	high-value target		

SECTION V – INTELLIGENCE AND THE INTEGRATING PROCESSES

3-27. An integrating process consists of a series of steps that incorporate multiple disciplines to achieve a specific end. Integrating processes begin in planning and continue during preparation and execution. Commanders and staffs use the integrating processes to synchronize specific functions throughout the operations process. The intelligence staff supports the integrating processes by providing detailed and relevant all-source intelligence on the various aspects of the threat, terrain and weather, civil considerations, and other significant aspects of the OE. (See ADP 5-0 for doctrine on the integrating processes.)

3-28. Key integrating processes include—

- IPOE.
- Information collection.
- Targeting.
- Risk management.
- Knowledge management.

Note. IPOE is not discussed in this section. See paragraphs 3-15 through 3-17 for a discussion of the importance of the entire staff's collaborative involvement, see paragraphs 3-25 and 3-26 for a discussion of IPOE in the context of the MDMP, and see paragraphs 5-42 through 5-61 for a detailed discussion of IPOE in the context of the intelligence staff.

INFORMATION COLLECTION

3-29. *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). FM 3-55 discusses information collection capabilities, including human or automated sensors and assets directed to collect information that enables better decision making and expands an understanding of the OE.

3-30. Information collection is an integrated operations and intelligence function (see figure 3-4 on page 3-16). Collection management drives information collection. Therefore, collection management teams must understand information collection, as well as the *art* of effectively integrating collection management into information collection and the operations process.

3-31. Information collection provides commanders and staffs with detailed and timely intelligence, which assists them in gaining situational understanding of the threat and OE. Commanders and staffs accomplish situational understanding by answering intelligence requirements in time and space and identifying any threats to mission accomplishment. The intelligence staff provides commanders with predictive assessments (accounting for the domains and dimensions, as illustrated in figures 2-5 and 2-6 on pages 2-18 and 2-20, respectively) of the enemy, terrain and weather, civil considerations, and other significant aspects of the OE. (See FM 3-55 and ATP 2-01 for doctrine on information collection.)

Note. The intelligence warfighting function's contributions to information collection include collection management and intelligence operations. However, intelligence PED and intelligence analysis are integral to information collection.

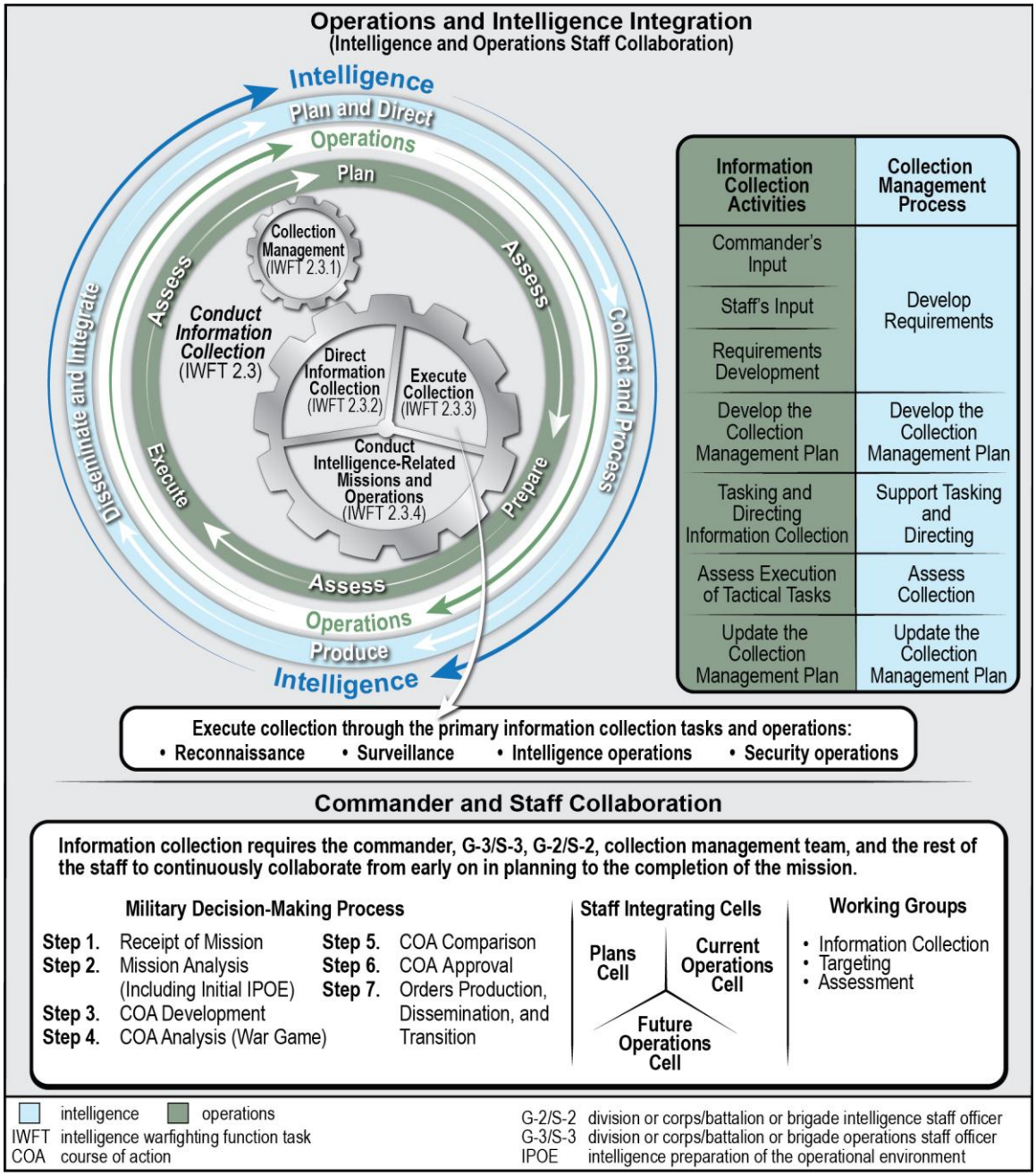


Figure 3-4. Intelligence contribution to information collection

3-32. *Conduct information collection* is an IWFT. The collection management team must understand the basics, nuances, and complexities associated with conducting the information collection tasks, discussed in detail in appendix B, not just collection management:

- Conduct collection management.
- Direct information collection.
- Execute collection.
- Conduct intelligence-related missions and operations.

CONDUCT COLLECTION MANAGEMENT

3-33. Collection management is commander driven. The collection management team, with assistance from the rest of the staff—especially the operations staff—manages intelligence requirements for the commander, prepares the collection management plan, and coordinates with the operations staff to maintain integration and synchronization as the information collection effort progresses. Chapter 5 discusses collection management extensively.

3-34. This discussion focuses on those aspects of collection management that require extensive staff cross-collaboration and coordination with and cooperation between the intelligence staff and other members of the staff (see also paragraph 3-41):

- Using ancillary collection assets during information collection.
- Executing technical collection during tactical operations and the complementary capabilities.

Using Ancillary Collection Assets

3-35. The G-2/S-2 and collection manager, in coordination with the rest of the staff, develop the collection management plan using primary collection assets (whose mission is to perform one of the four primary means of information collection: reconnaissance, surveillance, intelligence operations, and security operations), ancillary collection assets, and nonmilitary information sources. Ancillary collection assets are those units and systems tasked to perform information collection while also performing another mission during operations. They are sometimes referred to as nontraditional assets. Examples of ancillary collection assets include but are not limited to—

- Target acquisition radars.
- Air defense system sites.
- Logistics convoys.
- Military police performing security and mobility support.
- Helicopter battalions.
- Sniper teams.
- Civil affairs (CA) teams (unless already performing civilian reconnaissance).
- Special reconnaissance teams (unless performing strategic reconnaissance).
- Joint terminal attack controllers.
- Fire support teams.
- Army space control systems, if available.

3-36. The entire staff must cooperate with the G-2/S-2 and collection management team and perform detailed coordination to reasonably recommend these ancillary collection assets to the G-3/S-3 and operations staff for tasking and inclusion in Annex L (Information Collection) of the order. To ensure successful information collection, the tasking should be detail-oriented since the assets may be unfamiliar with information collection techniques and procedures. After tasking, staff control of these ancillary collection assets is important. (See ATP 2-01.)

Executing Technical Collection

3-37. The tactical execution of technical collection involves collaboration and detailed coordination across the staff. Technical collection and the evacuation of captured materiel for subsequent exploitation are usually not performed by the MI unit. Therefore, other types of units and logistical elements are heavily involved in technical collection activities.

Note. Commanders should not overlook the importance of technical collection in supporting TECHINT and DOMEX. In some situations, technical collection can provide valuable information and intelligence to support operations.

DIRECT INFORMATION COLLECTION

3-38. The operations staff integrates collection assets through a deliberate and coordinated effort across all warfighting functions. Tasking and directing information collection are vital in controlling limited collection assets. During tasking and directing information collection, the staff recommends cueing, redundancy, and mix, as appropriate. Staffs task information collection by issuing warning orders (WARNORDs), FRAGORDs, and operation orders (OPORDs). They direct collection assets by continuously monitoring the operation. Staffs retask to refine, update, or create new requirements. Tasking and directing information collection include two tasks:

- Develop the information collection plan.
- Execute, evaluate, and update the information collection plan.

3-39. Using intelligence handover lines is a flexible means of directing information collection, as well as analysis, to support key decisions and/or targeting. An ***intelligence handover line*** **is a control measure between two friendly units used to pass responsibility for the conduct of information collection against a specific enemy force**. Chapter 8 discusses intelligence handover lines.

EXECUTE COLLECTION

3-40. Executing collection focuses on requirements tied to the execution of tactical missions (reconnaissance, surveillance, intelligence operations, and security operations) based on the intelligence requirements. Collection activities acquire information about the threat and the AO, and they provide that information to intelligence processing and exploitation elements. Typically, collection activities begin soon after receipt of mission and continue throughout preparation and execution of the operation. They do not cease at the conclusion of the mission but continue as required. This allows the commander to focus combat power, execute current operations, and prepare for future operations simultaneously. (FM 6-0 lists G-3/S-3 responsibilities.)

CONDUCT INTELLIGENCE-RELATED MISSIONS AND OPERATIONS

3-41. The associated intelligence tasks (for example, *provide intelligence support to personnel recovery*) facilitate the conduct of reconnaissance and surveillance. These tasks also include specialized missions (such as exploitation of a sensitive site) that provide intelligence and information outside the traditional information collection construct. Conduct intelligence-related missions and operations includes six tasks:

- Establish a mission intelligence briefing and debriefing program.
- Conduct intelligence coordination.
- Support site exploitation.
- Conduct explosive ordnance disposal support.
- Provide intelligence support to personnel recovery.
- Conduct identity activities.

Note. The conduct intelligence-related missions and operations task emphasizes the importance of staff collaboration during collection management.

TARGETING

3-42. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting is an integral part of the operations process that organizes the commander and staff's efforts to integrate and synchronize fires into operations. Targeting seeks to create specific desired effects through lethal and nonlethal actions.

3-43. Targeting encompasses many processes, all linked and logically guided by the joint targeting cycle. Units may use the Army targeting methodology or the joint targeting cycle, as appropriate (according to the organizational echelon), to integrate and synchronize capabilities, across warfighting functions and information advantage activities, into operations to create the desired effects in time and space. The targeting

team recommends targeting guidance to the commander, develops targets, selects targets for attack, and coordinates, integrates, and assigns organic or allocated joint, interagency, and multinational fires to specific targets and target systems. (See FM 3-60.)

Target

A *target* is an entity or object that performs a function for the threat considered for possible engagement or other action (JP 3-60). Targets include an array of mobile and stationary forces, equipment, and capabilities that span the human, information, and physical dimensions. Threats can use targets to conduct operations. A target's importance is determined by its potential contribution to achieving the commander's objectives or otherwise accomplishing assigned tasks or reaching an effect. Targets are continuously refined or adjusted as an operation unfolds.

TARGETING WITHIN MULTIDOMAIN OPERATIONS

3-44. Targeting is a complex and multidisciplined effort that requires coordinated interaction among many groups. Army forces meet a diverse array of challenges and contribute to national objectives across a range of operational categories, including large-scale combat operations, limited contingency operations, crisis response, and support to security cooperation. While most operations conducted by Army forces occur either below the threshold of armed conflict or during limited contingencies, Army readiness focuses on large-scale combat operations.

3-45. Army forces conduct operations to support joint campaigns, which mostly occur as part of a larger coalition operation. Leaders must understand the interdependencies between their own assigned forces and the forces or capabilities provided by others to generate the complementary and reinforcing effects of combined arms approaches. Army forces employ joint and other unified action partner capabilities to the extent these capabilities are available. However, because peer threats can contest the force in all domains, Army forces must be prepared to conduct operations when some or all joint capabilities are unavailable to support mission accomplishment.

3-46. Army forces employ organic capabilities in multiple domains, and they continuously benefit from maritime and air strategic transportation and space and cyberspace capabilities that they do not control, including global positioning, satellite communications, and ISR. Lower echelons may not always notice the opportunities created by higher echelons or other forces that operate primarily in other domains; however, leaders must understand how the absence of those opportunities affects their concept of operations, decision making, and risk assessment.

TARGETING PRINCIPLES

3-47. Targeting proceeds from the commander's objectives to an assessment of the results achieved throughout an operation. Participants in the targeting process should adhere to these targeting principles for creating the desired effects while diminishing undesired or adverse collateral effects. The targeting principles are—

- **Focused.** Targeting focuses on achieving the commander's objectives. The function of targeting is efficiently achieving the commander's objectives within the parameters set at the operational level—directed limitations, the rules of engagement or the rules for the use of force, the law of war, and other guidance given by the commander. Every nominated target must contribute to attaining the commander's objectives.
- **Effects-based.** Targeting seeks to create specific desired effects through lethal and nonlethal actions or capabilities. Target analysis encompasses all possible means to create desired effects, drawing from all available capabilities. The art of targeting seeks to create desired effects with the least risk and time and resource expenditures.

- **Interdisciplinary.** Targeting is a command function that requires the participation of many disciplines, including all unit staff elements, other organizations, and multinational partners, to plan, prepare, execute, and assess targeting tasks.
- **Systematic.** A targeting methodology is a rational and iterative process that systematically analyzes, prioritizes, and assigns assets against targets to create those effects that will contribute to achieving the commander's objectives. During the operation, if the desired effects are not created, targets may be considered again in the process or operations may have to be modified.

TARGETING MEMBERS

3-48. Targeting team members are competent experts in doctrine and the processes and procedures associated with operations and targeting. The team understands existing authorities and critical staff capabilities that enable the creation and assessment of effects to support the commander's intent. Furthermore, the team understands its targeting duties and requirements enough to coordinate both vertically and horizontally. Team members have the flexibility to recognize changes in the OE and make timely coordination to affect targeting. Key targeting personnel may not exist at all echelons. The key targeting personnel within the intelligence staff include but are not limited to the—

- G-2/S-2.
- United States Air Force (USAF) staff weather officer (SWO).
- Intelligence targeting team officer.
- Collection manager.
- Analysis and control element (ACE) or brigade intelligence support element (BISE) chief.
- Field artillery intelligence officer (FAIO).

THE TARGETING PROCESS THROUGH THE ARMY TARGETING METHODOLOGY

3-49. Across the Army strategic contexts, the number of possible targets far exceeds the number of resources available to acquire and create desired effects. It is critical for the higher echelon to provide adequate guidance and anticipate the likely requirements for subordinate echelons. Targeting is a top-down driven process with a substantial need for bottom-up refinement. This applies to any circumstance requiring lead time or insertion into supporting planning or execution cycles. The importance of what targets to attack and with what available capabilities must be planned and prioritized. The decide, detect, deliver, and assess (D3A) Army targeting methodology is how the Army performs the targeting process. D3A is a flexible, repeatable four-function process, not designed to be time-constrained or rigidly sequential. (See figure 3-5.)

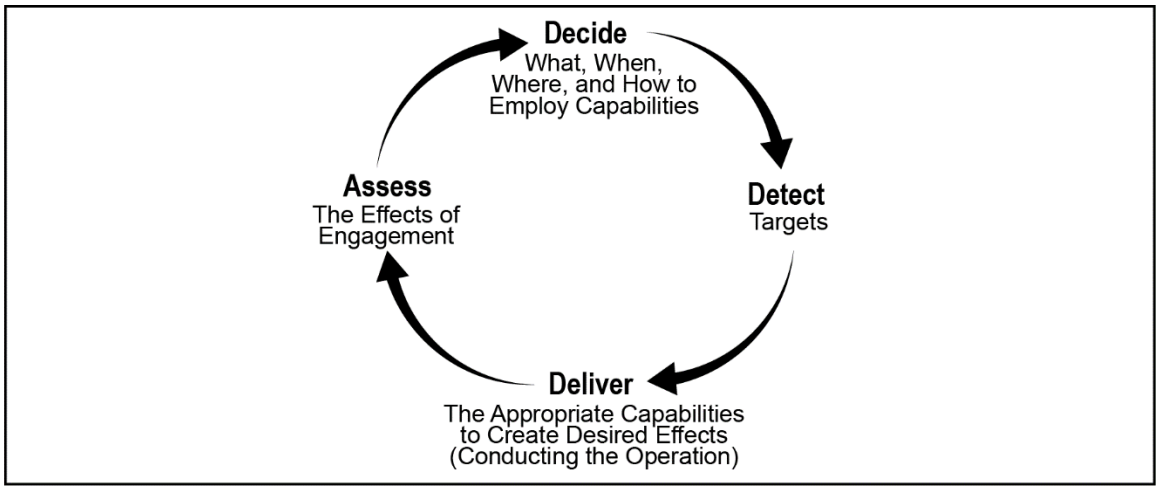


Figure 3-5. Decide, detect, deliver, and assess Army targeting methodology

3-50. The targeting process provides an effective method for matching friendly force capabilities against enemy targets to achieve the commander's desired effects and objectives. There are two general ways to frame the D3A Army targeting methodology:

- **During planning and the MDMP**, the staff uses the targeting methodology as a process to assist in product development and visualization. The staff applies the methodology to analyze the commander's guidance to determine the right targets, at the right place, at the right time. During the MDMP, the staff can make these decisions and apply the required assets to create desired effects. The staff can further discuss the methodology by developing COAs and war-gaming them. The staff also applies the methodology to assessment requirements and the analysis needed to facilitate future decisions.
- **As an integrating process during execution**, the targeting methodology enables the staff to apply targeting products (HPTLs, target selection standards [TSS], attack guidance matrices [AGMs], information collection synchronization matrices, and target synchronization matrices) to facilitate operations. The staff makes decisions continuously, adjusts detection methods or locations, and revises delivery options based on changes to threat COAs.

RISK MANAGEMENT

3-51. Risk management is the Army's primary process for identifying hazards and controlling risks during operations. *Risk management* is the process to identify, assess, and mitigate 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 collection assets. (See ATP 5-19 for risk management doctrine.)

3-52. Commanders must focus and use intelligence to explicitly understand the lethality of large-scale combat operations, preserve their combat power, and mitigate operational risk, when possible, 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.

3-53. Intelligence provides the commander the ability to detect adversary activities, predict enemy intentions, understand and track enemy capabilities across all domains, inform decisions, and provide realistic assessments of operational and tactical risks. 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 risks.

KNOWLEDGE MANAGEMENT

3-54. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). The purpose of knowledge management is aligning people, process, and tools within the organizational structure and culture to achieve a shared understanding. This alignment improves collaboration and interaction between leaders and subordinates and information sharing with subordinate units, higher-echelon headquarters, and unified action partners. (See ATP 6-01.1 for knowledge management doctrine.)

3-55. The intelligence staff participates in both the unit's overall knowledge management effort and its own staff knowledge management effort. Managing knowledge within the unit and the intelligence staff is critical to providing effective intelligence support. Important aspects of knowledge management include—

- Using the intelligence process with fundamentally sound procedures to ensure the right intelligence gets to the right users at the right time in a useable format, and the intelligence is integrated into operations, to include targeting, as appropriate.
- Ensuring the right focus and fundamentally sound procedures are used to avoid information overload and inundating the commander and staff with too much information and intelligence.

- Ensuring the intelligence staff is data literate according to Army Deputy Chief of Staff for Intelligence (DA G-2) standards.
- Avoiding circular reporting, which is receiving the same reports and information from sources other than the original source. Circular reporting can result in erroneous intelligence analysis and negatively affect the commander's decisions and the staff's control of operations.
- Protecting against threat misinformation, disinformation, deception, and collection countermeasures by emphasizing the use of all-source intelligence. The commander and staff can use single-source intelligence and combat information, but they must understand the risk of threat deception.

SECTION VI – COMMAND NODES AND CELLS AND BATTLE RHYTHM

3-56. Command nodes and cells and battle rhythm are important to C2. Effective C2 requires continuous, and often immediate, close coordination, synchronization, and information sharing across the staff. To promote this, commanders organize their staffs and other components of the C2 system into command posts (CPs) to assist them in effectively conducting operations. CPs provide a physical location for people, processes, and networks to directly assist commanders in understanding, visualizing, describing, directing, leading, and assessing operations. Across the CPs, commanders establish a battle rhythm as a procedural way to organize the activities within their headquarters and throughout the force. The battle rhythm is a deliberate daily cycle of command, staff, and unit activities that assist in synchronizing current and future operations.

COMMAND NODES AND CELLS

3-57. Intelligence operations are distributed across and support redundant and functionally integrated command nodes—main CPs and tactical CPs (which include support area CPs) and mobile command groups. Each command node retains the capacity to execute C2 of the warfighting functions synchronized with higher and lower echelons of command.

3-58. Intelligence personnel not assigned to intelligence cells in main CPs assist the G-2/S-2 in managing intelligence operations from across the battlefield. This generally includes intelligence personnel assigned to integrating cells in tactical CPs in addition to mobile command groups at the corps and division echelons. (See FM 6-0 for staff roles and responsibilities.)

Note. This publication provides information on intelligence cell structures based on modified tables of organization and equipment and force design updates. Commanders can task-organize based on mission requirements.

COMMAND POSTS

3-59. A *command post* is a headquarters, or a portion there of, organized for the exercise of command and control (FM 6-0). Corps, division, and BCT headquarters can employ a main CP, tactical CP, and mobile command group. Additionally, a corps and division can use a rear area CP. Each CP has specific functions by design that assist commanders in understanding, visualizing, describing, directing, leading, and assessing operations. The following includes CP functions common to all CPs:

- Conduct knowledge management, information management, and foreign disclosure.
- Build and maintain situational understanding.
- Control operations (by coordinating, synchronizing, and integrating).
- Assess operations.
- Coordinate with internal and external organizations.
- Perform CP administrative activities.

Main Command Post

3-60. A *main command post* is a portion of a unit headquarters containing the majority of the staff designed to command and control current operations, conduct detailed analysis, and plan future operations (FM 6-0). The main CP is the unit's principal CP, serving as the primary location for plans, analysis, sustainment coordination, and assessments. It includes representatives from all staff sections and information and C2 systems to conduct operations. At certain echelons, the main CP can act as a JTF, JFLCC, or a coalition forces land component commander.

3-61. The main CP is larger, has more staff members, and is less mobile than the tactical CP. It operates at both operational and tactical levels and as a fully functional, stand-alone CP. All battalion and above units are resourced with a main CP that includes an executive officer or chief of staff, as appropriate, to supervise the staff. The main CP conducts all meetings (which may include working groups, cells, and boards) required to achieve mission requirements.

3-62. Main CP general functions include—

- Controlling operations.
- Receiving reports from subordinate units and preparing reports required by higher headquarters.
- Planning operations, including branches and sequels.
- Integrating intelligence into current operations and plans.
- Synchronizing the targeting process.
- Planning and synchronizing sustainment operations.
- Assessing the progress of operations.

Tactical Command Post

3-63. A *tactical command post* is a portion of a unit headquarters designed to command and control operations as directed (FM 6-0). It relies on the main CP for planning, detailed analysis, and coordination as well as for certain functions remaining with the main CP that require intelligence reach. The tactical CP is connected digitally to the main CP, mobile command group, higher headquarters, and all subordinate unit headquarters, including joint and multinational partner intelligence organizations. The tactical CP can support the entire range of missions at that echelon, but it does not have the same longevity and capacity as the main CP. Additionally, the tactical CP should prepare to be able to communicate in a denied, degraded, and intermittent low-bandwidth environment.

3-64. A tactical CP intelligence cell—

- Supports current operations.
- Ensures the tactical CP remains informed of the current enemy situation.
- Makes recommendations related to the operation.

3-65. A tactical CP intelligence cell accomplishes these tasks by continually communicating and collaborating with the main CP intelligence cell and supported unit headquarters. The structure of a tactical CP is organic to the unit's mission. In most situations, the structure is designed based on unit SOPs and mission variables (METT-TC [I]). The echelon determines the proper location of the tactical CP relative to the forward line of own troops.

Mobile Command Group

3-66. The mobile command group is the commander's mobile CP. The commander selects key personnel based on mission variables to staff the mobile command group. These key personnel often represent those staff sections—typically maneuver, fires, and intelligence—that can immediately affect current operations.

3-67. The intelligence representative to the mobile command group must be integrated with echelons above brigade organizations, the main and tactical CPs, and subordinate commands through the intelligence architecture. The mobile command group intelligence officer—

- Assists the commander in interpreting intelligence reports and coordinating intelligence operations with the main and tactical CPs.
- Informs the commander of the intelligence running estimate and intelligence readiness.

Rear Area Command Post

3-68. Based on the situation, threat, size of the rear area, and the number of units in the rear area, corps and division commanders may form a rear area CP to assist in controlling operations. The rear area CP includes the support area as a subset of the rear area. The rear area CP enables corps and division commanders to exercise C2 over disparate functionally focused elements operating in rear areas that may exceed the effective span of control of the maneuver enhancement brigade or corps and division main CPs.

3-69. The rear area CP is not a separate section in a unit's table of organization and equipment. When commanders form a rear area CP, they do so from the personnel and equipment in the main and tactical CPs. It normally collocates with the maneuver enhancement brigade, which provides the rear area CP with signal connectivity, sustainment, security, and workspace.

3-70. Rear area CP functions include—

- Planning and directing sustainment.
- Terrain management.
- Movement control.
- Area security.
- Current and future operations.
- Providing the situational awareness of the deep, close, and security fights.
- Assisting the main CP with information flow from higher, lower, and lateral units.
- Coordinating with the host-nation, international organizations, nongovernmental organizations, and other stakeholders, as required.
- Issuing orders.

COMMAND POST CELLS

3-71. Commanders organize CP cells based on the situation. A *command post cell* is a grouping of personnel and equipment organized by warfighting function or by planning horizon to facilitate the exercise of command and control (FM 6-0). Staff elements comprising personnel and equipment from staff sections form CP cells, which are typically organized as integrating and functional cells. (See figure 3-6.) These CP cells provide staff expertise, communications, and information systems that work together to assist the commander in planning and controlling operations.

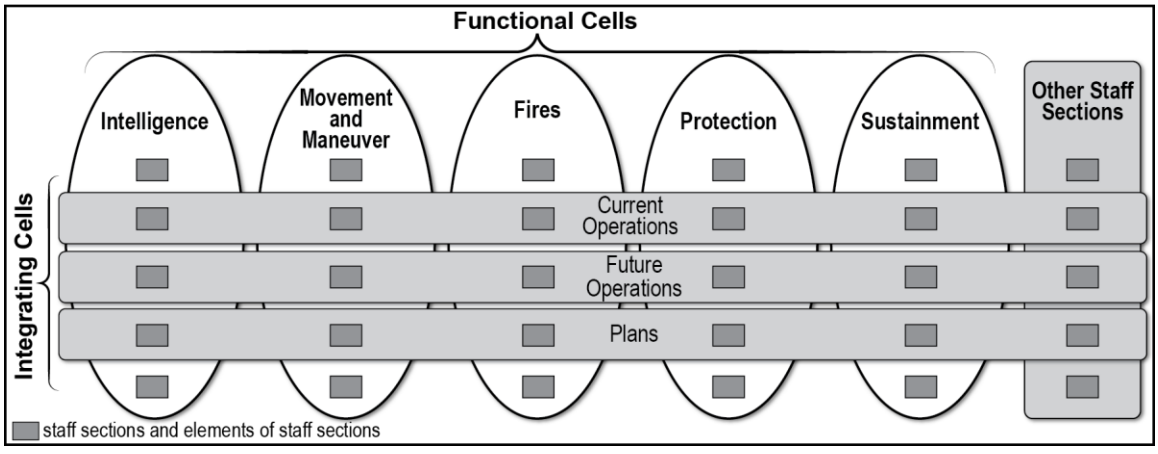


Figure 3-6. Command post cells

Note. Resourcing for CP cells is different at each echelon. Specific information can be found in the doctrinal publications for each echelon.

Integrating Cell

3-72. Integrating cells coordinate and synchronize forces and warfighting functions within a specified planning horizon. A *planning horizon* is a point in time commanders use to focus the organization's planning efforts to shape future events (ADP 5-0). The three planning horizons are short-, mid-, and long-range; they are associated with the following cells, respectively:

- **Current operations integration cell (COIC):** The COIC is the focal point for the execution of current operations. This involves assessing the current situation while regulating forces and warfighting functions according to the commander's intent and concept of operations. All staff sections are represented in the COIC either permanently or on call. Intelligence personnel assigned to the COIC ensure all relevant intelligence regarding the enemy and other threats, terrain and weather, and civil considerations are integrated into the COP. The COIC—
  - Issues, monitors, evaluates, directs, and controls the execution of orders.
  - Conducts limited short-range planning and coordinates this effort within the functional cells.
  - Continually updates IPOE.
  - Conducts regular operations and assessment briefings.
  - Maintains and displays the COP.
  - Conducts shift changes, assessments, and other briefings as required.
- **Future operations cell:** The future operations cell focuses on adjustments to the current operation—including the positioning or maneuvering of forces in depth—that facilitate the continuation of the current operation.
- **Plans cell:** The plans cell (responsible for mid- to long-range planning operations) develops plans, orders, branches, and sequels using the MDMP to prepare for operations beyond the scope of the current order. The plans cell oversees military deception planning. The G-5 leads the plans cell and oversees planning for future operations. The intelligence planner—
  - Assists in developing plans, orders, branches, and sequels.
  - Monitors the common intelligence picture (CIP) and COP.
  - Stays abreast of current operations by coordinating with the COIC.
  - Coordinates with the ACE, BISE, or equivalent intelligence analysis element to produce intelligence products required for planning and orders production.

Functional Cell

3-73. Functional cells coordinate and synchronize forces and activities by warfighting function. Organizing staff sections among CP functional cells expands the commander's ability to exercise C2 and makes the C2 system more resilient. The functional cells in a CP are intelligence, movement and maneuver, fires, protection, and sustainment. Chapter 5 discusses the intelligence staff and the intelligence functional cell.

BATTLE RHYTHM

3-74. A headquarters' battle rhythm consists of a series of meetings (to include working groups and boards), briefings, and other activities synchronized by time and purpose. The *battle rhythm* is a deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations (FM 6-0). The chief of staff or executive officer oversees the unit's battle rhythm and ensures activities are logically sequenced so the output of one activity informs another activity's inputs. This is important not only within the headquarters but also in the unit's battle rhythm as it nests with the higher-echelon headquarters.

3-75. Understanding the purpose and potential decisions of each meeting and activity is equally important. This understanding allows members of the staff and subordinate commanders to provide appropriate input to influence decisions. The battle rhythm enables—

- A commander's decision making.
- A routine for staff interaction and coordination.
- Interaction between the commander and staff.
- Staff synchronization across time, space, and purpose.
- Planning by the staff.

3-76. In conjunction with the integrating processes, *working groups*—groupings of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function (FM 6-0)—are important in integrating and synchronizing intelligence into operations. Effective integration and synchronization require the entire staff's full participation in the information collection working group as well as the intelligence staff's full participation in the other working groups, especially the targeting, CEMA, and protection working groups.

3-77. EMS actions, as discussed in paragraph 1-103, provide a good example of the criticality of detailed staff coordination and effective working groups. Coordinating and deconflicting SIGINT collection, EW operations, and spectrum management connect to executing optimal information collection, CEMA integration, targeting, and information advantage activities. The intelligence and CEMA staffs must collaborate with the rest of the staff and across working groups, especially the CEMA and targeting working groups.

3-78. Working groups address various subjects depending on the situation and echelon. Brigade and battalion headquarters have fewer working groups than higher echelons. Working groups may convene daily, weekly, monthly, or intermittently depending on the subject, situation, and echelon. Typical working groups, at corps and division headquarters, scheduled within the unit's battle rhythm include—

- Assessment.
- Civil-military operations (CMO).
- CEMA.
- Information collection.
- Information operations.
- Knowledge management.
- Protection.
- Sustainment.
- Targeting.
- Airspace control.

Note. Time permitting, some units conduct a targeting coordination board that unites key members of the CEMA, information collection, targeting, and other working groups to obtain the commander's validation and approval of targeting within current and future operations.

Chapter 4
Army Strategic Contexts and Intelligence

SECTION I – OVERVIEW

4-1. The Army is a globally engaged, regionally responsive force that provides a full range of capabilities to CCDRs. The Army provides the joint force with the capability and capacity for the application of landpower. Army forces meet a diverse array of challenges and contribute to national objectives across a wide range of operational themes, including large-scale combat operations, limited contingency operations, crisis response, military engagement, and support to security cooperation. The Army also provides a broad range of organizations, units, and capabilities to support theater operations.

4-2. Combatant commands develop theater campaign plans that rely on the operational themes as well as campaign and operations activities. When a situation forces a branch to the campaign plan, it may eventually lead to armed conflict. In these situations, the full capability of the intelligence enterprise supports the combination of offensive, defensive, and stability operations to seize, retain, and exploit the initiative and consolidate gains to ultimately return to competition.

4-3. Army intelligence is an inherent part of any joint and multinational combined arms team; intelligence activities conducted facilitate successful joint operations. The intelligence enterprise supports the joint force across the competition continuum through the aggressive execution of information collection and intelligence production. A portion of the Army intelligence force is designated to support the joint force. (See figure 4-1.)

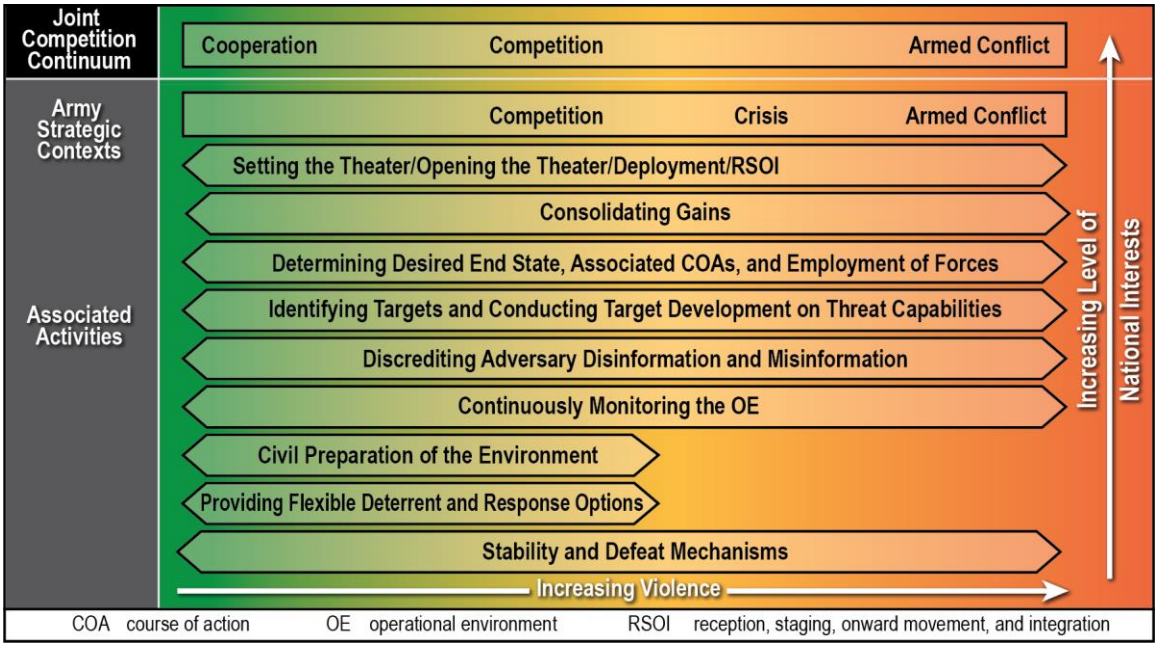


Figure 4-1. Joint competition continuum aligned with the Army strategic contexts

ARMY STRATEGIC CONTEXTS

4-4. Army doctrine describes the strategic situation through three contexts—competition, crisis, and armed conflict—in which Army forces conduct operations (see figure 4-1 on page 4-1). Therefore, the rest of this publication uses the Army strategic contexts as a major doctrinal construct to discuss intelligence. Supporting Army forces, as part of unified action, across the strategic contexts require an effective intelligence warfighting function that is continuously vigilant and flexible. The Army synchronizes its intelligence effort with unified action partners to achieve unity of effort and meet the commander's intent. Intelligence unity of effort is critical in accomplishing the mission. The character of effective and flexible intelligence support transitions across the Army strategic contexts.

INTELLIGENCE SUPPORT

4-5. Effective intelligence support assists in identifying and creating exploitable advantages in the OE. It is important to note—some peer threats view themselves in continual conflict, whether war in the traditional sense has begun. Intelligence professionals must consider this peer threat perspective and seek advantages to provide commanders with options against the threat across the strategic contexts. The intelligence staff must also understand how intelligence warfighting function capabilities support the tenets and imperatives of operations across the strategic contexts—doing so optimizes the integration of operations and intelligence. While some intelligence tasks and activities are specific to certain strategic contexts, many of the tasks and activities span across all three strategic contexts. Commanders and staffs must collaborate with the intelligence staff to adequately address the planning, collection and PED, storage and safeguarding, and analysis of intelligence and associated contextual data during each Army strategic context.

4-6. The intelligence staff must coordinate with the rest of the staff continuously. This coordination ensures the first imperative of operations—*see yourself, see the enemy, and understand the OE*—is always at the forefront of synchronizing operations and intelligence and identifying advantages against threat forces. Threat forces seek advantages in multiple domains and dimensions to overwhelm U.S. forces' ability to react. At times, these advantages are not readily identified because threat activities, windows of opportunity, and friendly efforts to exploit those windows and reach an advantage occur over extended time windows (in some situations, over decades). Successful intelligence operations must remain agile and flexible to continuously monitor OE changes and friendly and enemy strategic and operational effects, so the commander and staff can adjust forces and capabilities when needed.

Long-Term Situational Understanding Challenges

The broad nature of the Army strategic contexts and long-duration time windows are challenges to Army commanders and staffs. While many aspects of the theater are inherently national- and joint-level activities, the Army also has an important role. The effort to provide continuous situational understanding across the strategic contexts and account for all domains and dimensions is carefully focused through the operational variables (PMESII-PT) and pre-mission analysis of the OE. Focusing a large volume of information and intelligence down to a manageable amount of relevant information is time-consuming and requires detailed analysis. Often, there are limitations on the conduct of information collection during competition—and sometimes during crisis. Despite these challenges, Army commanders and staffs must support the planning and execution of flexible deterrent and response options as well as defeat and stability mechanisms to achieve desired end states. Gaps and problems with gaining situational understanding during competition can result in an even greater challenge as friendly forces transition into crisis and armed conflict.

4-7. Intelligence support is inherently difficult and is often discussed throughout this manual as *fighting for intelligence*. Fighting for intelligence applies as much to intelligence support to Army units and organizations during competition (including long-term situational understanding) or crisis as it does to intelligence support to a division conducting offensive operations during a large-scale combat operation. Each strategic context discussion in this chapter concludes with a fighting for intelligence discussion. (See paragraphs 1-120 through 1-125 for a discussion on the concept of fighting for intelligence.)

SECTION II – COMPETITION BELOW ARMED CONFLICT

4-8. Competition exists when two or more state or nonstate adversaries have incompatible interests but neither seeks armed conflict. Nation-states compete using all instruments of national power to gain and maintain advantages that assist them in achieving their goals. Low levels of lethal force can be part of competition. Adversaries often employ cyberspace capabilities and information warfare to destroy or disrupt infrastructure, interfere with government processes, and conduct activities in a way that does not cause the United States and its allies to respond with force. Competition provides military forces—

- Time to prepare for armed conflict.
- Opportunities to assure allies and partners of resolve and commitment.
- Time and space to set the necessary conditions to prevent crisis or armed conflict.

ADVERSARY METHODS

4-9. Conducting effective operations during competition requires a broad understanding of the strategic security environment and common adversary methods and objectives. During competition, adversaries seek to further their own interests using a variety of methods to hinder the United States from achieving its objectives. Therefore, the intelligence staff must understand adversary methods and their associated goals and desired effects. This knowledge assists the intelligence warfighting function in integrating and synchronizing with the other warfighting functions to generate combat power and apply it against adversary actions.

Note. Peer threats conduct activities over prolonged time windows, so peer threat objectives, advantages, and effects may not be recognized immediately. In some situations, these advantages and effects may be observed slowly over expanded timeframes and eventually lead to crisis and possibly armed conflict. fragment

ADVERSARY ACTIVITIES TO ACHIEVE STRATEGIC GOALS

4-10. By using a range of military and nonmilitary activities, peer threats use all instruments of national power to further their interests. The adversary's use of diplomatic, economic, informational, and military activities shapes the OE to the adversary's advantage well before armed conflict. Adversaries operate aggressively in the space or cyberspace domains during competition and crisis to influence the OE and deter or degrade friendly operations. Adversaries target foreign audiences to promote strategic messages on the international stage. At times, these messages are not legitimate or correct; the adversary's intent is to get the messages out first, outside of the friendly forces' ability to effectively counter these messages. Analyzing the possibility of threat and friendly forces leveraging a window of opportunity to gain or maintain human, information, and physical advantages is an important aspect of intelligence support during competition.

ADVERSARY ACTIVITIES TO COUNTER A U.S. RESPONSE

4-11. An adversary may attempt to prevent or constrain the United States' ability to project forces to the region and limit U.S. response options by using the following methods:

- Conduct information warfare activities to manipulate the acquisition, transmission, and presentation of information in a manner that legitimizes adversary actions and portrays the United States as the aggressor.

- Conduct preclusion activities through nonlethal means to undermine relationships, raise political stakes, manipulate public opinion, and erode resolve to constrain or eliminate basing rights, overflight corridors, logistics support, and concerted allied actions.
- Isolate the United States from allies and partners by fostering instability in critical areas and among relevant actors to increase U.S. operational requirements.
- Create sanctuary from U.S. and partner forces through international law and treaty agreements, monitoring and attacking partner forces from across international borders and using proxy forces.
- Conduct systems warfare by executing cyberspace attacks against critical force projection and sustainment infrastructure nodes to delay or disrupt the United States' ability to deploy forces. Systems warfare approaches include nonattributable attacks on domestic infrastructure and the employment of networked military capabilities that support isolation and preclusion efforts.

ADVERSARY ACTIVITIES TO PRECLUDE U.S. ACCESS TO A REGION

4-12. Establishing favorable conditions by shaping an OE is critical to the United States' success and the adversary's success. Adversaries seek to establish conditions that limit or prevent U.S. access to a region, typically in locations close to either adversary borders or U.S. allied-partner borders. This includes but is not limited to—

- Forward positioning of layered and integrated air defenses, long-range fires, and other A2 capabilities.
- Positioning of systems capable of delivering conventional and nuclear munitions.
- Positioning of intermediate-range ballistic missiles and cruise missiles.
- Positioning of fixed-wing aircraft.
- Positioning of unmanned aircraft systems (UASs).
- Positioning of naval surface and subsurface forces.
- Early warning surveillance radars.
- Rocket artillery.
- Conducting offensive cyberspace activities against friendly C2, infrastructure, and sustainment capabilities.
- EW capabilities.
- Counterspace capabilities.

4-13. Adversaries seek exploitable advantages in the OE; therefore, U.S. forces should expect that adversaries are observing them, including U.S. forces' intentions and activities across all echelons within CONUS and outside the continental United States (OCONUS). Security activities and CI considerations for all echelons are important, ranging from technology protection and force modernization security to tactical unit deployments and exercises. Adversaries may reach and exploit advantages in terms of intelligence collection and then use the intelligence to cause grave harm to U.S. interests and operations.

OPERATIONAL ASPECTS

4-14. Operations during competition—

- Deter malign adversary action.
- Set conditions to support friendly operations and the effective use of various capabilities should deterrence fail.
- Shape an OE with allies and partners in ways that support U.S. strategic interests and policy aims.

4-15. Preparation for armed conflict is the primary focus of Army conventional forces during competition. Operations during competition focus on—

- Setting the theater.
- Building allied and partner capabilities and capacity.
- Improving joint and multinational interoperability.
- Protecting forward-stationed forces.

- Preparing to transition and execute operation plans (OPLANs).
- Training and developing leaders for operations in specific theaters.
- Promoting and protecting U.S. national interests and influence.
- Building partner capacity and partnerships.
- Recognizing and countering adversary attempts to gain positions of relative advantage across the domains and dimensions.

4-16. Competition activities are continuous within an area of responsibility (AOR). Army forces participate in and conduct numerous other activities to support the CCDR's theater campaign plan. These activities include developing intelligence, countering weapons of mass destruction, providing support to humanitarian efforts, achieving information advantages, and organizing and participating in combined training and exercises. The CCDR uses these activities to improve security within partner nations, enhance international legitimacy, gain multinational cooperation, and influence adversary decision making. This cooperation includes exchanging information and sharing intelligence, obtaining access for U.S. forces in peacetime and crisis, and mitigating conditions that could lead to crisis and armed conflict.

4-17. The theater army and subordinate Army forces perform the following major activities during competition:

- Execute flexible deterrent options and flexible response options.
- Set the theater across warfighting functions, including in terms of preparing for intelligence operations and intelligence staff activities during crisis and armed conflict.
- Tailor Army forces.
- Project the force. (See appendix C.)

4-18. Other competition activities include but are not limited to—

- Exchanging information and sharing intelligence with unified action partners.
- Assisting allies and partners to improve their military capabilities and capacity.
- Medical support.
- Cooperative training.
- Supporting local institutions.

4-19. Operations during competition consist of various long-term military engagements, security cooperation, and deterrence missions, tasks, and actions. Typically, these operations also occur to support the CCDR's theater campaign plan or theater security cooperation plan. CCDRS use these plans as tools to organize, integrate, and execute joint operations.

CONSOLIDATING GAINS

4-20. Experience proves that Army force activities conducted during competition assist in ensuring stability and reduce the potential for man-made crises or armed conflict throughout a region, even in locations where no previous combat has occurred. During competition, Army forces may consolidate gains from previous conflicts for many years as JFCs seek to maintain relative advantages against a specific adversary and sustain enduring political outcomes. Examples of consolidating gains during competition include but are not limited to—

- Increasing theater supply stocks.
- Developing and revising detailed contingency plans and perfecting tactical tasks to execute OPLANs for large-scale combat operations.
- Promoting interoperability with host-nation units. This consideration includes intelligence agreements, exercises, interoperability agreements with unified action partners, and expedited means to revise intelligence sharing agreements, when necessary.
- Promoting and facilitating civil-military integration and interorganizational cooperation between unified action partners and indigenous populations and institutions responsible for executing governance.
- Infrastructure improvement. This consideration includes constant revisions and measures to improve the survivability of the intelligence architecture within the theater.

- Assessing and improving protection measures against adversary capabilities.
- SIGINT surveys and other intelligence surveys and assessments within the theater.
- Leveraging Army engagements during the execution of foreign assistance, which includes humanitarian and civic assistance.

FIGHTING FOR INTELLIGENCE

4-21. Intelligence is integral in supporting operations during competition. Often, this intelligence support is expressed as setting the theater among Army intelligence professionals. Continuous monitoring of the OE to determine changes that may lead to an escalation of hostilities must occur to give decision makers adequate warnings to determine and execute optimal deterrent and response actions. The intelligence staff must establish a baseline intelligence architecture to meet a broad range of requirements, to include ensuring information is available to support decision making if the strategic context transitions to crisis and armed conflict. Intelligence must be continuously developed to ensure Army and other joint forces are prepared to meet the multitude of scenarios that could possibly drive change and escalate conflict. If the situation does escalate, intelligence support must be able to focus on critical stability and defeat mechanisms for subsequent activities and operations.

4-22. Intelligence products assist the commander in countering actions by adversaries that challenge the security of forward-stationed units and the stability of a nation or region and are contrary to U.S. interests. Intelligence provides the commander and staff with the ability to—

- Detect indicators of imminent threat activities and understand enemy intentions.
- Track enemy activities and capabilities across the domains and dimensions.
- Understand how the threat is attempting to gain and/or maintain positions of relative advantage.
- Make informed decisions and realistic assessments of operational and tactical risks.
- Support targeting.
- Support information advantage activities.

4-23. Support to contingency plan development, which is treated as a branch to the campaign plan, is a vital activity during competition. Different situations within an AOR can cause a branch to the campaign plan, including regional instability, armed aggression, natural or man-made disasters, or humanitarian crises. Intelligence assists in identifying these potential situations and participates in developing plans to mitigate these scenarios.

4-24. Intelligence databases also have an important role in setting the theater from an intelligence perspective. Managing and creating unclassified and classified databases provide interoperable and collaborative environments for Army and joint forces, national agencies, and multinational organizations. Databases facilitate intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach. Within each theater, the development and validation of databases generally occur in a top-down manner, with significant support from regionally aligned forces and special operations forces. This allows units to maintain, populate, and continually update a thorough and accurate set of databases during subsequent Army strategic contexts. However, there may be instances when regionally aligned forces must develop and populate an authoritative database of threat signatures and associated contextual information, in conjunction with joint forces and the DIA. This is particularly true when an area quickly transitions from competition to crisis. In some scenarios, each echelon below theater army must prepare to establish localized intelligence databases during any strategic context. Unit SOPs should outline the requirements for managing, formatting and standardization, indexing and correlation, normalization, storage, security protocols, and associated applications.

Note. It is critical for commands to update intelligence databases continually with actual and potential threat information to maximize the value of intelligence products and reports.

Two Key Aspects of Building Databases and Intelligence to Support Crisis and Armed Conflict

Intelligence enterprise units and organizations should carefully use a federated analytical approach in developing and maintaining authoritative databases of threat indicators and key capability signatures and associated contextual information across all the domains and dimensions.

Army intelligence units and organizations, in coordination with the intelligence enterprise, should use a federated analytical approach in analyzing threat systems similarly to joint TSA. ***Note.*** Army analysis of threat systems is not conducted to joint standards and is not captured in the same format as joint TSA and target development. When working as part of or to support the joint force, Army forces perform joint TSA and conduct target development to joint standards.

SECTION III – CRISIS

4-25. *Crisis* is an emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives (JP 3-0). During crisis, armed conflict has not yet occurred, but it is either imminent or a distinct possibility that requires a rapid response by forces prepared to fight if deterrence fails. A crisis can be long in duration, but it can also reflect a near-simultaneous transition to armed conflict. Leaders do not assume that a crisis provides additional time for a transition to armed conflict. Crisis is different from crisis response, which can result from a natural or human disaster.

ADVERSARY METHODS

4-26. When conducting activities in an OE, peer threats seek to gain or maintain advantages against opponents. As a crisis develops, a peer threat uses information warfare and preclusion to shape the situation. This may include the adversary escalating or de-escalating its activities based on an assessment of the situation, which includes a calculation of the risk. During crisis, adversary methods include but are not limited to—

- Shaping a crisis.
- Controlling escalation.
- Mitigating U.S. deterrence.

ADVERSARY ACTIVITIES TO SHAPE A CRISIS

4-27. Peer threats shape a crisis to their benefit by seeking to exploit real or perceived advantages, which can be local, regional, and/or global. Peer threats use information warfare and preclusion to gain an information advantage against U.S. messaging and further isolate U.S forces and capabilities from allies.

4-28. Units and organizations, at and across echelons, conduct continuous information collection (including ISR within the joint force) to gain situational understanding of threat activities, capabilities, intent, and COAs. Threat forces seek to employ capabilities and conduct operations faster than friendly forces can act to gain and maintain a position of relative advantage. Threat forces can gain this advantage by finding a window of opportunity where friendly forces are either denied or delayed by specific circumstances from using the dynamics of combat power (leadership, firepower, information, mobility, survivability).

ADVERSARY ACTIVITIES TO CONTROL ESCALATION

4-29. Peer threats may attempt to control the escalation of a crisis to avoid armed conflict with the United States by initiating actions to prevent or counter a U.S. response. These actions may focus on the United States and its allies by using the instruments of national power. These actions may include creating conditions on the ground designed to make U.S. military responses either too expensive to employ or too late to affect the political situation. A peer threat may also—

- Accelerate its operational timeline.
- Employ information warfare.
- Increase support to proxy forces.
- Increase the number of forward deployed units in the region.
- Initiate crisis in other theaters to distract U.S. forces and diffuse U.S. response in the area of greatest interest.

Note. In extreme situations to control escalation, an adversary may conduct a limited attack in response to U.S. reactions to the activities that precipitated the original crisis.

ADVERSARY ACTIVITIES TO MITIGATE U.S. DETERRENCE

4-30. As an adversary plans for operations during crisis, there are several key actions the adversary considers to mitigate U.S. deterrence efforts and ensure U.S. operations do not significantly interfere with adversary interests. These actions may include—

- Conducting limited attacks to expose friendly force vulnerabilities. These attacks may also degrade the deterrence value of deployed forces and destroy credibility among current and potential partners.
- Disrupting or delaying the deployment of Army and joint forces through cyberspace attacks and denial of space capabilities.
- Exploiting gaps in national interests among the United States, partner nations, and potential partners by attacking weaker countries whom the United States has no treaty obligations to defend.
- Conducting deception operations to conceal real intent.
- Increasing the use of proxy forces to coopt, coerce, or influence the local population, organizations, and governments within a crisis region.
- Creating multiple dilemmas for the United States by attacking or threatening the use of force against potential partner nations in regions outside of the crisis region.
- Impacting the will of the public through information warfare, including cyberspace attacks.
- Threatening the use of nuclear weapons to prevent intervention by the United States, allies, and partners.

OPERATIONAL ASPECTS

4-31. A crisis can result from one or a multitude of events/actions such as adversary actions/indicators of an imminent action or natural or human disasters. Examples of events/actions that can lead to a crisis include but are not limited to—

- Aggressive behavior by an adversary to coerce and intimidate an opponent with the threat of force.
- The presence of indicators foreshadowing a military coup or change of political power.
- Increased dissemination of disinformation or misinformation targeted toward a country’s population and the international community.
- Disease outbreak.
- Build-up of military forces at an international border.
- Failed elections.
- Famine.

4-32. Although an opponent has not yet used lethal force as its primary means of achieving objectives, crisis can escalate to armed conflict. Combat power derived from the intelligence warfighting function, in conjunction with the other warfighting functions, is critical in providing credible lethal capabilities to assist in deterring further provocation and compelling an adversary to cease aggressive action.

4-33. Some peer threats view conflict as a continuous condition in which sharpened or reduced periods of violence occur and recur. Additionally, adversaries may perceive themselves in a different context or state of conflict than U.S., allied, and partnered forces—what is viewed by one side as crisis might be perceived by the other side as armed conflict or competition.

4-34. Changing the intensity of its actions, even when that intensity reduces tension, does not end an adversary's campaign to oppose U.S. interests. Intelligence professionals must continuously assess the OE and demonstrate flexibility in determining adversary actions, the changes they cause, and how information and intelligence can be used to de-escalate the situation or further prepare U.S. and allied partners for armed conflict. Regardless of the capabilities employed, there are generally two broad outcomes from a crisis:

- Deterrence is maintained and de-escalation occurs.
- Armed conflict begins.

CONSOLIDATING GAINS

4-35. During and after a crisis response, Army forces consolidate gains to deny adversary forces the means to extend the crisis or create a similar crisis in the future. This often entails maintaining an enhanced force posture in a joint operations area for a time to demonstrate U.S. willingness to defend allies and partners. Continuous intelligence operations to support U.S. forces, allies, and partners are essential during any crisis. Commanders must emphasize information collection before and during the transition from competition to crisis to maintain a detailed understanding of the threat and continuously assess the situation, positioning their forces to retain the initiative.

4-36. During these transitions, threat forces attempt to exploit perceived vulnerabilities by conducting lethal and nonlethal activities against U.S. forces, allies, and partners. The threat's use of disinformation and misinformation can be used to shape threat narratives to justify ongoing or pending actions, including the use of force. Commanders and staffs should focus on potential threat and friendly strengths, vulnerabilities, and advantages across the domains and dimensions. Continuous information collection and intelligence analysis are critical in ensuring flexible deterrent and/or flexible response options.

FIGHTING FOR INTELLIGENCE

4-37. Operations during crisis place increasing demands on the intelligence warfighting function. The intelligence staff increases its knowledge of the threat and the specific OE, focuses the commander and staff with relevant information and intelligence, and expands various intelligence capabilities as part of the intelligence architecture. With the shift from competition to crisis, the theater army shifts to refining contingency plans and preparing estimates for the phased increase of ground forces and capabilities. During crisis, intelligence operations focus on the following:

- Support theater openings in terms of finding and exploiting advantages.
- Gain and maintain situational understanding of threat intent and COAs, activities, and the nature of those activities and effects across the theater.
- Provide support to noncombatant evacuation operations, when needed.
- Provide support to targeting and prepare for targeting during armed conflict.
- Provide support to force projection and prepare for the possibility of a contested deployment.
- Provide support to information advantage activities, as appropriate.
- Provide support to protection activities.
- Provide focused analysis of the domains and human, information, and physical dimensions, then properly focus that into analysis of the operational variables.
- Provide support to identify and implement flexible deterrent and response options and follow-on activities and operations.

- Significantly modify the intelligence architecture to prepare for the possibility of armed conflict.
- Set conditions to reset theater intelligence and the intelligence architecture.

4-38. The intelligence staff must understand threat intent and COAs as well as ongoing activities in terms of the threat's perspective, which often includes an extended time window. Leveraging the intelligence enterprise, including allies and partners, assists in understanding the threat's perspective. This situational understanding is essential in gaining and maintaining advantages against the threat's use of the five broad peer threat methods—information warfare, systems warfare, preclusion, isolation, and sanctuary (see paragraph 2-21).

4-39. Truly understanding the OE across the domains and dimensions, including important interrelationships, significantly increases the likelihood that commanders and staffs can accurately predict when, where, and how the threat will conduct actions. When commanders and staffs can predict threat actions, friendly force capabilities can be used to quickly gain positions of relative advantage. However, intelligence is rarely perfect. When commanders and staffs have a lower level of situational understanding, it is important to develop and rely on detailed indicators of possible threat intent and COAs and continually track those indicators.

SECTION IV – ARMED CONFLICT

4-40. Armed conflict encompasses the conditions of a strategic relationship in which opponents use lethal force as the primary means for achieving objectives and imposing their will on the other. The employment of lethal force is the defining characteristic of armed conflict, and it is the primary function of the Army. Entering and terminating armed conflict are political decisions. Army forces may enter conflict with some advanced warning during a prolonged crisis or with little warning during competition. How well Army forces are prepared to enter an armed conflict ultimately depends on decisions and preparations made during competition and crisis. Army forces provide landpower to the joint force and conduct limited contingency or large-scale combat operations to ensure enduring political outcomes favorable to U.S. interests.

Note. Large-scale combat operations are the focus of Army readiness and reflect the most intense and destructive form of armed conflict. Therefore, the rest of this section will focus on large-scale combat operations.

WARFARE

4-41. The object of war is to impose a nation or group's will on its enemy in pursuit of policy objectives. Regardless of the specific objectives, the decision to wage war represents a major policy decision and changes how Army forces use military capabilities. The nature of war, its principles, and its elements remain consistent over time. However, warfare, the conduct and characteristics of war, reflects changing means and contexts. The Army's multidomain operations concept accounts for the constant nature of war and the changing character of warfare. Its balanced approach guides how Army forces operate across the competition continuum given the prevailing characteristics of anticipated OEs now and in the near future.

4-42. There are several important aspects of warfare discussed in FM 3-0. These aspects include the methods of warfare. There are many different methods of warfare, depending on the situation and actors, but they generally fall into two broad categories:

- *Conventional warfare* is a violent struggle for domination between nation-states or coalitions of nation-states (FM 3-0). Conventional warfare is generally executed by two or more military forces through armed conflict. It is commonly known as conventional warfare because it means to fight enemy forces directly, with comparable military systems and organizations.
- *Irregular warfare* is the overt, clandestine, and covert employment of military and nonmilitary capabilities across multiple domains by state and non-state actors through methods other than military domination of an adversary, either as the primary approach or in concert with conventional warfare (FM 3-0). Irregular warfare may include the use of indirect military activities to enable partners, proxies, or surrogates to achieve shared or complementary objectives.

4-43. Offensive, defensive, and stability operations are inherent elements of conventional and irregular warfare. Divisions and higher echelons typically perform some combination of all three elements in their operations simultaneously. However, the lower the echelon, the more likely it is for that formation to be focused on one element at a time. The three types of operations differ:

- An *offensive operation* is an operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). Offensive operations are how commanders impose their will on an enemy. The offense is the most direct means of seizing, retaining, and exploiting the initiative to gain a physical and psychological advantage. Offensive operations typically include a sudden action directed toward enemy vulnerabilities, capitalizing on speed, surprise, and shock.
- 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). Typically, 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, and they seek to destroy as many of the enemy forces as possible. Defensive operations preserve control over land, resources, and populations, and they protect lines of communications and critical capabilities against attack. Commanders can conduct defensive operations in one area to free forces for offensive operations elsewhere.
- A *stability operation* is an operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental 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 action.

Note. Offensive, defensive, and stability operations are important doctrinal constructs across many of the Army intelligence doctrinal publications.

LARGE-SCALE COMBAT OPERATIONS

4-44. Large-scale combat on land occurs within the framework of a larger joint campaign, usually with an Army headquarters forming the base of a joint force headquarters. These operations typically entail high tempo, high resource consumption, and high casualty rates. Large-scale combat introduces levels of complexity, lethality, ambiguity, and speed to military activities not common in other operations.

4-45. During large-scale combat operations, Army forces should expect deployments to be contested by enemy actions in all domains. In a contested deployment, the first challenge during large-scale combat operations is defeating a network of sophisticated A2 and AD systems. Enemy forces will attempt to deny U.S. and multinational forces access to the AO by contesting U.S. and multinational forces in each of the domains and dimensions of the OE. The joint force may even have to fight for intelligence to identify threat locations, strengths, and vulnerabilities to gain an initial lodgment.

4-46. Once joint and Army forces achieve an initial lodgment, they must be prepared to immediately conduct tactical operations. As a lodgment is formed, the threat will likely employ a variety of new capabilities to deny friendly forces freedom of maneuver. Friendly forces must be prepared to operate quickly across each domain and dimension. These multidomain efforts must entail joint synchronization, Service interdependencies, and the cross-domain convergence of capabilities at a time and place to create an operational advantage. Army forces must account for constant enemy observation, including the threat from cyberspace, space-based, and unmanned systems that saturate the OE. Army forces take measures to defeat the enemy's ability to effectively mass effects while creating exploitable advantages to mass effects against enemy capabilities and formations.

4-47. The challenge for and requirements on the intelligence warfighting function from deployment to initial lodgment and subsequent operations are substantial. Developing effective collection management plans and tasking collection assets (in depth and with redundancy) are essential. Intelligence support identifies windows of opportunity to counter the threat's capabilities and enable the joint force to maintain freedom of action and gain positions of relative advantage. (The advantage can be a human, information, or physical advantage.) (See appendix C for intelligence support to force projection operations.)

ADVERSARY METHODS

4-48. Although peer threats mainly seek to obtain their strategic objectives during competition, they will engage in armed conflict if they view the rewards are worth the risk. During armed conflict, peer threats employ combinations of threat methods to render U.S. military power irrelevant whenever possible and inflict unacceptable losses on the United States, its allies, and its partners. Peer threats use diplomatic, economic, informational, and military means to facilitate meeting their objectives.

CHINA

4-49. China considers three aspects in the country's view of conflict:

- **Comprehensive national power** comprises hard power (military capability and capacity, defense industry capability, intelligence capability, and related diplomatic actions such as threats and coercion) and soft power (economic power, diplomatic efforts, foreign development, global image, and international prestige). Ultimately, all forms of conflict must enhance China's comprehensive national power.
- **Deception** is essential to China's tactics to achieve desired perceptions by its opponents. These perceptions are ultimately exploited to further China's objectives. Central to deception is having opponents make decisions not based on what is occurring in an OE. When doing so, opponents are faced with making decisions and conducting actions regarding situations or circumstances in which China has already set the conditions to have an advantage.
- **The Three Warfares** are designed to unbalance, deceive, and coerce opponents to influence their perceptions in ways that create advantage. The Three Warfares are universally nonlethal, do not involve direct combat operations, and are designed to support and reinforce the traditional military operations of the People's Liberation Army. The Three Warfares are—
  - **Public opinion warfare**—China's high-level information campaign designed to set the terms of political discussion.
  - **Psychological warfare**—the deliberate manipulation of psychological reactions in targeted audiences designed to create and reinforce attitudes and behaviors favorable to China's objectives and guide adversary behavior toward China's preferred outcomes.
  - **Legal warfare**—the setting of legal conditions to unbalance potential opponents by exploiting international or domestic law in order to hinder their military operations, create legal justification for People's Liberation Army operations worldwide, and support Chinese interests through a valid framework.

4-50. During armed conflict, China employs systems warfare in combination with the other threat methods, such as preclusion, isolation, and sanctuary. China employs these threat methods throughout the domains and at all levels of warfare. Systems warfare involves—

- Bypassing enemy systems' areas of strength, gaining a combat advantage by approaching them asymmetrically.
- Developing systems that excel at exploiting perceived vulnerabilities in enemy systems, thereby offsetting their strengths by undermining their systems' ability to perform assigned missions.
- Undermining international alliances through diplomatic efforts.
- Conducting cyberspace attacks to disable air or seaports.
- Using special operations forces to undermine civilian morale through covert operations.

4-51. At the tactical level, systems warfare centers largely on targeting high-value battlefield systems such as radars, command and communications nodes, field artillery and air defense systems, and critical logistics support means. (For Chinese tactics, see ATP 7-100.3 and FM 3-0.)

RUSSIA

4-52. Russian forces seek to shape the OE to gain and maintain relative advantages across the domains and dimensions. Russia seeks to do this by synchronizing capabilities and their effects simultaneously to overwhelm U.S. and allied force capabilities and capacity and weaken the United States' national will to continue a conflict. (For Russian tactics, see FM 3-0.)

4-53. Russian goals are centered on creating constraints that prevent success of the United States' campaign by using methods that focus on four key areas:

- **Disrupt or prevent understanding of the OE.** Russian information warfare activities manipulate the acquisition, transmission, and presentation of information in a manner suitable to Russia's preferred outcomes.
- **Target stability.** Russia may foster instability in key areas and among key groups so regional security conditions do not support U.S. operational requirements.
- **Disaggregate partnerships.** Russia acts upon U.S. allies and partners to reduce the United States' ability to operate in its preferred combined, joint, and interagency manner.
- **Prevent access.** Russia employs preconflict activities to deny access to U.S. forces, using nonlethal means initially and transitioning to lethal means if necessary. Russia seeks to undermine relationships, raise political stakes, manipulate public opinion, and attack resolve to constrain or deny basing rights, overflight corridors, logistics support, and concerted allied action.

4-54. Similar to U.S. forces, Russian forces operate combined arms forces to exploit the effects of both precision strikes and massed fires. Russian forces also—

- Employ all available national elements of power both before employing conventional warfare and maneuver forces and after employing conventional warfare.
- Employ deep maneuver against lesser opponents, when possible, to defeat an enemy's will to resist early in a conflict.
- Mass capabilities in pursuit of more limited objectives while fixing their adversary along a broad front.
- Employ denial and deception to mask the true intent of operations.
- Use the effects of strike actions to create the condition for military success.
- Apply intelligence methods and decision making that are scientifically based to—
  - Understand the conditions of an OE that will impact operations.
  - Determine the tactical functions required and calculate the required allocation of combat power needed to accomplish a mission in a specific time and location.
  - Understand the psychological and cognitive issues among competing friendly forces, aggressor forces, the local population, and other actors in an OE.

CONSOLIDATING GAINS

4-55. During armed conflict, Army forces deliberately plan to consolidate gains throughout an operation. This is part of defeating the enemy in detail to accomplish overall policy and strategic objectives. From a small unit perspective, consolidating gains can be actions on the objective and preparing for enemy counterattacks, while from a theater army perspective, it can be incorporating partner-nation forces into ongoing operations. From the intelligence perspective, intelligence support to consolidating gains often focuses on situational understanding, warning intelligence, support to force protection, identity activities, and cultural understanding; it also assists in determining termination criteria or when it is operationally acceptable to transition from large-scale combat operations to post-conflict competition.

4-56. Consolidating gains initially focuses on the exploitation of tactical success to ensure enemy forces cannot reconstitute any form of resistance in areas where they were initially defeated, or that enemy forces have not successfully conducted a deception operation to create a friendly force vulnerability or achieve a position of relative advantage. While the deep and close areas of the operational framework are important, the rear area has a special importance during consolidating gains due to bypassed, stay-behind, or infiltrated enemy forces; airborne, air assault, or special operations forces; terrorist cells; guerilla, partisan, or insurgent forces; the use of chemical weapons; or an effective combination of these forces and capabilities can significantly degrade friendly force operations. The impact of these types of threat operations can create crippling logistics, C2, civil population, and worldwide and U.S. public opinion issues.

4-57. Army forces must continuously consolidate gains to make temporary gains enduring. Like many activities, success is far more likely when the intelligence effort is carefully integrated and synchronized with operations. Typical operational functions and their reporting intelligence requirements include—

- Locating bypassed enemy forces, bypassed or abandoned munitions and weapons, and stay-behind special purpose and proxy forces.
- Populace and resource control measures.
- Reestablishing law and order.
- Providing humanitarian assistance.
- Restoring key infrastructure.

4-58. When consolidating gains during armed conflict, the role of intelligence is vital in assessing relevant aspects of the OE, including but not limited to—

- Detecting both positive and negative trends.
- Discrediting disinformation and misinformation.
- Determining the effectiveness of friendly operations.
- Identifying actions that could threaten hard-won gains.
- Assisting with the difficult transitions between offensive, defensive, and stability operations and the transition to post-conflict competition.

TRANSITIONS BETWEEN OFFENSIVE, DEFENSIVE, AND STABILITY OPERATIONS

4-59. A main goal of defensive operations is defeating the enemy's attacks and transition, or threaten to transition, to the offense. Units must deliberately plan for transitions to identify and establish the necessary friendly and enemy conditions for a successful transition. As friendly forces meet their defensive objectives, forces consolidate and reorganize for offensive operations or prepare to facilitate forward passages of lines for fresh formations. Units should do everything possible to prevent enemy forces from reinforcing their forward echelons, consolidating, or reorganizing while friendly forces prepare for follow-on operations.

4-60. Intelligence is critical to supporting the commander and staff as they—

- Assess when they have enough combat power to maintain pressure on the enemy.
- Identify opportunities to complete the defeat of enemy formations in order to reduce the risk of future casualties fighting the same enemy formations after recovery.
- Assess the effects of battle on enemy forces relative to their own unit.

4-61. When offensive operations culminate before enemy forces are defeated, friendly forces rapidly transition to the defense. Commanders may deliberately transition to the defense when enemy forces are incapable of fully exploiting an opportunity, or when they believe they can build combat power to resume the offense before enemy forces can react effectively. Depending on where culmination occurs, friendly forces may have to reposition forces on defensible terrain and develop a form of defense and scheme of maneuver based on an assessment of the mission variables (METT-TC [I]).

4-62. Successful offensive operations end because Army forces have achieved their assigned objectives. A successful offense can also require a transition to a defensive posture dominated by stability operations and a strategic environment moving toward post-conflict political goals. These operations have the goal of transitioning responsibility for security and governance to legitimate authorities other than U.S. forces.

4-63. As a transition to stability operations occurs, leaders focus on stability operations tasks and information advantage activities to inform and influence populations and conduct security force assistance. Effective collaboration with diplomatic and humanitarian organizations enhances the ability to achieve stability mechanisms. Army forces play a key role in enabling the joint force to establish and conduct military governance until a civilian authority or government is given control of its assigned areas.

TRANSITION TO POST-CONFLICT COMPETITION

4-64. Army forces conclude armed conflict by establishing conditions favorable to the United States; they consolidate gains and prosecute operations with this desired end state. As hostilities end, stability operations tasks dominate operations with the purpose of transitioning responsibilities to legitimate authorities in a secure environment. Army forces provide the joint force with the option of establishing a military transitional government before transitioning full governing responsibility to host-nation or other provisional governments.

4-65. Standards for transitioning governance responsibility depend on the credibility, capability, and capacity of the governing organization to maintain the favorable conditions established during armed conflict. Strategic leaders determine the broad conditions for transition at the outset of operations and refine them based on how the situation changes. Army forces play a key role in understanding the host-nation culture, understanding critical infrastructure, assisting strategic leaders in developing realistic transition goals and timings, and determining the duration and scale of U.S. commitments required to maintain stability.

4-66. In some situations, operations may rapidly transition from large-scale combat operations to stability operations with the requirement to maintain continuous security while grappling with a new and very different set of challenges. Army units and organizations may modify their task organizations and priorities to meet additional tasks associated with stability operations. Some of the typical tasks associated with stability operations include the following: establish civil security, establish civil control, restore essential services, support to governance, support economic and infrastructure development, and conduct security cooperation.

4-67. This transition is very complex and difficult for the intelligence warfighting function. Intelligence must support all six tasks; it must often support combatting terrorism, arms control, counterinsurgency, counterdrug operations, and foreign internal defense in a larger context. Essential to intelligence support during the transition to the enable civil authority phase of operations is determining how intelligence units can support enabling the sustainability of civil authority. During these operations, intelligence staffs and units have a different focus, organize in a different manner, and perform unique tasks:

- Many unique aspects of the OE—such as sociocultural factors, regional and local politics, and financial intelligence—become important.
- For special operations forces, integration and interoperability with conventional forces become critical. (See FM 6-05.)
- Fusion centers and other unique analytical centers are formed.
- Certain aspects of operations—such as counter-improvised explosive devices, counterterrorism, and screening local hires—become more important.

FIGHTING FOR INTELLIGENCE

4-68. Of all the Army strategic contexts, armed conflict creates the greatest challenge for the intelligence warfighting function, and large-scale combat operations against a peer threat is the most challenging form of armed conflict. The demands of large-scale combat operations consume all staff elements to provide the necessary support in the level of detail and at the *tempo*—the relative speed and rhythm of military operations over time with respect to the enemy (ADP 3-0)—these types of operations require. During large-scale combat, intelligence support is continually conducted to provide commanders and staffs the detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute operations during unified action. An intense focus on the critical elements of intelligence support—such as supporting the commander and staff's understanding, visualization, and ability to direct operations as well as assisting to drive the unit's battle rhythm—is required. Chapter 8 details the roles and techniques associated with fighting for intelligence during large-scale combat operations.

This page intentionally left blank.

PART TWO

Major Intelligence Activities

The doctrinal concepts in part I—intelligence and operational fundamentals—are important to fully understand the content in part II, which discusses major intelligence activities—intelligence staff support (chapter 5) and intelligence operations (chapter 6). Chapters 5 and 6 further set the foundation to understand the specifics of fighting for intelligence, which is discussed in detail in part III.

Chapter 5

Intelligence Staff Support

SECTION I – OVERVIEW

5-1. Staffs support commanders in making and implementing decisions and in integrating and synchronizing combat power. Competent staffs multiply a unit's effectiveness. They provide timely and relevant information and analysis, make estimates and recommendations, prepare plans and orders, assist in controlling operations, and assess the progress of operations for the commander. A staff primarily—

- Supports the commander.
- Assists subordinate commanders, staffs, and units.
- Informs units and organizations outside the headquarters.

5-2. Effective intelligence support is multifaceted, and the G-2/S-2 and intelligence staff are ultimately responsible for providing intelligence support to the commander and staff. The complexities of collecting against and conducting analysis on a determined and adaptive, threat that is technologically capable across all domains, creates challenges for the G-2/S-2 and intelligence staff. Other complexities that can challenge the intelligence staff include but are not limited to—

- A multitude of factors within the OE (across the human, information, and physical dimensions).
- Sophisticated intelligence capabilities.
- The intelligence architecture.
- Time constraints during the execution of the intelligence process.
- The many requirements to support multidomain operations.

5-3. This chapter discusses how the intelligence staff provides intelligence support to the commander and staff, including—

- Intelligence staff composition and responsibilities.
- Key IWFTs.
- Situational understanding, the CIP, and the COP.

5-4. Figure 5-1 shows important aspects of fighting for intelligence from the context of the intelligence process, with emphasis on the commander's role in driving the intelligence warfighting function and the G-2/S-2's role in synchronizing intelligence.

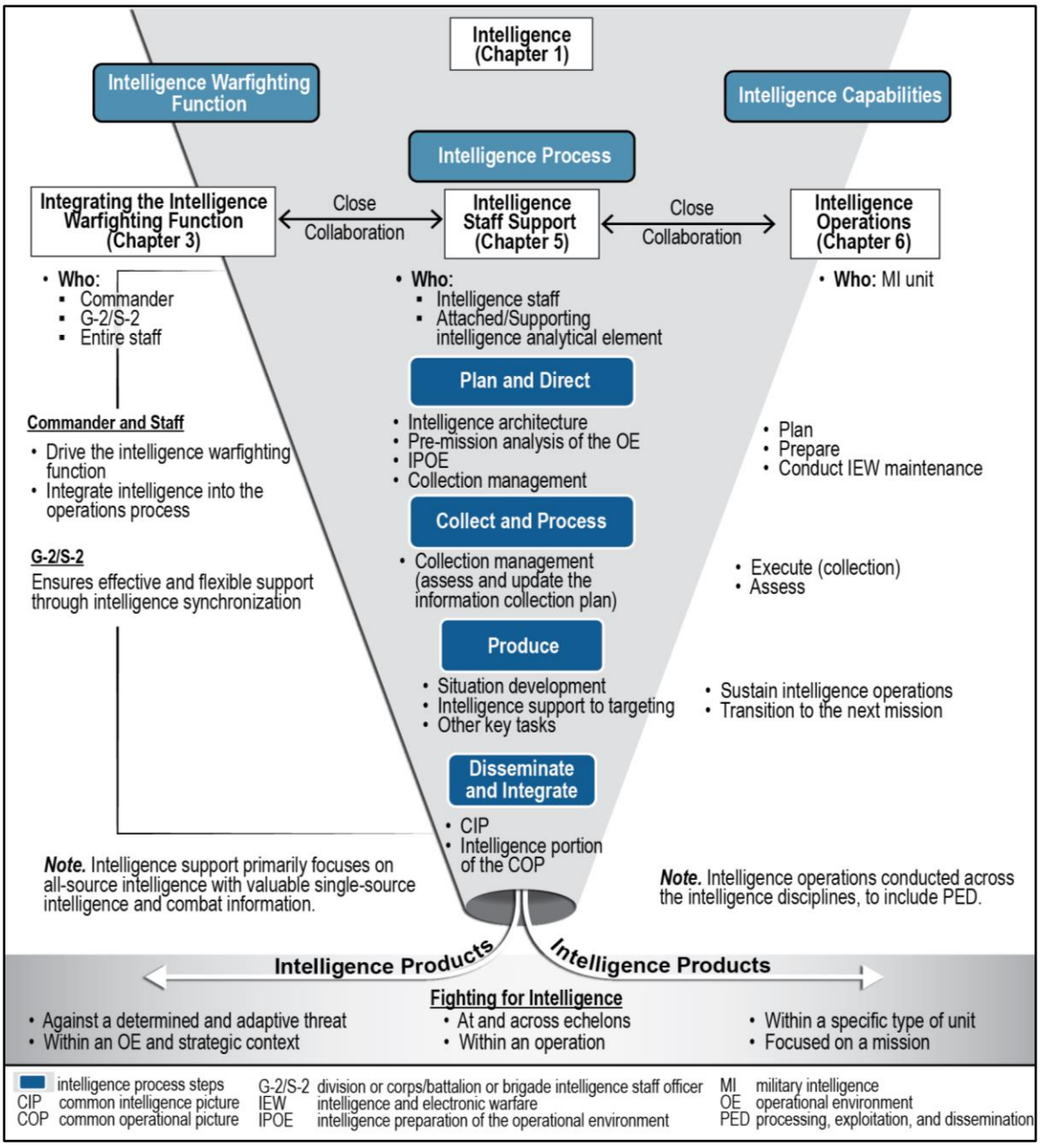


Figure 5-1. Military intelligence activities

SECTION II – INTELLIGENCE STAFF COMPOSITION AND RESPONSIBILITIES

5-5. The first aspect of understanding intelligence staff support is understanding the intelligence staff's composition and responsibilities, which differ by echelon but are also similar across echelons. The G-2/S-2 organizes its staff, provides focus, assigns tasks, and synchronizes the entire intelligence effort. However, the discussions about staff responsibilities interrelate with preceding discussions about staff teamwork, the operations process, integrating processes, and leveraging intelligence and collaborating with higher, subordinate, and adjacent units and organizations.

INTELLIGENCE STAFF COMPOSITION

5-6. The composition of the intelligence staff differs significantly across echelons—from theater army to BCT levels. The G-2/S-2 organizes its staff, to include the supporting intelligence analytical element, to meet the various requirements resulting from the conduct of operations. The higher the echelon, the more personnel within the intelligence staff and the more sophisticated the structure. Generally, certain functions are common across echelons and drive the organization of the intelligence staff. Forming permanent instead of ad hoc teams or sections is preferable because of the skills and proficiency necessary to perform those functions. Although there are intelligence staff elements in other CP cells, most of the intelligence staff sections reside in the main CP intelligence cell. Additional staff integration occurs through cross-functional working groups such as the information collection, protection, and targeting working groups.

5-7. The intelligence functional cell commonly includes the following:

- The G-2X/S-2X.
- Collection management.
- Targeting.
- The ACE or BISE (at the BCT level [see ATP 2-19.4]).
- IEW maintenance and intelligence sustainment.
- Intelligence communications.
- The USAF SWO or staff weather team, when augmented.

Notes. Higher headquarters may augment the intelligence cell with additional capabilities to meet mission requirements.

This chapter discusses the intelligence staff, to include the supporting intelligence analytical element as a critical element of the intelligence staff. Intelligence analytical elements are either attached, under OPCON, DS, or in another support relationship to the headquarters and headquarters company or other headquarters that includes the staff at that echelon. For example, at the division level, the division ACE is controlled by the division G-2.

INTELLIGENCE STAFF RESPONSIBILITIES

5-8. Staff members have specific duties and responsibilities associated with their area of expertise. They must be ready to advise the commander and other senior leaders about issues pertaining to their area of expertise without advanced notice. However, regardless of their career field or duty billet, all staff sections share a common set of duties and responsibilities, to include—

- Managing information within their area of expertise.
- Building and maintaining running estimates.
- Conducting staff research.
- Analyzing problems.
- Performing IPOE.
- Developing information requirements.
- Advising and informing the commander.
- Providing recommendations.
- Preparing plans, orders, and other staff writing, including recommendations on Annex A (Task Organization).
- Exercising staff supervision.
- Performing risk management.
- Assessing operations.
- Conducting staff inspections and assistance visits.
- Performing staff administrative procedures.

5-9. The intelligence staff is primarily responsible for providing the commander and staff with intelligence on the threat, terrain, weather and weather effects, civil considerations, and other significant aspects of the OE. Other intelligence staff responsibilities include but are not limited to—

- Enabling an effective intelligence process:
  - Plan, establish, and revise an intelligence architecture in close collaboration with the G-6/S-6 and other staff members.
  - Leverage data, information, and intelligence to provide the best intelligence support possible.
  - Lead collection management, which drives information collection. Develop a draft of Annex L (Information Collection) of the order to assist the G-3/S-3.
  - Ensure ongoing information collection—collecting the information needed for anticipated decisions and intelligence requirements.
  - Use knowledge management techniques to optimize intelligence support.
  - Answer requests for information (RFIs) from higher, subordinate, and adjacent units.
  - Disseminate intelligence to higher, subordinate, and adjacent units and organizations.
- Determining and requesting foreign disclosure office/representative support to facilitate collaboration with unified action partners and allies.
- Facilitating an understanding of the OE, with the greatest emphasis on the threat, terrain, weather and weather effects, civil considerations, and other significant aspects of the OE:
  - Conduct pre-mission analysis of the OE, including analysis of threat capabilities and the population (especially information dimension effects) across the domains and dimensions.
  - Lead IPOE and produce the various IPOE products.
  - Analyze and evaluate civil considerations in close collaboration with the G-9/S-9.
  - Facilitate the USAF SWO or staff weather team in effectively providing forecasts and weather effects on friendly and enemy capabilities.

Note. Commanders, supported by their staffs, must develop and maintain the best possible understanding of their OE, including the domains, dimensions, and the operational and mission variables. (See paragraph 2-31 for means to understanding the OE.) Figures 2-5 and 2-6 on pages 2-18 and 2-20, respectively, illustrate the inclusion of the domains, dimensions, and the operational and mission variables into staff activities and analysis, specifically the intelligence staff's responsibility to provide the commander and staff with intelligence on the threat, terrain, weather and weather effects, civil considerations, and other significant aspects of the OE.

- Supporting all forms of planning and assessments, to include targeting and the other integrating processes:
  - Write Annex B (Intelligence) of the order.
  - Provide intelligence support to targeting (through lethal and nonlethal means).
  - Provide intelligence support to CA units executing operations with unified action partners and regional and local populations and institutions.
  - Provide intelligence support to psychological operations, operations security (OPSEC), military deception, and other information advantage activities.
  - Provide intelligence support to risk management.
  - Provide intelligence support to knowledge management.
- Supporting the conduct of operations and the commander's decisions:
  - Answer intelligence requirements and provide advice.
  - Perform situation development, maintain the intelligence running estimate, and develop the CIP and the intelligence portion of the COP.
  - Provide support to protection and sustainment (including specific requirements in the rear area).
  - Provide support to combat assessment.

- Supporting security programs, to include the following:
  - Supervise command and personnel security programs.
  - Evaluate physical security vulnerabilities to support staff sections, particularly the operations and signal staffs.
  - Perform staff planning and supervise the special security office, when applicable.

The G-2/S-2

The G-2/S-2 leads the intelligence staff and has responsibility for what the intelligence staff does and does not accomplish. The G-2/S-2 is the primary advisor to the commander and staff on the intelligence warfighting function. Additionally, the G-2/S-2 has staff responsibility for the USAF SWO.

Successful intelligence support is based on the successful execution of the intelligence process, which the G-2/S-2 enables through intelligence synchronization. However, the G-2/S-2, as one person, must depend on its staff to provide effective intelligence support to the unit and facilitate situational understanding and effective targeting.

The G-2/S-2 is not responsible for the conduct of intelligence operations by the MI unit beyond conducting collection management. (See ATP 2-01.) The MI unit commander is responsible for the conduct of intelligence operations by the MI unit. Chapter 3 discusses the roles of the G-3/S-3, G-2/S-2, collection manager/collection management team, and MI unit commander/MI unit related to intelligence operations.

Notes. Due to the nature and fluidity of large-scale combat operations, commanders will have to make decisions with imperfect intelligence. Intelligence that is too late for commanders to make timely decisions results in a loss of the initiative and lost battles and engagements.

As much as possible, the intelligence staff depends on thorough and disciplined all-source analysis. All-source analysis reduces the possibility of error, bias, deception, disinformation, and misinformation by considering multiple sources of information and intelligence. However, when necessary, the commander and staff may have to depend on either single-source intelligence or combat information without all-source intelligence analysis or verification.

The cyberspace domain and the information dimension require specialized expertise from outside the traditional military staff, such as industry and academia. Intelligence support to the cyberspace domain and the information dimension often requires specific authorities, moves at a high tempo, and requires close coordination with higher-level friendly military cyberspace activities and sometimes with nonmilitary cyberspace activities.

SECTION III – KEY INTELLIGENCE WARFIGHTING FUNCTION TASKS

5-10. Chapter 1 describes how the intelligence warfighting function supports operations through a broad range of doctrinal tasks referred to as IWFTs. The intelligence staff is responsible for some of those tasks, MI units are responsible for other tasks, and both the intelligence staff and MI unit have shared responsibility for some tasks. Figure 5-2 on page 5-6 illustrates key IWFTs from an understanding the OE perspective; this section discusses the most important IWFTs from the intelligence staff's perspective. Appendix B provides a detailed discussion of the IWFTs.

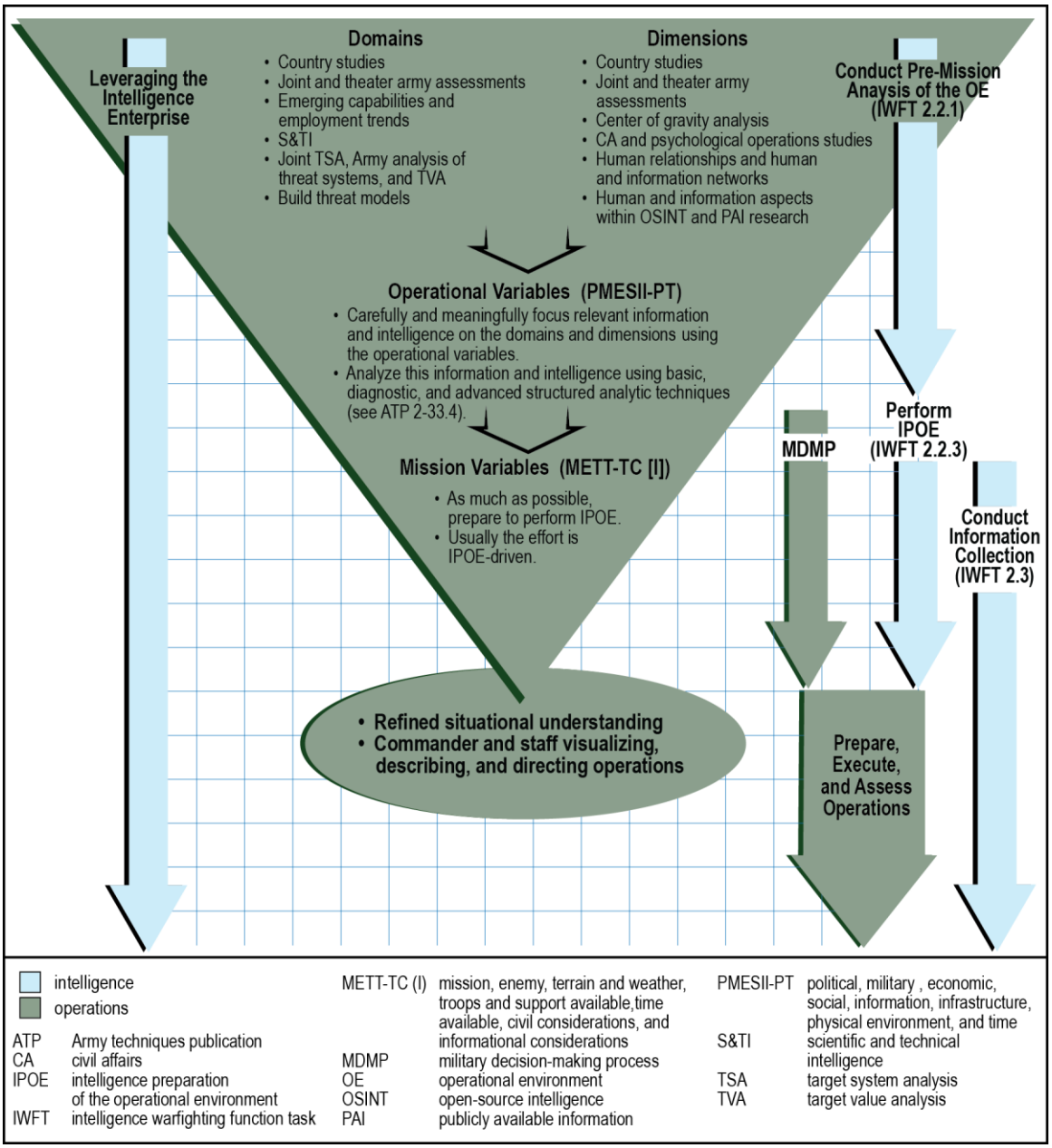


Figure 5-2. Key intelligence tasks that support understanding the operational environment

PLAN, ESTABLISH, AND REVISE AN INTELLIGENCE ARCHITECTURE

5-11. As discussed in chapter 1, the intelligence architecture has an important role in providing intelligence support. The G-2/S-2 and the intelligence staff plan, establish, and revise the intelligence architecture in close collaboration with higher-level and subordinate G-2/S-2s and the MI unit commander and staff at that echelon. Additionally, the intelligence staff must coordinate with key members of the staff, especially the G-6/S-6 and G-3/S-3. (See chapter 8 for the intelligence architecture during large-scale combat operations.)

5-12. The intelligence architecture consists of more than a unit's organic collection capabilities, systems, and personnel. It also includes all elements of the intelligence network and associated communications architectures (including the PACE communications plan) to enable intelligence operations and support to mission requirements. (See FM 6-02 for doctrine on PACE planning.)

PLANNING

5-13. Planning the intelligence architecture is inseparable from long-range planning for future intelligence operations. The intelligence staff can neither perform long-range planning without carefully considering the intelligence architecture nor plan an intelligence architecture without carefully considering long-range planning. The intelligence architecture is connected directly to the types and methods of intelligence support necessary for future operational plans. This planning is roughly equivalent to developing a blueprint for a house that is based on a larger plan to build a housing area in that area. The unit cannot count on using intelligence capabilities during an operation if those capabilities are not accounted for in the intelligence architecture and supported by a larger communications plan. Once the intelligence architecture is in place and the unit is conducting operations, periodic changes are necessary; these changes are called revisions.

5-14. When developing the intelligence architecture, the intelligence staff collaborates with the MI unit staff to consider the personnel, organizations, systems, and procedures necessary for developing intelligence, including those required for intelligence operations. It is critical for the intelligence staff to collaborate with the commander and staff as early as possible and throughout planning to ensure the intelligence architecture is adequately planned and established as soon as possible.

5-15. The G-2/S-2 and intelligence staff also ensure the higher-headquarters linkage to the unit and subordinate unit requirements are adequately integrated into their intelligence architecture to enable effective information collection, PED, and analysis and production to support mission requirements. This ensures the intelligence architecture supports the necessary operational and technical connections between collection assets, control elements, PED capabilities, analytical cells, and various CPs to enable an effective information flow of intelligence to commanders and staffs and access (both inward and outward) across the intelligence enterprise. The intelligence architecture must also account for all complementary capabilities and intelligence-related missions and operations employed by the unit.

ARCHITECTURE DETAILS

5-16. 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 planning products include but are not limited to the different—

- **Intelligence capabilities.** Chapter 7 provides a list of organic and supporting general intelligence collection and all-source intelligence capabilities by echelon; each general intelligence collection capability comprises specific collection assets (platforms and collectors) with specific technical collection capabilities and associated PED. The intelligence staff must compile a list of all appropriate general intelligence capabilities that are part of the architecture, which must address bandwidth requirements, preparing for operations, collecting the required information, and the associated PED. The intelligence staff must then assess all applicable general intelligence capabilities to list the specific intelligence capabilities required for the architecture.
- **Communications means.** Collection assets operate through many different communications means, which include formal message traffic, databases, product libraries, chat rooms, intelligence dissemination systems, and various voice methods.
- **Technical networks.** Technical networks are those information management and information system connections that enable resource and information sharing. Intelligence architecture products capture not only networks and their technical specifications but also how architecture elements relate and interoperate with each other. Intelligence personnel disseminate and access information and intelligence on several networks, including NIPRNET, SIPRNET, JWICS, coalition networks, and intelligence broadcast systems.
- **Tactical considerations.** The intelligence architecture should address likely tactical considerations such as mission tasks, technical control means, tipping and cueing, IEW and other maintenance, security measures, and medical support.

COLLECTION MANAGEMENT

5-17. *Collection management* is, in intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required (JP 2-0). Collection management includes ensuring information collection, intelligence reach, RFIs, and requests for collection result in adequate information, combat information, and intelligence to support operations. (See ATP 2-01.)

Note. In the Army, tasking authority derives from the commander and resides with the G-3/S-3. Within Army operations, neither the collection manager, G-2/S-2, nor intelligence staff members have tasking authority. To retask an asset, the G-2/S-2 must closely collaborate with the G-3/S-3, as well as address information collection issues within the COIC so intelligence is continually ready to support decision making, targeting, and other aspects of operations. It is important for the collection manager, ACE or BISE chief, and the appropriate G-3/S-3 representative to quickly work through information collection issues.

5-18. Collection management is the primary driver for overall information collection planning, as discussed in paragraph 3-30. The overlap of collection management and information collection planning occurs in the—

- Development of the collection management plan.
- Use of intelligence handover lines and other graphic measures.
- Feasibility and details of employing ground reconnaissance.
- Planning of fires and sustainment to support the information collection effort.

5-19. The following are inherent in conducting collection management:

- Intelligence reach and RFIs.
- Monitoring available collection assets and assessing their ability to provide the required information.
- Recommending adjustments to new requirements or locations of collection assets, if required.
- Collection orchestration, as part of the operational-level model.

COLLECTION MANAGEMENT AND INTELLIGENCE ANALYSIS

5-20. During any phase of military operations, CCIRs are critical to the commander's decisions and staff control. The intelligence warfighting function focuses on answering intelligence requirements. Both collection management and intelligence analysis are driven by PIRs, targeting intelligence requirements, and other intelligence requirements that subsequently drive the development of specific information requirements (SIRs). SIRs assist in tasking or requesting collection assets to collect information that results in effective intelligence that answers the commander's requirements.

5-21. Collection management supports the intelligence analysis process and intelligence analysis supports the collection management process and both must account for PED activities. These activities must be synchronized, and analysts within both activities must collaborate closely to enable the intelligence warfighting function. Intelligence analysis sets the stage for collection management, which includes developing information requirements that later result in intelligence requirements that drive effective information collection. This enables intelligence analysts to answer the commander's intelligence requirements. The intelligence staff conducts collection management in collaboration with the operations staff to collect, process, and analyze information that affects operations. (See ATP 2-33.4 for doctrine on intelligence analysis.)

COLLECTION MANAGEMENT FUNCTIONS

5-22. The collection management functions—requirements management, mission management, and execution management—provide a useful way of viewing collection management as a whole. They also provide a potential means of structuring the collection management team and filling positions. These functions divide those processes and tasks associated with collection management to assist the collection management team in collaborating with and synchronizing information collection across the staff, various echelons, and other units and organizations.

5-23. Army and joint doctrine have their own doctrinal models for the collection management functions. The Army developed its model (except for execution management) based on its tactical-level point of view; the joint force developed an operational-level model. Similar to the intelligence process, each model represents a framework that guides thought; they are not prescriptive. Units can use either the Army or joint model based on whichever is most useful to their needs. (See ATP 2-01.)

A Tactical-Level Model

5-24. Collection management teams consider the commander's information collection guidance, information requirements (which become intelligence requirements), IPOE outputs, and intelligence analysis in the context of friendly operations in order to develop an effective collection management plan. During collection management, the three functions effectively divide the collection management effort, ensuring its success. (See figure 5-3.)

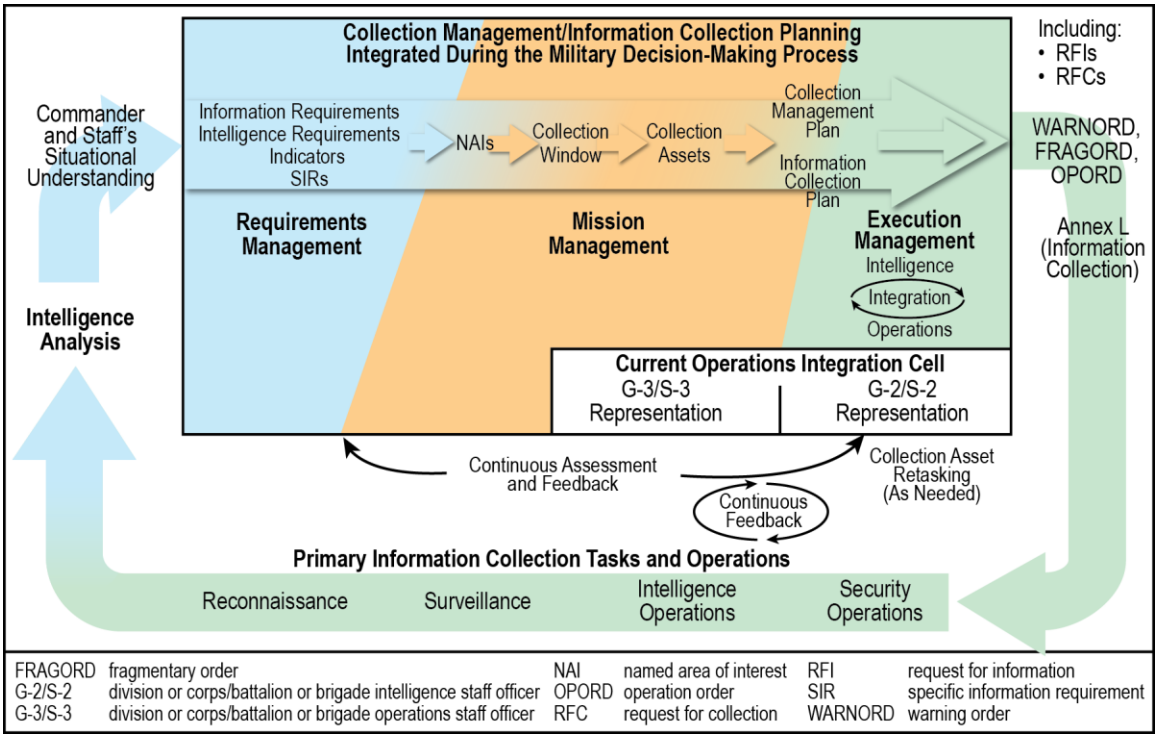


Figure 5-3. Collection management using the Army tactical-level model

An Operational-Level Model

5-25. JP 2-0 describes the distinct functions of collection requirements management (CRM), collection operations management (COM), and collection orchestration in a joint intelligence context and provides some useful and detailed techniques associated with these functions. Units can adapt this joint operational-level model to Army operations with some modifications. For example, units can use this model at higher echelons during inherently joint operations or during operations that require significant interactions with a joint headquarters.

5-26. At the appropriate echelons, Army collection orchestration is the integration, synchronization, and optimization of the intelligence process and operations, including national and theater collection integration; all-domain, multidiscipline collection strategy development; and the end-to-end synchronization of CRM, COM, reconnaissance, DOD ISR mission management, and PED.

Note. Collection orchestration outside of the operational-level model for collection management belongs to the G-3/S-3, who has overall responsibility for information collection and tasking collection assets to conduct information collection.

5-27. In the joint operational-level model, collection management teams also consider the commander's information collection guidance, information requirements (which become intelligence requirements), IPOE outputs, and intelligence analysis in the context of friendly operations to develop an effective collection management plan. The most significant modification required to use this model for Army operations is accounting for the G-3/S-3's information collection requirements. (See figure 5-4.) The G-3/S-3—

- Integrates information collection during plans and operations in coordination with the rest of the staff.
- Is the only staff officer with tasking authority from the commander.
- Can authenticate all plans and orders and synchronize all warfighting functions in time, space, and purpose.

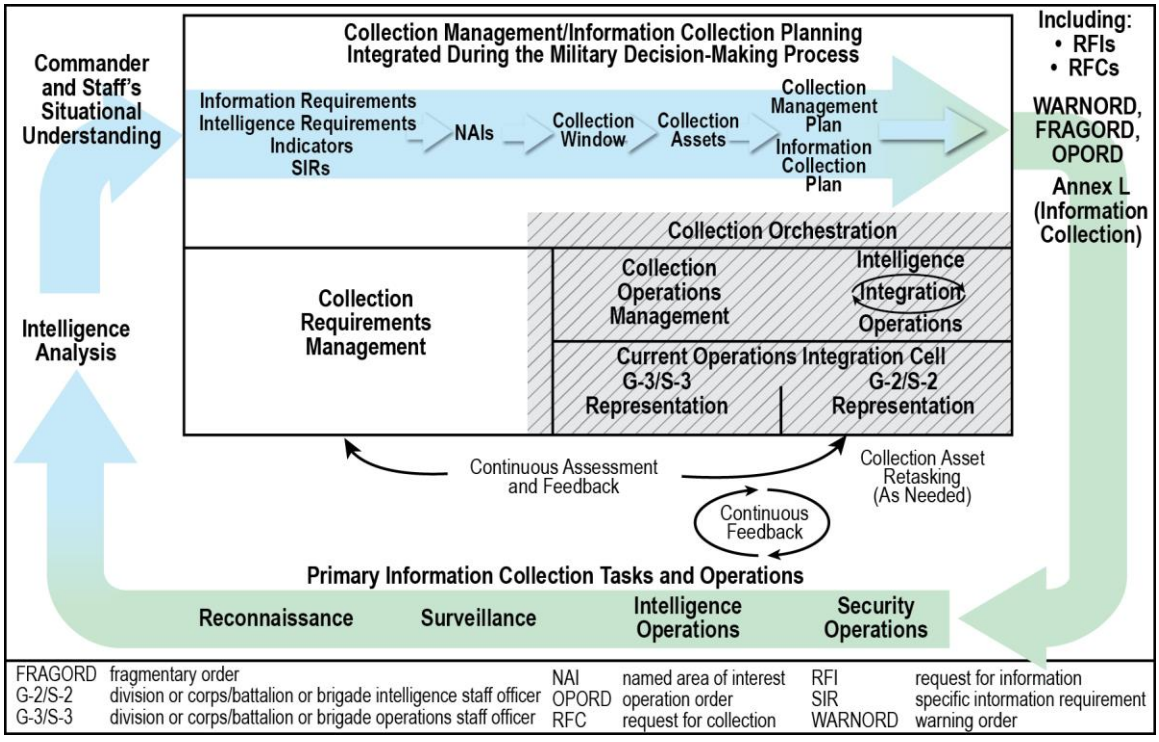


Figure 5-4. Collection management using the joint operational-level model

COLLECTION MANAGEMENT PROCESS

5-28. Conducting the complex and detailed tasks associated with collection management is inherent in the collection management process. Based on the commander and staff's participation, the collection management team, in close coordination with the operations staff, performs the five tasks of the collection management process—each discussed in detail in ATP 2-01:

- Develop requirements.
- Develop the collection management plan.
- Support tasking and directing.

- Assess collection.
- Update the collection management plan.

5-29. The collection management tasks are continuous but not necessarily sequential; they are the basis for creating, tasking, and executing the information collection plan. (See figure 5-5.) This is accomplished through the challenging balance of—

- Developing requirements that effectively support operations during *requirements management*.
- Developing recommendations to task collection assets, including associated details such as the *where*, *when*, and *how* for that collection, and coordinating with those assets or their C2 element to ensure an effective information collection effort throughout the entire operation during *mission management.*
- Ensuring a continuous integrated and synchronized information collection effort through timely and flexible adjustments to collection throughout the operation during *execution management*.

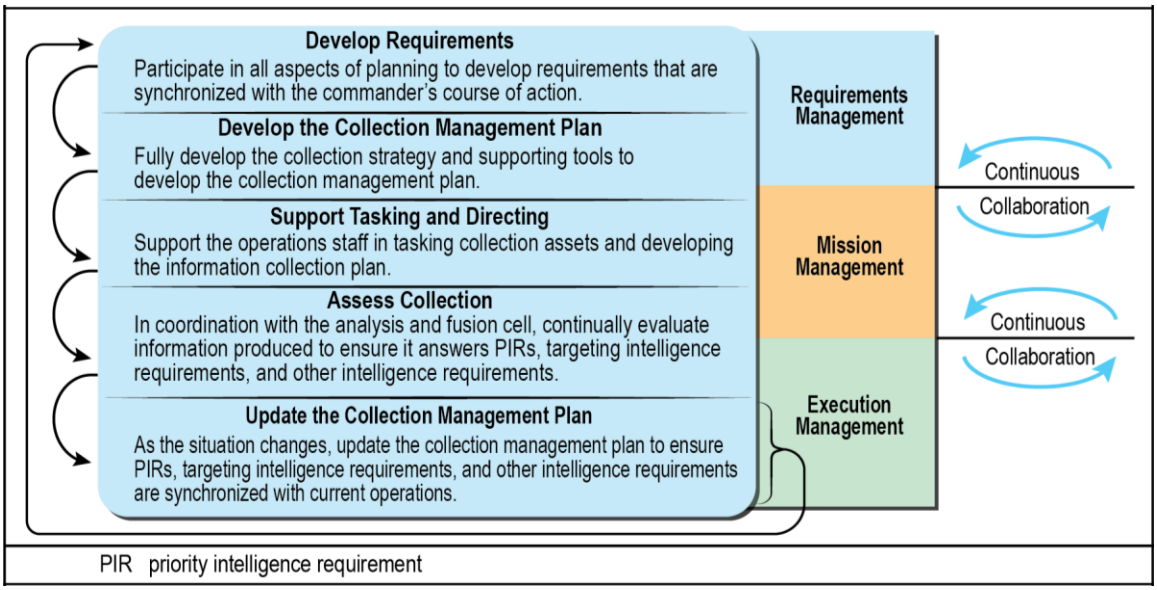


Figure 5-5. The collection management process

5-30. Effective collection management focuses on answering intelligence requirements by analyzing these requirements, planning collection based on tasks to collection assets, and then assigning these tasks in an order. The collection management plan synchronizes and coordinates collection assets and PED in the overall concept of operations, and positions and tasks collection assets so they can collect the right information, shift priorities as the situation develops, or execute a branch or sequel.

Note. *Concept of operations* is a statement that directs the manner in which subordinate units cooperate to accomplish the mission and establishes the sequence of actions the force will use to achieve the end state (ADP 5-0).

THE INTELLIGENCE ANALYSIS CONTINUUM

5-31. There is far more to intelligence analysis than simply IPOE. Intelligence analysis must support the commander's decisions, situational understanding, ADM, the MDMP, information advantage activities, targeting, planning and executing deception operations, force protection considerations, and continuous operational assessments. In any operation, friendly and enemy forces will endeavor to set conditions to develop positions of relative advantage. Setting these conditions begins with pre-mission analysis of the OE, which provides relevant knowledge about the OE that is incorporated into the ADM and then used later during other intelligence analysis tasks. (See figure 5-6 on page 5-12.)

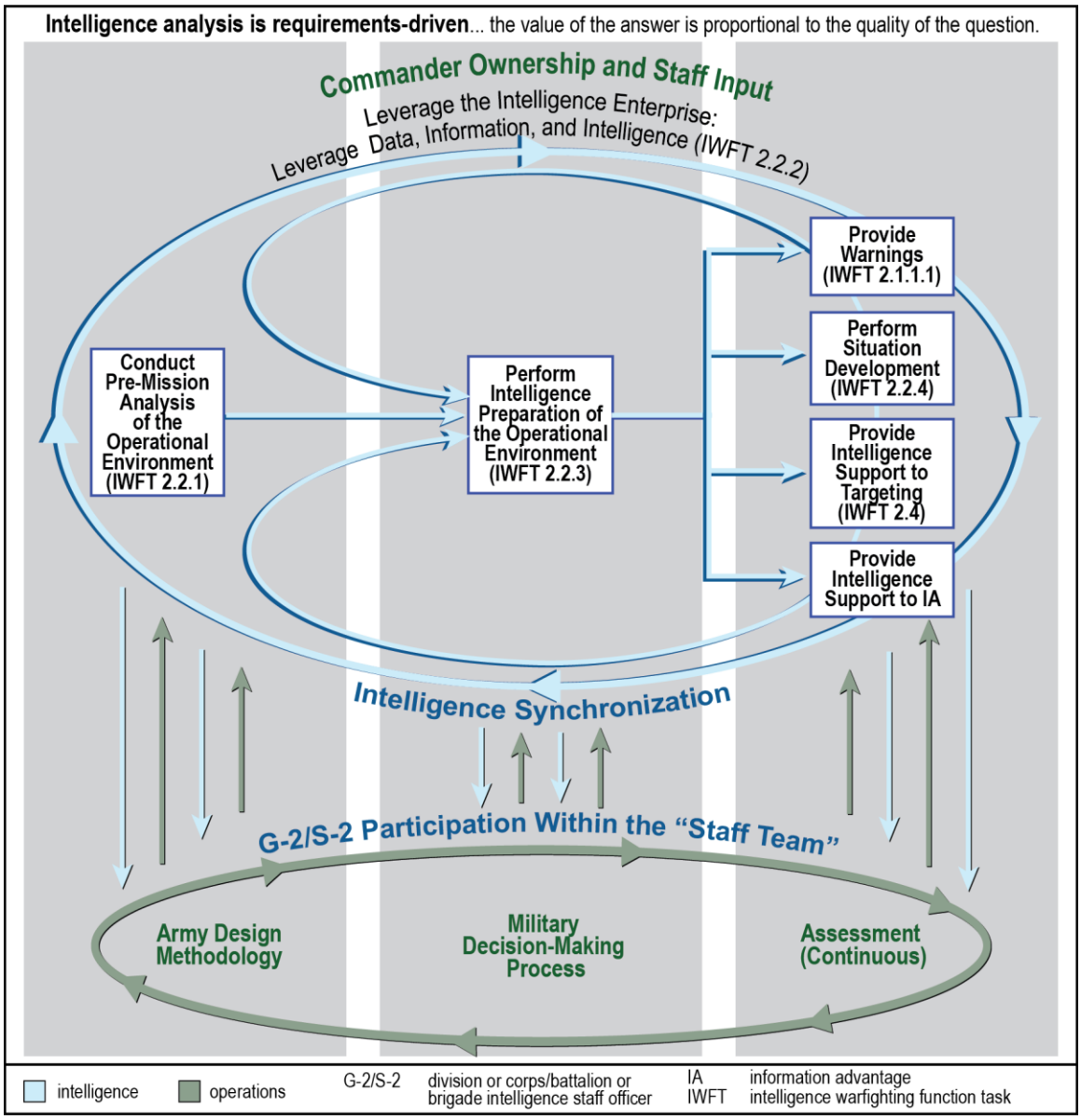


Figure 5-6. The intelligence analysis continuum

5-32. During the MDMP, the intelligence staff leads IPOE and conducts continuous intelligence analysis to understand the OE and the options it presents to friendly and threat capabilities. For example, threat databases and signatures developed during pre-mission analysis of the OE assist in assessing threat capabilities and vulnerabilities during IPOE. This information facilitates decision making during the MDMP and provides a common understanding on how friendly forces may gain positions of relative advantage across multiple domains and dimensions. This is essential when determining how best to mitigate sophisticated threat A2 and AD systems, IADSs, deception, information warfare, systems warfare, the EMS and EW, UASs, robotic capabilities, and long-range fires capabilities, as well as accounting for civil considerations in the OE.

5-33. Based on relevant aspects of the OE (determined during IPOE), including the domains and dimensions, the commander and staff continuously assess information, operations, and changes in the OE. Warnings intelligence, situation development, intelligence support to targeting, and intelligence support to information advantage activities assist the commander and staff in further shaping the OE to facilitate mission success. The continuous assessment of collected information also mitigates risk to friendly forces while identifying opportunities to leverage friendly capabilities to open a window of opportunity.

LEVERAGE DATA, INFORMATION, AND INTELLIGENCE

5-34. Several areas in this publication mention leveraging and collaborating across the intelligence enterprise and intelligence architecture but in different contexts. This task is an inherent part of intelligence support and pertains to every other task in this chapter. An echelon does not collect all the information it needs, and an intelligence staff does not conduct all the intelligence analysis and production it needs to support the commander and staff. Every echelon uses data, information, and intelligence from higher, lower, and adjacent intelligence staffs and elements.

5-35. Information outside of military sources can be valuable, especially for the operational variables (PMESII-PT) and civil considerations. Academia, industry, and non-DOD information can be especially valuable, as well as PAI, in providing critical insight and awareness across all domains and dimensions, especially the human and information dimensions. Allies and other multinational partners have unique collection capabilities and valuable intelligence, including insight into specific regions and ongoing tensions. The joint force and other Services have unique and specialized data, information, and intelligence on many areas, especially within the maritime, air, space, and cyberspace domains (including ES data and information). Generally, higher-level Army echelons have more time, resources, and a broader context to produce intelligence; lower-level echelons may often have a more detailed and timelier picture of the enemy they face in the close area. Optimizing the task of leveraging data, information, and intelligence and effectively collaborating across echelons are both an art and the application of science.

CONDUCT PRE-MISSION ANALYSIS OF THE OPERATIONAL ENVIRONMENT

5-36. To perform IPOE and the other important intelligence tasks that support operations, the intelligence staff must conduct a significant amount of analysis before receipt of mission. The intelligence staff cannot wait until receipt of mission to start intelligence analysis. As discussed in chapter 2, there are several tools and processes, some led by the G-2/S-2 and intelligence staff, that assist the commander and staff in understanding the OE. Intelligence analysis plays an important role in facilitating this understanding; therefore, the analytical effort must start as early as possible. As operational planning occurs in terms of theater campaign plans, contingency plans, and other planning (such as the ADM), the intelligence staff provides intelligence support, which is connected to facilitating an understanding of the OE through sequential analysis and developing various intelligence products. The result is an ever-increasing level of operational focus:

- Analysis and products that account for the different aspects of the domains and dimensions, including their interrelationships. ***Note.*** While considering the domains and dimensions, these intelligence products may not be structured based on the domains and dimensions.
- Analysis and products that account for the operational variables and how they interrelate.
- Analysis and products that specifically address a threat; localized terrain; weather and weather effects; civil considerations, including cultural aspects of the OE; and other significant aspects of that area to prepare the staff for the MDMP, including IPOE.

DOMAINS AND DIMENSIONS (GENERAL INTELLIGENCE)

5-37. During competition, for those units and organizations without much operational or geographic focus, the intelligence staff must first understand a threat and the regional civilian population and other significant factors (for example, destabilizing natural disasters across a region). Using the domains and dimensions as a framework provides a helpful context and checklist to ensure the intelligence staff's holdings are as complete as possible and to build a comprehensive understanding of the OE. Information and intelligence usually flow first from the U.S. IC, academia, DIA, the theater army G-2 and military intelligence brigades-theater (MIB-Ts), and other higher-echelon intelligence units and organizations (such as MDTFs [see paragraph 2-82]) in various forms. Some of this information and intelligence is or can be databased and some cannot. As this occurs, it is useful for intelligence staffs to practice their intelligence skills and compile or create intelligence products to further build their knowledge and proficiency as analysts. Analyzing and describing threat force capabilities, and even the whole of a threat government, are especially valuable in preparing for potential future operations. Producing these products should also assist intelligence staffs in finding information and intelligence gaps.

5-38. During crisis and armed conflict with a specific operational or geographic focus, as time and the situation allows, producing general intelligence products on the threat and regional civilian population is of value. The greater the level of understanding of the OE at the general or holistic level, the better the understanding of the OE for a specific mission.

OPERATIONAL VARIABLES (INTELLIGENCE FOR CONTINGENCY AND FUTURE PLANS)

5-39. The next level of operational focus is moving from generalized analysis, information, and intelligence to analysis, information, and intelligence specific to a contingency, possible operation, or known future operation. This can include the employment of ADM. In these instances, the joint force may perform joint IPOE, and higher-level Army echelons may perform a rather broad IPOE. However, lower-level Army echelons that have not received a mission do not perform IPOE yet. Another important aspect of intelligence support at this point during competition is analysis of threat systems, which is different from joint TSA. Joint intelligence and higher-level Army intelligence, even when not structured based on the operational variables, directly address one or more of the operational variables. This joint intelligence and higher-level Army intelligence flow to lower-level units and organizations.

5-40. The operational variables provide a second useful checklist, along with the domains and dimensions, to judge the completeness of intelligence products and information and intelligence gaps. The operational variables assist the commander and staff in understanding important factors, within and across the domains and dimensions, in a more focused manner and relevant to Army operations. At all echelons, intelligence staffs must practice their intelligence skills and compile or create intelligence products (focusing on one or more operational variables) to further build their knowledge and proficiency as analysts.

THREAT, TERRAIN, WEATHER, AND CIVIL CONSIDERATIONS (PREPARING FOR THE MILITARY DECISION-MAKING PROCESS)

5-41. After contingency or other future plans are established, the next level of operational focus is preparing for receipt of mission, which starts the MDMP. Data, information, and intelligence focused on a specific threat (including the human and information dimensions), as well as localized terrain, weather and weather effects, and civil considerations (including the human and information dimensions) are invaluable to successfully performing IPOE. Beyond compiling data, information, and intelligence from other sources, conducting analysis and developing intelligence products for these categories are very similar to performing steps 2 and 3 of the IPOE process. While all aspects of building as much data, information, and intelligence are important, it is especially crucial to prepare detailed threat characteristics, models, and capabilities (considering the dimensions and domains), as much as possible, before receipt of mission.

PERFORM INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

Notes. IPOE should not be confused with joint IPOE. IPOE is used during Army operations; joint IPOE is used by joint headquarters and joint units. JP 2-0 describes joint IPOE differently than the conduct of the Army's IPOE.

Intelligence preparation of the operational environment **is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations**. IPOE was previously known as intelligence preparation of the battlefield (IPB). FM 2-0 has changed the term from IPB to IPOE to better reflect the multidomain aspects of the OE within the name of the process. However, IPB has already accounted for and discussed the domains and dimensions of the OE across its four steps; therefore, there is no change to the definition of IPOE, which matches the definition of IPB, and there is no change to the four steps of IPB, now IPOE. Despite the name change, readers should still refer to ATP 2-01.3.

5-42. IPOE allows commanders and staffs to start from a mission-focused holistic approach to analyze the OE to support the mission. The approach—

- Describes all relevant aspects of the OE that may impact friendly, threat, and neutral forces.
- Considers all relevant domains and dimensions that may impact friendly and threat operations.
- Identifies windows of opportunity to leverage friendly capabilities against threat forces to reach a position of relative advantage (human, information, or physical).
- Allows commanders to leverage positions of relative advantage at a time and place most advantageous for mission success with the most accurate information available.

5-43. IPOE results in intelligence products used during the MDMP to assist in developing friendly COAs and decision points for the commander. Additionally, the conclusions reached and the products (which are included in the intelligence estimate) developed during IPOE are critical in planning information collection and conducting targeting. When discussing IPOE, it is natural to discuss the various IPOE products; however, the following outcomes of the IPOE process are as important as developing IPOE products:

- Collaboration across the staff and with the commander.
- Effective consideration of the range of possible threat COAs and capabilities (not just the most dangerous and most likely).
- Careful analysis and detailed consideration of the terrain, weather, and significant mission and/or operational variable considerations.
- A fair and accurate portrayal of the threat during COA development and analysis (war game).

5-44. The G-2/S-2 and intelligence staff lead the staff effort, but IPOE must include the entire staff—at least during key portions of the process. Often IPOE's success is either set or not set, depending on what has occurred before IPOE. This intelligence effort applies the IWFTs of—

- Plan, establish, and revise an intelligence architecture.
- Leverage data, information, and intelligence.
- Conduct pre-mission analysis of the OE.

MISSION FOCUS

5-45. Upon receipt of a WARNORD or mission (or in anticipation of a mission), the commander and staff draw relevant information categorized by the operational variables and filter it into the mission variables (METT-TC [I]) used during mission analysis. During IPOE, the staff focuses on the relevant aspects of the OE regarding the staff's warfighting function. The staff focuses primarily on the mission variables of enemy, terrain and weather, and civil considerations. However, based on the staff's echelon, type of OE, type of operation, and changes in the OE, the staff may need to account for other significant aspects of the OE.

5-46. To be effective, IPOE must—

- Consider all domains and dimensions.
- Define the commander's AOI by its geographic boundaries and across all domains to focus collection and analysis within the AOI.
- Describe how the enemy, terrain and weather, and civil considerations will affect friendly and threat operations. This subtask involves the commander and the entire staff collaborating to determine these effects. No matter how complex, the staff must thoroughly consider the civil considerations (including information) that are significant to the mission.
- Include relevant aspects of the OE that relate to relative advantages and defeat or stability mechanisms.
- Support each step of the MDMP with IPOE products.
- Consider the operational framework. (See chapter 2.)
- Facilitate the commander's ability to visualize the desired end state and a broad concept of how to shape current conditions into that end state.
- Support the commander in directing the intelligence effort.
- Facilitate understanding threat characteristics and threat goals, objectives, and COAs.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT PROCESS STEPS

5-47. The IPOE process consists of the following four steps:

- Define the OE.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat COAs.

Note. Although there are four steps to the IPOE process, IPOE must seamlessly combine with pre-mission analysis of the OE; the leveraging of data, information, and intelligence; and situation development to serve as a continuous effort, with all staff members providing support to the intelligence warfighting function. Continuous analysis and assessments are necessary to maintain situational understanding of the OE in constant flux.

Step 1—Define the Operational Environment

5-48. An OE for any specific operation comprises more than the interacting variables that exist within a specific physical area. It also involves interconnected influences from the global or regional perspective (such as politics, economics) that affect OE conditions and operations. Thus, each commander's OE is part of a higher commander's OE. Defining the OE results in the identification of—

- Significant characteristics of the OE that can affect friendly and threat operations.
- Gaps in current intelligence holdings.

5-49. Step 1 is important because it assists the commander in defining relevant aspects of the OE in time and space. This is equally important when considering characteristics of the domains and dimensions of the OE. Aspects of the OE may act simultaneously across the battlefield but may only factor in friendly or threat operations at specific times and locations.

5-50. During step 1, the intelligence staff must identify those significant characteristics related to the mission variables of enemy, terrain and weather, and civil considerations that are relevant to the mission. The staff evaluates significant characteristics to identify gaps and initiate information collection. The staff then justifies the analysis to the commander. Failure to identify or misidentifying the effect these variables may have on operations at a given time and place can hinder decision making and result in developing an ineffective information collection strategy. During step 1, the AO, AOI, and area of influence must also be identified and established.

5-51. Understanding friendly and threat forces is not enough; other factors, such as culture, languages, tribal affiliations, and operational and mission variables, can be equally important. Identifying the significant characteristics of the OE is essential in identifying the additional information needed to complete IPOE. Once approved by the commander, this information becomes the commander's initial intelligence requirement, which focuses the commander's initial information collection effort and the remaining IPOE process steps.

5-52. Additionally, where a unit will be assigned and how its operations will synchronize with other associated operations must be considered. For example, the intelligence staff should be forming questions about where the unit will deploy within the entire theater and the specific logistics requirements to handle the operation's contingency plans.

Step 2—Describe Environmental Effects on Operations

5-53. During step 2 of the IPOE process, the staff describes how significant characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect threat forces. This evaluation focuses on the general capabilities of each force until the development of threat COAs in step 4 of IPOE and friendly COAs later in the MDMP. The entire staff determines the effects of friendly and threat force actions on the population.

5-54. If the intelligence staff does not have the information required to form conclusions, it uses assumptions to fill information gaps—always careful to ensure the commander understands when assumptions are used in place of facts to form conclusions.

Step 3—Evaluate the Threat

5-55. The purpose of evaluating the threat is to understand how a threat can affect friendly operations. Although threat forces may conform to some of the fundamental principles of warfare that guide Army operations, these forces have obvious, as well as subtle, differences in how they approach situations and problem solving. Understanding these differences is essential to understanding how a threat force will react in each situation.

5-56. Threat evaluation does not begin with IPOE. The intelligence staff conducts threat evaluations and creates threat models during the pre-mission analysis of the OE. Using this information, the intelligence staff refines threat models, as necessary, to support IPOE. When analyzing a well-known threat, the intelligence staff may be able to rely on previously developed threat models. When analyzing a new or lesser-known threat, the intelligence staff may have to evaluate the threat and develop threat models during the MDMP's mission analysis step. When this occurs, the intelligence staff relies heavily on the threat evaluation conducted by higher headquarters and other intelligence agencies.

5-57. In situations where the mission is not oriented on a threat force, intelligence analysis and intelligence products may focus on terrain, weather, and civil considerations. (An example of this type of situation is a natural disaster.) However, IPOE must consider potential hazards and threats, such as terrorism, to any operation, as well as how friendly forces are under constant observation and contact by peer threats.

Step 4—Determine Threat Courses of Action

5-58. During step 4, the intelligence staff identifies and develops possible threat COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during the COA steps of the MDMP. Identifying and developing valid threat COAs minimize the potential of surprise to the commander by an unanticipated threat action and support the development of important branches and sequels.

5-59. Failure to fully identify and develop valid threat COAs may lead to the development of an information collection strategy that does not provide the information necessary to confirm what COA the threat has taken, potentially resulting in friendly forces being surprised and possibly defeated. When needed, the staff should identify all significant civil considerations (those identified as OE significant characteristics) to portray the interrelationship of the threat, friendly forces, and population activities.

5-60. The staff develops threat COAs in the same manner friendly COAs are developed. ADP 5-0 provides a model for developing valid threat COAs that are suitable, feasible, acceptable, unique, and consistent with threat doctrine or patterns of operation. Although the intelligence staff has the primary responsibility for developing threat COAs, it needs assistance from the rest of the staff to present the most accurate and complete analysis to the commander.

Intelligence Preparation of the Operational Environment Products

5-61. While there are other important IPOE process outcomes, the development of several IPOE products is also important. These products assist in driving subsequent steps of the MDMP, targeting, collection management, protection, risk management, other processes, and the conduct of IPOE at lower echelons. While not all inclusive, figure 5-7 on page 5-18 shows the flow of common products across IPOE's four steps.

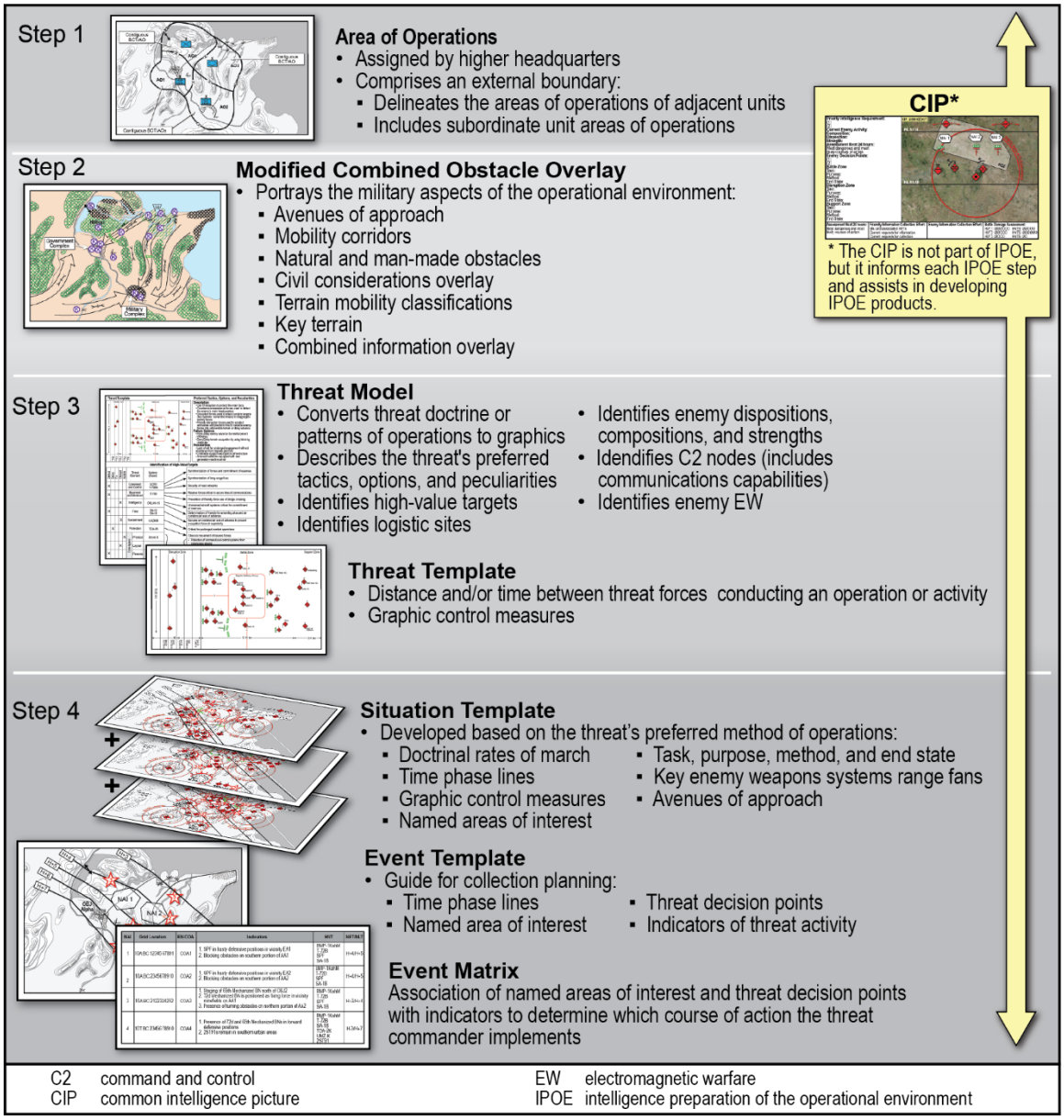


Figure 5-7. Common intelligence preparation of the operational environment products

PROVIDE WARNINGS

5-62. Across the range of military operations, various collection assets provide early warnings of threat action. As analysts screen incoming information and message traffic, they provide the commander with advanced warnings of threat activities or intentions that may change the basic nature of the operation. These warnings enable the commander and staff to quickly reorient the force to unexpected contingencies and to shape the OE.

5-63. Analysts can use analytic techniques and their current knowledge databases to project multiple scenarios and develop indicators as guidelines for providing warning intelligence. An *indicator* is, in intelligence usage, an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action (JP 2-0). Analysts project future events and identify event characteristics that can be manipulated or affected. Characteristics that cannot be manipulated or affected should be incorporated into unit SOPs as warning intelligence criteria. (See ATP 2-01 and ATP 2-01.3 for doctrine on indicators.)

PROVIDE INTELLIGENCE SUPPORT TO TARGETING

5-64. Commanders and staffs need timely, accurate, relevant, and predictive intelligence to support the targeting effort, which includes the selection, prioritization, execution, and assessment of targets. Therefore, the intelligence support to targeting effort must be resourced, carefully planned, and supported by a large portion of the intelligence architecture. Intelligence support to targeting occurs across most of the intelligence warfighting function. While all intelligence disciplines and complementary capabilities support targeting, the effort is ultimately focused by the close collaboration between the all-source intelligence analysis element (whether dedicated to targeting or ad hoc), the collection management element, and various targeting and fires elements, including the target development working group, if applicable. Certain staff elements, including the USAF SWO, CEMA officer, and space operations officer, also have an important role. Intelligence support to targeting includes support to planning (target development), identifying (target detection), and assessing the effect of those operations (combat assessment).

5-65. Characteristics that best describe the intelligence support to targeting effort include deliberate planning, collaboration across intelligence enterprise echelons, and precise intelligence to target threat capabilities at the right time and place to open windows of opportunity to achieve positions of relative advantage. Unfortunately, providing precise intelligence is challenging because threats, especially peer threats, make it difficult to collect on and analyze threat systems. Intelligence analysis to predict threat COAs (considering terrain and weather effects), provide intelligence specific to a location and time, and accurately assess the employment of capabilities is difficult. Intelligence support to targeting includes tracking highly mobile targets and simultaneously engaging targets, including targets in complex terrain (such as subterranean and urban areas and jungle and mountainous terrain) and targets across multiple domains and dimensions (for example, targeting threat information systems).

5-66. The intelligence warfighting function provides support during D3A—from developing plans through the MDMP and executing the operation after the MDMP. The targeting process is continuous and so is intelligence support to targeting. Just like IPOE, intelligence support to targeting is based on the data, information, and intelligence that result from planning, establishing, and revising the intelligence architecture; conducting pre-mission analysis of the OE; and leveraging data, information, and intelligence. While not all-inclusive, figure 5-8 illustrates intelligence support to targeting before receipt of mission and during and after the MDMP.

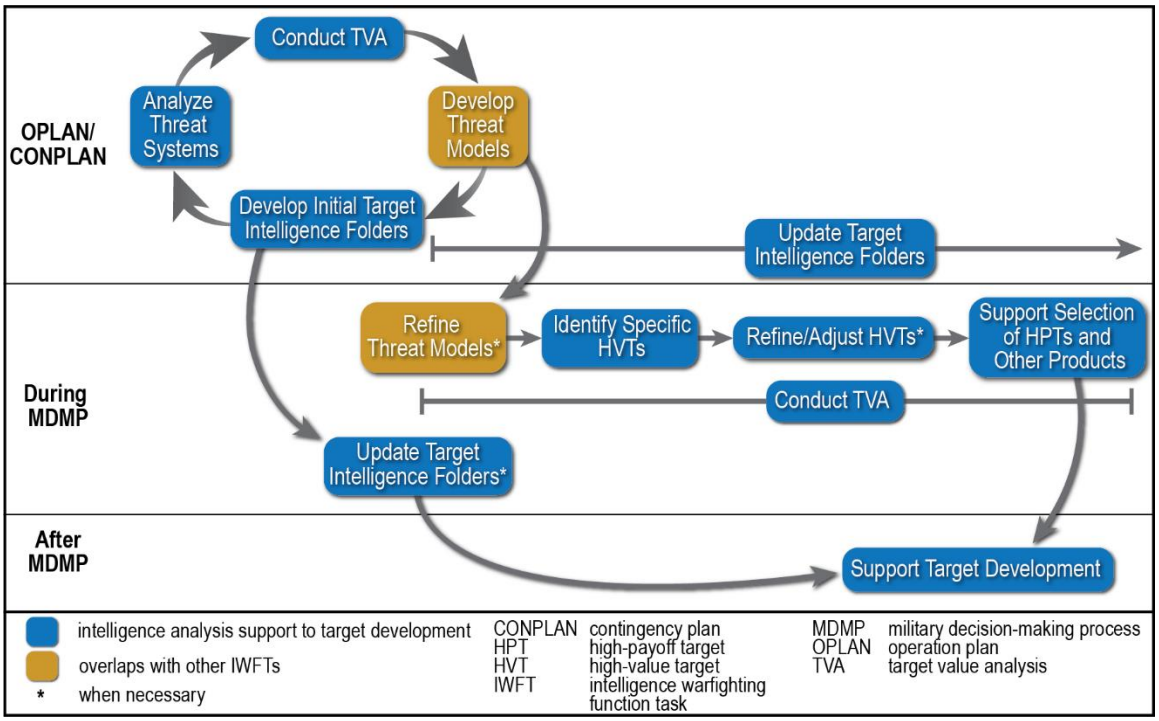


Figure 5-8. Intelligence support to targeting over time

DECIDE

5-67. During the MDMP, targeting becomes more focused based on the commander's guidance and intent. Once the commander determines objectives, the intelligence staff must continuously review them with respect to the threat and the changing situation to ensure they remain relevant to the commander's intent. Intelligence provides the commander with an understanding of the threat in terms of probable intent, objectives, strengths, vulnerabilities, and COAs (at a minimum, most likely and most dangerous). Additionally, intelligence analysts recommend objectives based on enemy capabilities, vulnerabilities, centers of gravity, and likely COAs.

5-68. The decide function of the targeting methodology provides the overall focus and sets priorities for information collection and attack planning. Decide, the most important targeting function, requires close interaction between the intelligence, plans, operations, CEMA, fire support, space, and legal. The intelligence staff analyzes threat systems and their components to make a recommendation for generating the commander's intended effect on the target, although the fire support officer, in collaboration with the G-3/S-3, makes the final decision. The intelligence input is based primarily on the AGM, determining the most effective friendly means available to produce the commander's desired effect on the target. The decide function draws heavily on the staff's knowledge of the threat, a detailed IPOE (which occurs simultaneously), and a continuous assessment of the situation. Targeting priorities are addressed for each phase or critical event of an operation.

5-69. During the targeting meeting, the collection management team advises the targeting working group on the ability of available collection systems to acquire and identify HPTs, track HPTs, and support BDA on HPTs. The team assists the working group, as needed, in revising the intelligence architecture to disseminate target-related intelligence to attack systems in near real time. The targeting working group further refines event templates and associated event matrices (developed during IPOE) into targeting matrices, which provide the level of detail the collection management team requires to focus information collection to support targeting. The team uses targeting matrices, IPOE products, and TSS to divide HPTs into collection functions (acquire and identify, track, and support BDA), SIRs, NAIs and TAIs, and specific collection tasks. (See figure 5-9.) (See ATP 2-01, ATP 2-01.3, and ATP 2-33.4.)

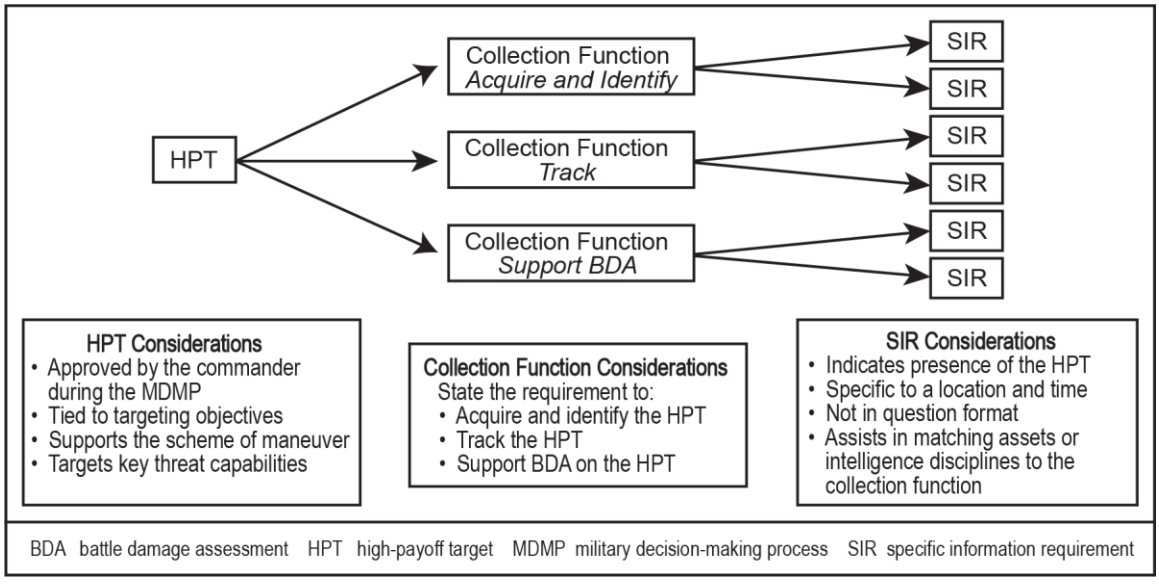


Figure 5-9. High-payoff target to specific information requirements

DETECT

5-70. The COIC is primarily responsible for directing the execution of the information collection effort to detect HPTs identified during the decide function. The intelligence cell (with the COIC) must focus its intelligence analysis efforts to support both situation development and the targeting effort. Therefore, close coordination between the intelligence cell and the FSE is critical. Key staff members in this effort include the G-3/S-3, G-2/S-2, information operations officer, FAIO, targeting officer, fire support coordinator, and fire support officer.

5-71. The collection manager directs the information collection synchronization effort, focusing on PIRs and target intelligence requirements. The collection manager ensures the information collection plan supports the finalized targeting plan. The collection management team, in coordination with the targeting team (or intelligence targeting officer), develops collection strategies to satisfy PIRs and targeting intelligence requirements. The collection management team may have to differentiate collection tasks to support the acquire and identify or track collection function when a collection asset cannot perform both collection functions. This is a major challenge during large-scale combat operations at which time the concept of persistent surveillance is often not possible. National technical means may have to serve as an intermittent form of surveillance, in conjunction with Army collection assets, to acquire and identify and track HPTs and may be one of the primary means to detect targets in the space and cyberspace domains. Some collection assets provide actual targetable information while information from other collection assets requires PED to produce valid targets.

5-72. The target priorities developed in the decide function are used to expedite the processing of targets. The collection management team—

- Plans for synchronized collection, focusing on the proper HPT at each phase in the COA.
- Plans collection to satisfy that set of SIRs, if BDA is required to support the COA.
- Plans and arranges, when possible, direct dissemination of targeting intelligence from the collector to the targeting cell or the appropriate fires element.

5-73. During operations, the collection management team—

- Monitors the execution of the collection management plan.
- Uses the information collection matrix to ensure collection assets focus on the proper HPTs (and their associated NAIs and TAIs).
- Alerts the appropriate fires element as targets of opportunity present themselves.
- Cross-cues collection assets to support the targeting effort.

5-74. When detecting an HPT, the information is quickly disseminated to the FAIO to determine if the target meets the commander's attack guidance, the target's priority, and if the target complies with TSS. To ensure target-related intelligence is disseminated quickly, the FAIO is normally collocated in the intelligence cell with communications to the FSE/fires cell. The intelligence cell also supports targeting through other means in conjunction with the CEMA cell, space operations officer, and the rest of the staff. The FAIO coordinates with the intelligence cell and disseminates target-related intelligence directly to the FSE/fires cell. If the target meets the commander's attack guidance and targeting priorities, it is actioned in accordance with the commander's intent. In those instances when the situation dictates developing a new HPT, or when the staff assesses a significant change to an existing HPT, subsequent target development must occur. HPTs have the potential to change by targeting cycle, phase, activating event, or other criteria directed by the commander. When subsequent target development is necessary, the targeting information is forwarded for intelligence analysis and the target development process must occur quickly. Upon identifying a target specified for attack, analysts pass the target to the FSE/fires cell or the appropriate staff proponent, who directs the desired prosecution of effects against the target. (See ATP 2-01, ATP 2-01.3, and ATP 2-33.4.)

DELIVER

5-75. During the deliver function, the intelligence staff analyzes threat systems and their components to make a recommendation for generating the commander's intended effect on the target although the fire support officer, in collaboration with the G-3/S-3, makes the final decision. The intelligence input is based primarily on the AGM—determining the most effective friendly means available to produce the commander's desired

effect on the target. During the deliver function, the collection management team cues collectors to continue tracking targets during its engagement. Preplanned or cued BDA collection and reporting assist in determining if the engagement produced the desired effects; if not, continued tracking supports immediate reengagement. (See ATP 2-01, ATP 2-01.3, and ATP 2-33.4.)

ASSESS

5-76. Intelligence supports the assessment function by determining if targeting actions have met the desired effects and if reattack is necessary to perform essential fires tasks and achieve the commander's intent for fires. Intelligence support to combat assessment relates to specific targets by completing physical damage assessments and functional damage assessments. During the assess function, the collection management team continuously assesses the information collection effort and compares ongoing actions to the collection management plan and the original intent. As operations progress and the situation deviates from the plan, it is important to ensure information collection supports all requirements. If the staff's assessment reveals that some requirements are not answered, the collection management team must reevaluate the collection management plan. Then the team and staff must provide input on adjustments to the collection effort, retasking, or the development of new tasks. The collection management team and current operations track the situation relative to those requirements to determine the completion of the collection task, the effectiveness of targeting and resulting effects on the target, continued synchronization with other operations or emerging collection opportunities, and most critically, the requirements for target reattack, if required.

5-77. The assess function is nested in the overall continuous assessment of operations within the operations and intelligence processes. Assessments are directly connected to the commander's decisions throughout the conduct of operations. Planning for assessment identifies key aspects of the operation that the commander directs be closely monitored and identifies where the commander wants to make the decisions. Intelligence has a major role in assessments.

5-78. The assess function is performed through *combat assessment*—the determination of the overall effectiveness of force employment during military operations (JP 3-60). Operational assessments are normally conducted only at echelons above brigade. Combat assessment is composed of three related elements: BDA, munitions effectiveness assessment, and reattack recommendations.

PROVIDE INTELLIGENCE SUPPORT TO INFORMATION ADVANTAGE

5-79. Chapter 2 discusses the OE dimensions; human, information, and physical advantages; and positions of relative advantage in accordance with FM 3-0. Initially, commanders and staffs should maintain a balanced outlook and approach to reaching human, information, and physical advantages. While not entirely new in execution, the recent doctrinal articulation of identifying and reaching advantages within and across dimensions can be somewhat complex. For example, most information advantages result from human and physical advantages, and several considerations to apply lethal and nonlethal means to reach a targeting effect span across all three dimensions. Additionally, most information advantages result from human and physical factors that are activities intrinsic to Army operations.

5-80. In many instances, especially during competition and crisis, commanders and staffs must understand many relevant aspects of the OE, including friendly and enemy capabilities and factors across the domains and dimensions, to conduct operations and activities to reach an information advantage. Additionally, commanders and staffs must understand and appreciate the complex interrelationship between the human, information, and physical dimensions from a friendly, threat, and other actors' perspective. Units and intelligence organizations should leverage the Army Cyber Command G-2 and the Cyber Military Intelligence Group, the JFC information planning cell, and the Deputy Director for Global Operations for assistance in developing information advantage-specific support requirements.

5-81. Intelligence support to information advantage includes the following:

- Support to understanding the OE, including the domains and dimensions.
- Understanding threat information warfare capabilities and ongoing activities so friendly forces can preempt with their own messaging.

- IPOE.
- Situation development.
- Collection management.
- Support to all information aspects of targeting.
- Support to countering misinformation and disinformation efforts, including OSINT support.
- Support to determining protection and security activities to mitigate threat activities.
- Many aspects of CI, including technology protection.

FM 2-0 modified the IWFTs to support information advantage:

- ART 2.4.2, *Provide Intelligence Support to Information Operations*, from FM 2-0, dated 06 July 2018, has been deleted.
- ART 2.4.2, *Provide Intelligence Support to Information Operations*, subtasks have been captured under IWFT 2.2.5, *Provide Intelligence Support to Unique Missions*. Some of the subtasks include—provide intelligence support to public affairs, military information support operations, CEMA, cybersecurity, OPSEC, and military deception. (See appendix B.) (ART Army tactical task)

PERFORM SITUATION DEVELOPMENT

5-82. The intelligence staff performs continual situation development once IPOE is completed to support the unit's MDMP. Situation development involves the logical next steps of taking IPOE and MDMP results and continuing to support the commander and staff in terms of understanding, visualizing, and decision making—except for support to targeting, which is a separate task. IPOE products are converted into threat-tracking intelligence products as well as into the development of standard intelligence products that support situational understanding and a unit/organization's battle rhythm. Analysts continually produce current intelligence to answer the commander's requirements; update and refine IPOE products, as needed; and support transitions to the next phase of an operation, branch, or sequel.

5-83. While IPOE initially shapes the development of situation development products, performing situation development is different from performing IPOE. Situation development products are more useful when key staff members collaborate with the intelligence staff. There are several standard doctrinal intelligence products associated with this task. Different units should freely modify these doctrinal products or develop their own, as long as they meet the doctrinal intent of providing relevant and timely support to the commander and staff. Some of these intelligence products include—

- Event templates and associated event matrices. (See ATP 2-01.3.)
- Intelligence estimates. (See ATP 2-33.4.)
- Intelligence running estimates. (See ATP 2-33.4.)
- INTSUMs. (See ATP 2-33.4.)
- Graphic INTSUMs. (See ATP 2-33.4.)
- Intelligence reports. (See ATP 2-33.4.)
- Periodic intelligence reports. (See ATP 2-33.4.)
- BDA charts.
- Visualization products (according to the commander's preference).

5-84. The intelligence staff can develop these products in digital, hardcopy, and/or acetate formats, depending on the echelon; various C2 and intelligence systems; DDIL communications environments; and the unit's PACE plan. Performing situation development at any echelon also depends on how commanders and staffs decide to share, integrate, and synchronize the CIP and COP across echelons.

SECTION VI – SITUATIONAL UNDERSTANDING, THE COMMON INTELLIGENCE PICTURE, AND THE COMMON OPERATIONAL PICTURE

5-85. As an operation progresses, the intelligence staff facilitates the commander and staff's situational understanding through as timely and accurate situation development as possible. Information collection at and across echelons results in combat information and the dissemination of data and information to intelligence elements for analysis and the production of intelligence. The G-2/S-2 and intelligence staff perform many activities to integrate and synchronize intelligence collection, PED, and intelligence analysis at and across echelons, including collection management. Each echelon performs information collection and also collaborates across echelons to share data, information, and intelligence, which can be maintained at or accessed by that echelon.

5-86. The fog and friction of operations and information collection, as well as time constraints, can significantly challenge the intelligence staff. As this occurs, the intelligence staff provides continuous intelligence products, within the capabilities of intelligence analysis systems, including the COP, to facilitate the commander and staff's situational understanding. The COP is the most important operational product used to establish a shared understanding between echelons. The intelligence staff provides the intelligence portion of the COP to the rest of the staff for integration into the COP. However, the G-2/S-2 ultimately succeeds or fails—not by producing any particular intelligence product or CIP; the G-2/S-2 succeeds by providing the commander what the commander needs, with respect to accurate intelligence, when the commander needs it.

5-87. Concurrent with producing intelligence, the intelligence staff collaborates across echelons to maintain a shared or common interpretation of threat locations, capabilities, objectives and intent, COAs, strengths, and vulnerabilities. While the G-2/S-2 and intelligence staff's primary responsibility is to their commander and staff, they must also continually collaborate and share products, such as the CIP and intelligence portion of the COP across echelons. This open collaboration—usually up and down at least one echelon and with adjacent units—and a common intelligence interpretation result in better intelligence for each echelon's commander and staff and supports a shared operational understanding between echelons. Figure 5-10 depicts the complex and intense effort to both support the commander and staff and collaborate across echelons with other intelligence staffs to support a common interpretation.

5-88. There are several areas where friction occurs while providing the commander and staff with intelligence to drive decision making and targeting and have a common interpretation between echelons:

- The commander can disagree with the analysis. After providing the commander with the logic, if the commander still disagrees, the G-2/S-2 and intelligence staff must adopt the commander's analysis while still considering other possible threat actions to support branches and sequels.
- The higher- or lower-level or adjacent-unit G-2/S-2 or representative can disagree with the intelligence interpretation of many threat aspects of the situation.
- Commanders across echelons can have a very different understanding, including their interpretation of the threat situation.
- Communications between echelons can be degraded, intermittent, and limited.

5-89. The intelligence warfighting function works through this friction and then resets the CIP, as needed. Resetting a common interpretation of the situation and building a new CIP are necessary as commanders make decisions, operations transition, or echelons start a new MDMP and IPOE.

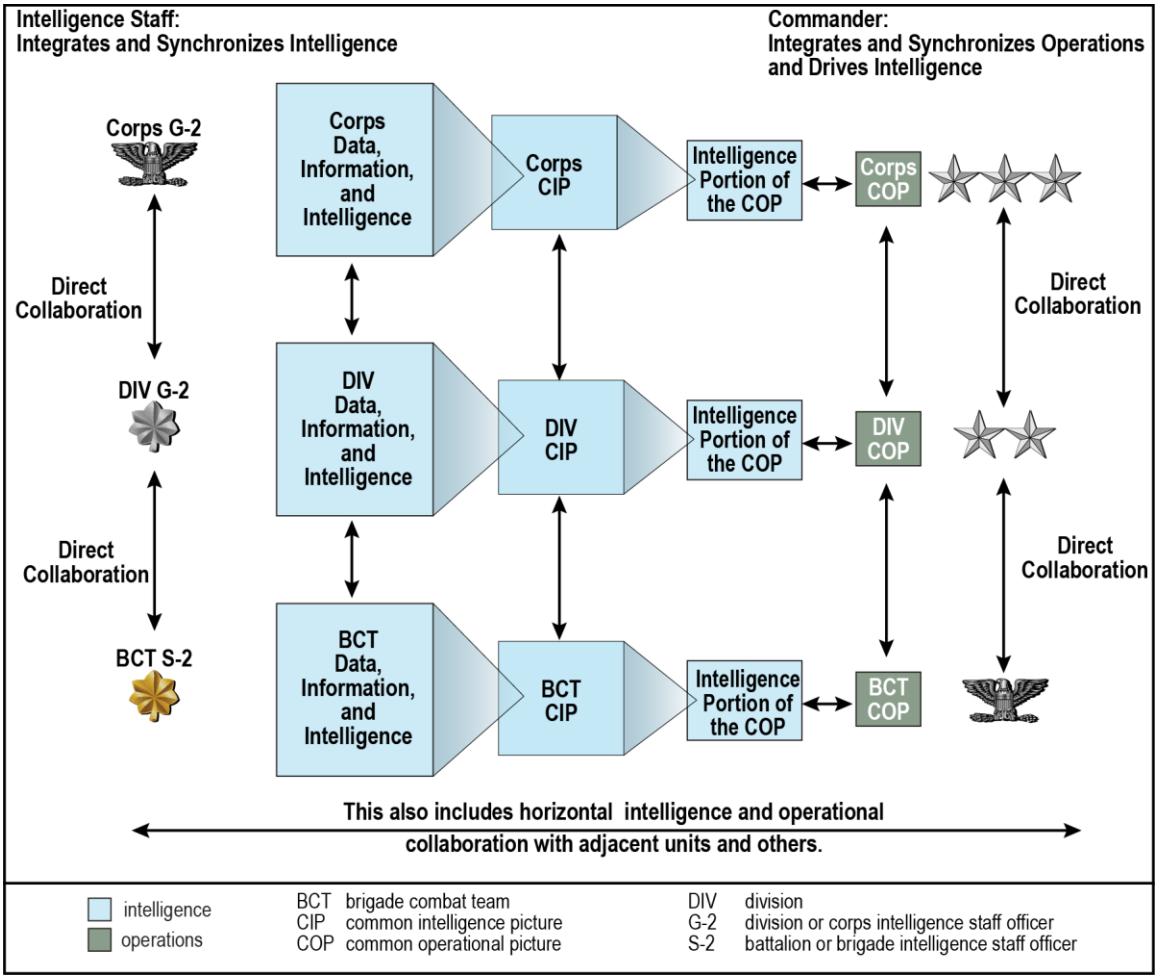


Figure 5-10. The effort to support the commander and maintain common intelligence across echelons and laterally

THE COMMON INTELLIGENCE PICTURE

5-90. The *common intelligence picture* is a single, identical display of relevant, instructive, and contextual intelligence information regarding enemy, adversary, and neutral force disposition, and supporting infrastructures derived from all sources at any level of classification, shared by more than one command, that facilitates collaborative planning and assists all echelons to enhance situational awareness and decision making (JP 2-0). For Army purposes, the CIP is viewed as a single display or any combination of displays and products that—

- Support the commander and staff's situational understanding.
- Allow the development of the intelligence portion of the COP.
- Assist collaboration between echelons to support a common interpretation of key aspects of the threat.

Note. In most instances, current technology and systems do not support a single CIP accomplishing all that is mentioned above. Therefore, the CIP can be any combination of the intelligence products discussed under situation development (see paragraph 5-83) as well as overlays, either digital or acetate.

5-91. The CIP relies on constant intelligence synchronization and continuing assessments. Specifically, the CIP is based on—

- Data, information, and intelligence from multiple echelons, organizations, and agencies.
- Leveraging the intelligence enterprise.

5-92. The commander often directs how information and intelligence should be displayed on the CIP; the G-2/S-2 and intelligence staff should ensure the information and intelligence are tailored to the commander's requirements. The following include some key aspects of the CIP:

- The CIP is derived from—
  - All intelligence disciplines, complementary capabilities, and ancillary collection assets.
  - Threat and civil considerations information across all domains and dimensions of the OE.
- The CIP is driven by unit SOPs and collaboration up and down one echelon.

5-93. G-2/S-2s must consider the following (not all-inclusive) when developing the CIP:

- Commander's requirements.
- The unit's mission.
- CIP classification.
- Echelon of CIP development.
- CIP management procedures.
- Available intelligence architecture and bandwidth.
- Types of information to be displayed.
- How information is to be displayed.
- Dissemination and ingestion methods and procedures.
- Reporting timelines.

5-94. The CIP focuses on describing the OE, the threat, and threat COAs. This product should have both a visual and textual component. If organized appropriately, both components will convey a clear and relevant threat narrative consistent with operational terminology. Intelligence staffs must exercise high control over the threat narrative to ensure consistency, which supports the commander and staff's situational understanding. Chapter 8 discusses developing the CIP during large-scale combat operations.

INTELLIGENCE PORTION OF THE COMMON OPERATIONAL PICTURE

5-95. The G-2/S-2 and intelligence staff carefully consider what aspects of the CIP to disseminate to the operations staff as the intelligence portion of the COP. The *common operational picture* is a display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (ADP 6-0). Although the COP is ideally a single display, it may include more than one display and information in other forms, such as graphic representations or written reports, automatic updates, and overlays, often digitally stored in a common database. The intelligence portions of the COP are those messages and overlays relating to threats, terrain and weather, and civil considerations in the common database. The G-2/S-2 and intelligence staff ensure the common database reflects the most current information and intelligence available to maintain the timeliness, accuracy, and relevancy of the intelligence portion of the COP.

5-96. The commander and staff must account for and mitigate any limitations in the COP based on the C2 system and technology used to generate the COP. The threat situation and civil considerations portions of the COP, while updated by the intelligence staff regularly, are sometimes limited to displaying somewhat latent and composite locations and threat force dispositions. *Somewhat latent* indicates that in most situations, those locations were captured at a specific time and are not automatically updated. *Composite* indicates that in some situations, those locations were captured across multiple dates/times. The intelligence portion of the COP may also require further explanation from the intelligence staff or other intelligence products due to the complexity of the threat situation and mission variables.

5-97. With the complexity of the OE, the intelligence staff must be prepared to—

- Validate and maintain the threat portions of the COP in a timely and flexible manner.
- Collaborate with the rest of the staff to ensure the appropriate operational and mission variables are displayed.
- Effectively display the multiple types and layers of information the commander requires.

5-98. A COP is key to achieving and maintaining shared situational understanding in all domains and making effective decisions faster than the threat. The difficulty of maintaining a COP in a multinational environment varies based on training levels, language differences, level of data sharing, technical compatibility of systems, restrictions based on classification, and other national caveats.

5-99. The COP facilitates collaborative planning and assists commanders at all echelons in achieving shared situational understanding. The COP must consider relevant factors in domains affecting the operation as well as provide and enable a common understanding of the interrelationships between actions and effects through the human, information, and physical dimensions. Shared situational understanding allows commanders to visualize the effects of their decisions on other elements of the force and the overall operation.

This page intentionally left blank.

Chapter 6
Intelligence Operations

SECTION I – OVERVIEW

6-1. MI unit collection operations (intelligence operations) follow the Army's framework for exercising C2—the operations process. The major C2 activities conducted during operations are planning, preparing, executing, and continuously assessing. Intelligence commanders, supported by their staffs, use the operations process to drive the conceptual and detailed planning necessary to direct, lead, and assess intelligence operations.

6-2. Through intelligence operations, MI collection personnel and systems collect information about capabilities, activities, disposition, and all other threat characteristics within the OE. Intelligence professionals follow the guidance outlined by the intelligence disciplines and complementary capabilities to ensure all tasks are accomplished successfully and in accordance with intelligence regulations and policies.

6-3. MI collection personnel are trained and certified. MI sensors operated by MI personnel can be directed to collect information. These MI collection capabilities are distinct from other Army information collection capabilities, such as reconnaissance or surveillance. The distinction is required because intelligence collection must comply with all applicable U.S. laws and policy. (See appendix D.) Additionally, certain intelligence disciplines require specific training and certifications to conduct intelligence operations.

SECTION II – INTELLIGENCE OPERATIONS BASED ON INFORMATION COLLECTION

6-4. Information collection is the Army doctrinal construct for synchronizing and integrating the planning and employment of sensors and assets to collect information. The intelligence warfighting function's contributions to information collection include collection management and intelligence operations. Chapter 5 discusses how collection management, through the intelligence process, nests within information collection. To understand intelligence operations, intelligence professionals must also understand information collection and how intelligence operations nest within it (under the execute collection task).

INFORMATION COLLECTION AND INTELLIGENCE OPERATIONS

6-5. Intelligence operations is one of the four primary tactical tasks and missions the Army conducts as part of information collection. (See figure 6-1 on page 6-2.) The other three are reconnaissance, surveillance, and security operations.

Note. When necessary, maneuver units conduct offensive operations to collect information. This entails commanders assuming risk to determine threat characteristics in the OE. (See chapter 8.)

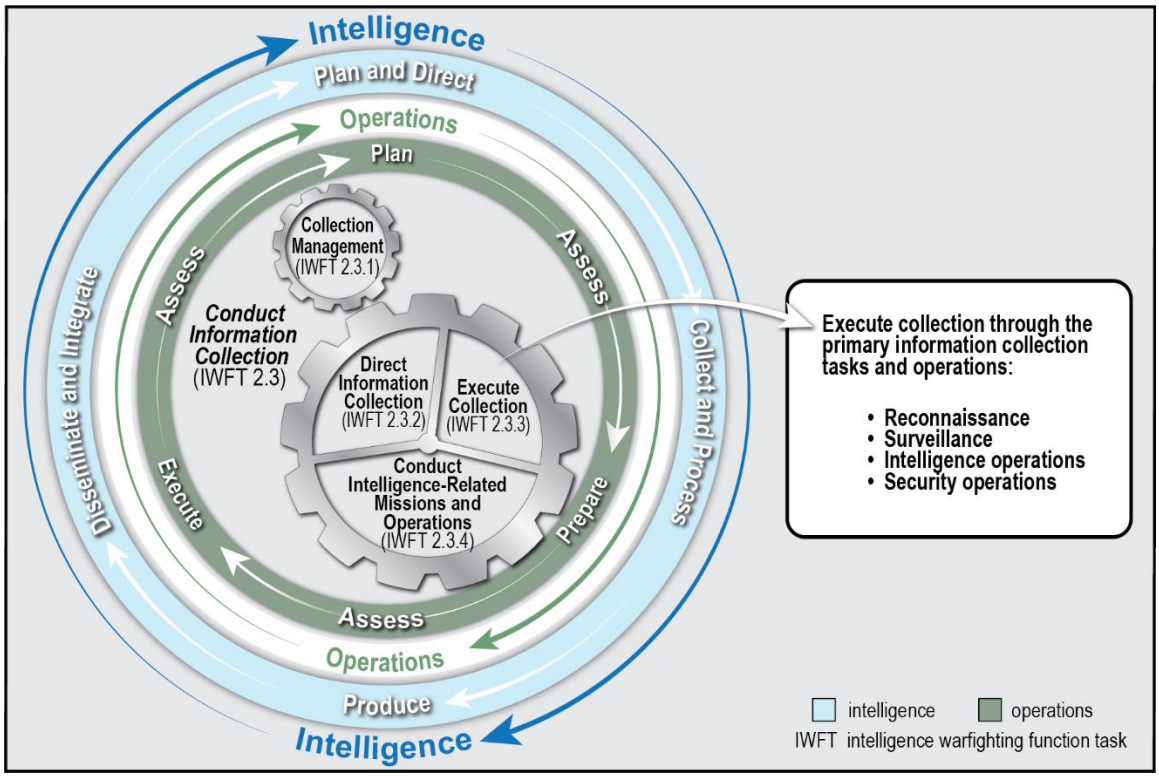


Figure 6-1. Intelligence operations as a primary tactical task

INTELLIGENCE OPERATIONS

6-6. Intelligence operations are driven by the need to answer questions and fill requirements crucial to the conduct of the supported force's overall operation. Units conducting intelligence operations follow the operations process. Collection activities acquire information and provide that information to intelligence analytical elements. Using products developed for the commander and staff, the G-3/S-3 and G-2/S-2 develop the information collection plan based on the commander's intent and concept of operations. The information collection plan is synchronized with current and future operations throughout the MDMP, especially during COA analysis (war game).

6-7. After the supported unit staff develops information collection tasks and assigns a collection mission to an MI unit, and the collection manager develops the information collection plan, the MI unit begins intelligence operations to support information collection through the execute collection task. The collection management team updates the information collection plan continuously based on post-collection and post-exploitation to determine if the collection satisfied the intelligence requirements. This effort is complex, and there is significant overlap between the supported unit intelligence staff and the MI unit. Therefore, the supported unit staff and the MI unit must collaborate closely and early-on during planning and throughout to the completion of operations.

6-8. Executing collection focuses on requirements connected to the execution of tactical missions based on the intelligence requirements. Intelligence informs commanders and staffs of where and when to look for—

- **The way:** Reconnaissance, surveillance, security operations, and intelligence operations.
- **The means:** Ranges from national and joint collection capabilities to individual Soldier observations and reports.
- **The end:** Intelligence that supports the commander's decision making.
- **The result:** The successful execution and assessment of operations depend on the effective synchronization and integration of the information collection effort.

Collection Management, Intelligence Operations, and Collaboration

The success of intelligence operations depends on the G-3/S-3, G-2/S-2, collection manager, and MI unit commander (or their representatives) closely collaborating through some complex and interrelated tasks:

- The G-3/S-3 tasks information collection, inside Annex L (Information Collection) of the unit order, based on the collection management plan.
- The collection management team, directed by the G-2/S-2, leads the development of the collection management plan.
- The MI unit must coordinate with and provide information to the collection management team during the development of the collection management plan; this is a team effort.
- The MI unit staff plans operations and produces an order, including tasks to all collection assets, based on the supported unit order, including Annex L (Information Collection).
- The G-2/S-2 and the MI unit commander must collaborate on and share responsibility for some other tasks related to intelligence operations such as maintaining the intelligence architecture, performing coordination, and planning IEW maintenance.
- The MI unit must immediately coordinate with the G-2/S-2 or collection manager, who in turn coordinates with the G-3/S-3, if there is a need to diverge from Annex L (Information Collection) tasks.

RECONNAISSANCE

6-9. *Reconnaissance* is a mission undertaken to obtain information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, geographic, or other characteristics of a particular area, by visual observation or other detection methods (JP 2-0). Reconnaissance produces information about the AO. It identifies terrain characteristics, enemy and friendly obstacles to movement, and the disposition of enemy forces and civilians so commanders can maneuver forces freely to gain and maintain the initiative. All units and personnel conduct reconnaissance; successful and effective units combine three methods to perform reconnaissance: dismounted, mounted, and aerial. Units primarily tasked to conduct reconnaissance with tailored and specialized capabilities include air cavalry and attack helicopter units, ground cavalry and scout units, chemical reconnaissance elements, engineer reconnaissance teams, and special operations forces. Chapter 8 discusses the types of reconnaissance. (See FM 3-55.)

SURVEILLANCE

6-10. Surveillance involves observing an area to collect information; the focus and tempo of this collection effort derive primarily from the commander's intent and guidance. Surveillance involves observing the threat and local populace in an NAI or TAI. Surveillance may be a stand-alone mission or part of a reconnaissance mission (particularly area reconnaissance). Surveillance is tiered and layered with technical assets that collect information; it is passive and continuous. (See FM 3-55.)

6-11. Surveillance tasks can be performed by—

- A variety of assets (in the land, maritime, air, space, and cyberspace domains).
- Means (Soldiers and systems such as artillery and air defense radars).
- Mediums (throughout the EMS).

SECURITY OPERATIONS

6-12. *Security operations* are those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow commanders to effectively use their protected forces. (ADP 3-90). Security operations are enabling operations that occur during all operations. (See FM 3-55.) Commanders usually conduct enabling operations as part of their objectives or supporting efforts. The security force uses a combination of reconnaissance and surveillance assets to accomplish its mission. Chapter 8 discusses the types of security operations. (See FM 3-55.)

INTELLIGENCE COLLECTION, THE COLLECTION MANAGER, AND THE REST OF THE SUPPORTED UNIT STAFF

6-13. The supported commander and staff plan and assess information collection at each echelon. Typically, an MI unit supports theater army, corps, division, and BCT echelons. In these cases, the MI unit collaborates closely with the supported commander and staff to plan, prepare, execute, and assess intelligence operations. Additionally, the MI unit usually serves as the means of C2 for any attached or supporting intelligence capability at that echelon. This collaboration ensures each echelon integrates and synchronizes intelligence operations from the theater strategic down to the tactical levels. For this reason, both the supported staff and MI unit staff members must thoroughly understand all aspects of the intelligence architecture, including the following capabilities:

- Collection.
- PED.
- Intelligence analysis activities.
- Technical channels.
- Procedures for IEW maintenance and other support.

COLLECTION MANAGER

6-14. If not already identified, designating a collection manager as part of the intelligence staff is vital to the success of intelligence support. The collection manager, working in conjunction with the G-2/S-2 and the rest of the staff, leads representatives from each staff section through the collection management process. (See ATP 2-01 for doctrine on the collection manager and collection management team.)

6-15. Collection managers—

- Collaborate with each staff section to understand and validate all intelligence requirements.
- Determine communications needs and procedures.
- Understand the sustainment needs of all available collection assets.
- Ensure collection times are relevant and purposeful.
- Assisted by the intelligence and operations staffs, ensure all tasked collection and PED requirements are nested and synchronized to answer intelligence requirements.

6-16. Regardless of the echelon, collection managers focus support on three distinct roles:

- Synchronizing collection to support current operations.
- Ensuring effective management and technical control across the intelligence disciplines and complementary capabilities.
- Planning support to future operations.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ASSET INTEGRATION

6-17. Joint ISR collection assets are important to Army tactical operations. In many situations, joint ISR collection is available to tactical units, providing they are not in movement and have connectivity, either through a broadcast dissemination system or within various intelligence databases. Although planning information collection starts with organic and supporting Army collection assets, Army units may receive a joint ISR asset through joint apportionment and allocation. The joint ISR process typically requires significant prior planning and approval. This is unlikely when the joint force is trying to gain access to an AO or within a highly contested OE. However, in certain situations, when an Army unit is the main effort, joint apportionment and allocation are possible.

6-18. In order to receive joint apportionment and allocation, the theater army and corps intelligence staff must determine what joint assets are available by collaborating and conducting coordination early in the joint planning process. The staff must also understand the various joint ISR scheduling and collection management tracking mechanisms, such as the air tasking order. Additionally, the staff must establish and integrate fire support coordination, air space coordinating measures, and other important coordination means, as well as plan the appropriate relationship and control means for the joint ISR assets.

STAFF CAPABILITY CONSIDERATIONS

6-19. Intelligence operations are complex. The staff must know and consider the practical capabilities and limitations of all unit organic and allocated assets. Capability considerations include the following:

- **Range.** Range deals with the collector's ability to provide target coverage. It is important for the staff to consider mission range (duration and distance) and the sensor range (how close the collection asset must be to the target to collect against it).
- **Communications.** The staff considers communications requirements from the asset to the CP. The staff determines the ability to maneuver, including transit and required collection time on specific NAIs and TAIs.
- **Day and night effectiveness.** The staff considers factors such as available optics and any effects of thermal crossover.
- **Battery/Power source life.** The staff considers how long the asset can collect and how often the battery/power source will have to be replenished to continue collection.
- **Bandwidth.** The staff considers available bandwidth and prioritizes requirements to ensure information can be continuously transmitted and accessed.
- **Expendability of asset.** The staff must consider the necessity to recover the collection asset or if it is expendable. What is the risk associated with emplacing and recovering the asset?
- **Technical characteristics.** Each asset must consider time factors (such as set-up and tear-down times) for task accomplishment. Other technical characteristics include—
  - Specific environmental threshold sensitivities for each collection asset that adversely affect or prohibit the effective use of both its platform and sensor (including factors such as terrain, weather, and soil composition).
  - Environmental effects on the collection asset (including factors such as urban or rural terrain and soil composition).
  - Whether the asset can continue to operate despite EA.
- **Reporting timeliness.** Each asset is assigned an earliest time and a latest time information reporting is of value according to the information collection plan and its supporting matrix. Other timeliness factors include—
  - How the asset transmits data/information in near real time, or how the asset should be recovered to collect the data.
  - The established reporting criteria for each collection asset.
  - How long it takes to disseminate collected information to each requester.
- **Geolocation accuracy.** Accuracy implies reliability and precision. The asset must be capable of locating a target accurately enough to engage it with precision-guided munitions.
- **Durability.** Durability includes factors such as—
  - Weather effects on the employment of the collection asset (platform and sensor payload).
  - EMS effects on the employment of the collection asset.
  - Whether the prime mover can traverse restricted terrain.
- **Detecting threat activity.** The staff considers whether the collection asset can detect the expected threat activity and whether the threat can deceive the collection capability.
- **Performance history.** Experienced staff officers must know which information collection capabilities are typically reliable to meet the commander's information requirements. Readiness rates, responsiveness, and accuracy, over time, may raise one collector's reliability factor.
- **Intelligence PED.** The staff considers whether the unit has the intelligence PED capacity, time, and architecture required to support planned and projected intelligence operations. Intelligence PED is required to conduct responsive intelligence operations to support dynamic maneuver and fire support missions. The following includes some considerations to optimize intelligence PED:
  - **Collect.** To accomplish the mission, PED units and elements must have the capability to receive collection from systems.
  - **Process.** The processing and fusion of collected data transform a larger volume of data into information and convert that information into a useable format.

- **Exploit.** PED personnel and systems quickly analyze the processed information to add operational context to the information and identify specific relevance to the mission.
- **Disseminate.** PED personnel and systems issue reports and products to provide combat information and related intelligence to commanders and operational elements. This reporting facilitates subsequent single-source and all-source intelligence, analysis, targeting, cueing of other collectors, and decision making.

SECTION III – INTELLIGENCE OPERATIONS GUIDELINES

6-20. There are guidelines for conducting successful intelligence operations. They are not checklists; rather, they describe ways to employ collection assets and develop the situation based on the commander's guidance. Mirroring the fundamentals of reconnaissance, these guidelines support efforts that result in timely collection and reporting of the accurate, relevant information needed to produce intelligence. The supported unit staff and MI unit staff must determine which guidelines to emphasize based on the situation. The following includes the intelligence operations guidelines:

- Maintain readiness.
- Ensure continuous intelligence operations.
- Orient on requirements.
- Provide mixed and redundant coverage.
- Gain and maintain sensor contact.
- Report information rapidly and accurately.
- Provide early warning.
- Retain freedom of movement.

MAINTAIN READINESS

6-21. MI unit readiness is a continuous priority through predeployment, deployment, and post deployment. Readiness is a key element during planning. The readiness of MI unit personnel and equipment impacts how MI capabilities can be leveraged to support an operation during planning. MI unit readiness also impacts the collection of information required to refine plans and issue orders and for operational execution.

6-22. As part of prepare, readiness focuses on—

- **Training.** MI commanders and leaders must establish a training plan focused on intelligence tasks and functions. This ensures MI personnel are prepared to conduct individual and collective tasks to support the unit's mission and are knowledgeable of equipment and other collection assets and databases. During training, recognizing opportunities to prepare for conventional force and special operations force (as well as joint and interagency) interdependence, interoperability, and integration can produce great dividends during operations. MI commanders and leaders that seize opportunities to collaborate with special operations and other intelligence organizations increase their understanding of each other's capabilities and facilitate interdependence, interoperability, and integration during operations. The Military Intelligence Training Standard (also known as MITS) series of publications—TC 2-19.400, TC 2-19.401, TC 2-19.402, TC 2-19.403, TC 2-19.404, and TC 2-19.405—provide information on MI training.
- **Maintenance.** This recurring event ensures intelligence assets are properly maintained and prepared to conduct information collection. For example, during planning, MI leaders should consider the availability of equipment maintainers and facilities for table of organization and equipment-based and commercial-off-the-shelf systems that may require dedicated field service representatives to provide repair and maintenance.
- **Equipment status.** The commander is ultimately responsible for equipment status. The status of collection assets must be monitored and reported to the appropriate staff elements.

- **Augmentation.** Whether in the reset-train-ready stage or preparing for a specific mission, it is necessary for MI units to identify and report any additional personnel or resources necessary to accomplish the mission. This often involves additional collection assets or specialized personnel such as linguists or technical experts.
- **Sustainment.** This involves the identification of outside resources, including the logistics, fuel, and protection necessary for mission success.

ENSURE CONTINUOUS INTELLIGENCE OPERATIONS

6-23. Commanders direct the conduct of information collection activities before, during, and after the execution of all operations. Commanders depend on intelligence to know where, when, and how best to employ forces during all military operations. Typically, collection activities begin soon after receipt of mission and continue throughout the preparation and execution of the overall operation. Collection activities do not cease after the operation concludes but continue as required:

- **Before execution** of the overall operation, intelligence operations focus on filling information gaps about all relevant aspects of the OE.
- **During execution**, intelligence operations focus on providing commanders with updated information that verifies the threat's composition, disposition, and intention as the operation progresses. This allows commanders to verify which COA the threat is actually adopting and determine if the plan is still valid based on actual events in the AO. Commanders can then make decisions, as needed, including adjustment decisions (those that modify the order to respond to unanticipated opportunities or threats).
- **After execution**, intelligence operations focus on maintaining contact with threat forces to collect the information necessary for planning subsequent operations and protecting the friendly force. In stability operations, intelligence operations often focus on relevant aspects of the AO and AOI and on the civil considerations designated by the commander.

ORIENT ON REQUIREMENTS

6-24. Commanders prioritize intelligence operations primarily by providing their guidance and intent early in planning. G-2/S-2s assist commanders in—

- Identifying and updating their PIRs.
- Ensuring PIRs are tied directly to the concept of operations and decision points.
- Focusing PIRs on their most critical needs (because of limited collection assets).
- Ensuring PIRs include the latest time information is of value (also called LTIOV) or the event by which the information is required.
- Approving requests for intelligence collection requirements beyond a unit's capabilities.
- Aggressively seeking the results of higher-echelon intelligence operations as well as the answers to information requirements across all echelons through intelligence reach.

6-25. Commanders assign information collection tasks based on a unit's collection capabilities. Therefore, commanders ensure the tasks they assign do not exceed the collection and analytical ability of their unit. When not using organic assets, commanders use previously established relationships to optimize effective operations as a combined arms team, when possible.

PROVIDE MIXED AND REDUNDANT COVERAGE

6-26. Commanders integrate their assets' capabilities to provide mixed and redundant coverage of critical locations identified during planning. The layering of collection assets through cueing, redundancy, and mixing assists in successfully answering requirements. Maximum efficiency in information collection is achieved when all collection assets are carefully employed together. The appropriate mix of collection assets assists in satisfying as many different requirements as possible. It also reduces the likelihood the unit will favor or rely on one particular unit, discipline, or system. The intelligence and operations staffs collaborate to balance requirements, available capabilities, and areas to be covered. Commanders and staffs continuously assess results to determine any changes in critical locations requiring this level of coverage.

GAIN AND MAINTAIN SENSOR CONTACT

6-27. Once a unit conducting intelligence operations gains sensor contact, it maintains that contact unless directed otherwise or the survival of the unit is at risk. In intelligence operations, gaining and maintaining sensor contact occur when the collection asset can observe or receive a signal or is observable from a person or object. Sensor contact is critical in signals intercept and imagery collection missions.

REPORT INFORMATION RAPIDLY AND ACCURATELY

6-28. Collection assets acquire and report timely and accurate information on all relevant aspects of the OE within the AOI. Collection assets report exactly what they observe and, if appropriate, what they do not observe. Seemingly unimportant information may be extremely important when combined with other information. Negative reports may be as important as reports of threat activity. To ensure collection assets report information rapidly, the intelligence staff collaborates with the signal staff to ensure communications plans incorporate collection asset communications requirements. The collection manager must establish a PACE communications plan for each collection asset and ensure it has been tested as information may quickly lose its value. Indicators and SIRs should be written such that they can be answered over the radio by a simple spot report in SALUTE format from the collection asset.

PROVIDE EARLY WARNING

6-29. Commanders and staffs position collection assets to provide early warning of threat action. Commanders use intelligence operations as part of their information collection effort to ascertain the threat COA and timing. They then orient these assets to observe these locations for indicators of threat actions. Timely and complete reporting is essential to providing early warning.

RETAIN FREEDOM OF MOVEMENT

6-30. Collection assets require battlefield mobility to successfully accomplish their missions. These assets do not engage in close combat in the execution of their collection tasks. The criticality of collection assets makes their survival the utmost consideration. If these assets are decisively engaged, collection stops, and personnel immediately execute the necessary battle drills. The collection asset leader's initiative and knowledge of the terrain, weather, and threat reduce the likelihood of decisive engagement and assist in maintaining freedom of movement. The IPOE process can identify anticipated areas of likely contact.

SECTION IV – CONDUCTING INTELLIGENCE OPERATIONS

6-31. Intelligence unit planning begins with receipt of mission, identifying information collection tasks in an order or plan. The unit then deliberately plans, prepares, and executes the mission in close coordination with the supported unit collection manager and other staff members to satisfy specific requirements. During the execution of intelligence operations, collection assets and supporting PED elements process, exploit, and disseminate intelligence reports and combat information. The staff continually assesses the effectiveness of the information collection plan to support the operations process. Combat information identified by the G-2/S-2 is immediately disseminated to the commander.

APPLYING THE OPERATIONS PROCESS IN INTELLIGENCE OPERATIONS

6-32. The operations process describes the sequence of activities performed by any military unit to accomplish a mission. (See ADP 5-0.) MI units conduct the same sequence of activities (plan, prepare, execute, and assess) to accomplish the tasks assigned to them. MI units follow the operations process to conduct intelligence operations the same way maneuver units do to conduct their operations. However, the conduct of intelligence operations requires collaboration and close coordination with the supported unit intelligence staff. (See figure 6-2.)

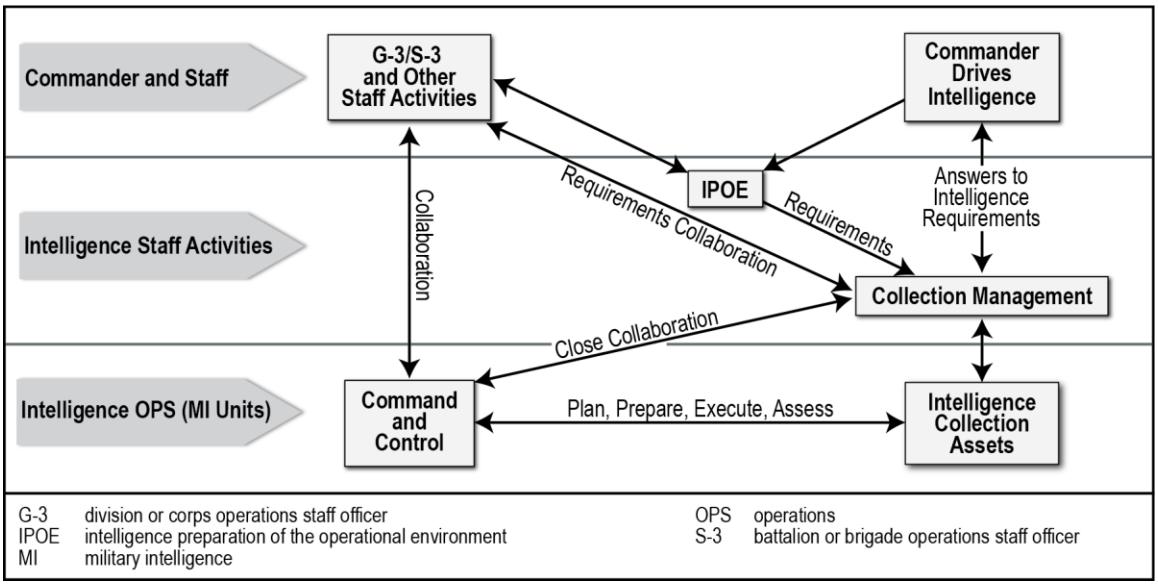


Figure 6-2. Intelligence support

PLAN

6-33. *Planning* is the art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about (ADP 5-0). It results in a plan or order that communicates the commander's intent, understanding, and visualization of the operation to subordinates, focusing on desired results.

Mission Planning

6-34. Mission planning begins when the MI unit receives or anticipates a new mission. This can come from an order issued by higher headquarters or derived from an ongoing operation. The MI unit relies on established SOPs to articulate individual and collective responsibilities during planning. The SOPs identify the participants, their responsibilities, and the tools or products required to produce intelligence.

6-35. Upon mission receipt, the supported unit's order and annexes must be examined to identify specified and implied tasks and constraints contained in the order's annexes. The MI unit commander and leaders should review Annex B (Intelligence), Annex D (Fires), Annex F (Sustainment), Annex H (Protection), Annex L (Information Collection), and Annex S (Special Technical Operations) to the base OPORD, as well as all supporting appendixes and tabs.

Military Intelligence Unit Commander

6-36. During planning, the MI unit commander uses specified and implied tasks, the supported unit's commander's guidance and staff assessments, and the information collection plan. This allows the MI unit commander to tailor planning considerations, which include but are not limited to—

- Determining the amount and type of equipment required and available for the mission.
- Determining and requesting the augmentation of personnel and equipment, including required PED support to conduct single-discipline and multidiscipline intelligence operations.
- Determining and requesting the augmentation of personnel for complementary capabilities.
- Determining the communications (network and voice) and connectivity architecture, requirements, and limitations to support the mission.
- Coordinating with other units to support the MI unit's mission, including but not limited to—
  - Medical personnel to establish casualty evacuation procedures.
  - The fire support officer to coordinate fire support.

  - The airspace coordinator if using airborne intelligence systems.
  - Supported units to ensure the required mission, communications, logistics, and life support are available for the MI element/personnel.
  - Maneuver units to coordinate terrain management where MI personnel are expected to operate.
  - Adjacent MI unit commanders to identify threat information and coordinate and deconflict operations.
- Observing subordinate execution of TLP by section, platoon, and company leaders.
- Identifying language requirements and requesting augmentation, as appropriate.
- Identifying intelligence contingency funds requirements. (See AR 381-141.)
- Identifying IEW maintenance support and procedures before deployment. During deployment, this requires continuous assessment, especially when there are few or no organic IEW technicians and facilities.

Troop Leading Procedures

6-37. During planning, MI unit leaders below the MI battalion level conduct TLP to prepare for intelligence operations. The *troop leading procedures* are a dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation (ADP 5-0). These procedures enable leaders to maximize available planning time while developing effective plans and preparing their units for an operation. TLP are also supported by risk management. It is important for MI unit leaders to collaborate with both their higher MI unit (when applicable) and the supported unit throughout the entire TLP process.

6-38. The TLP and the MDMP are similar but not identical. Commanders with a coordinating staff use the MDMP (see table 3-3 on page 3-12); company-level and smaller units use the TLP (see figure 6-3).

6-39. TLP consist of eight steps. The sequence of the TLP steps is not rigid. Leaders modify the sequence to meet the mission, situation, and available time. Some steps are performed concurrently while others may be performed continuously throughout the operation.

Step 1—Receive the Mission

6-40. MI leaders analyze mission objectives and current capabilities to accomplish the assigned mission, assess any possible issues (personnel, equipment, or maintenance) that could limit mission support, and raise any issues to the MI commander and supported that could hinder mission accomplishment unit.

Step 2—Issue a Warning Order

6-41. MI leaders of elements supporting a mission issue a WARNORD to participating elements and personnel as soon as possible (usually within an hour after receipt of mission). This ensures subordinate leaders have key information needed to maximize preparation time. The MI unit may have to issue multiple WARNORDs due to additional information or changes to the supported unit's WARNORD. The initial WARNORD should include a task organization (provides the detailed task organization for the mission: formation, personnel, and equipment) and timeline (provides a schedule of all preparatory tasks from receipt of mission to the start of collection).

Step 3—Make a Tentative Plan

6-42. MI leaders create a tentative plan based on the supported unit's WARNORD that attempts to meet mission requirements and remain within the framework of the commander's intent. MI leaders ensure—

- MI personnel and elements have all available information to complete the mission.
- Soldiers are prepared to execute any tasks assigned to them and their section/element.
- All equipment and vehicles are prepared for the mission, inventoried, and operational.

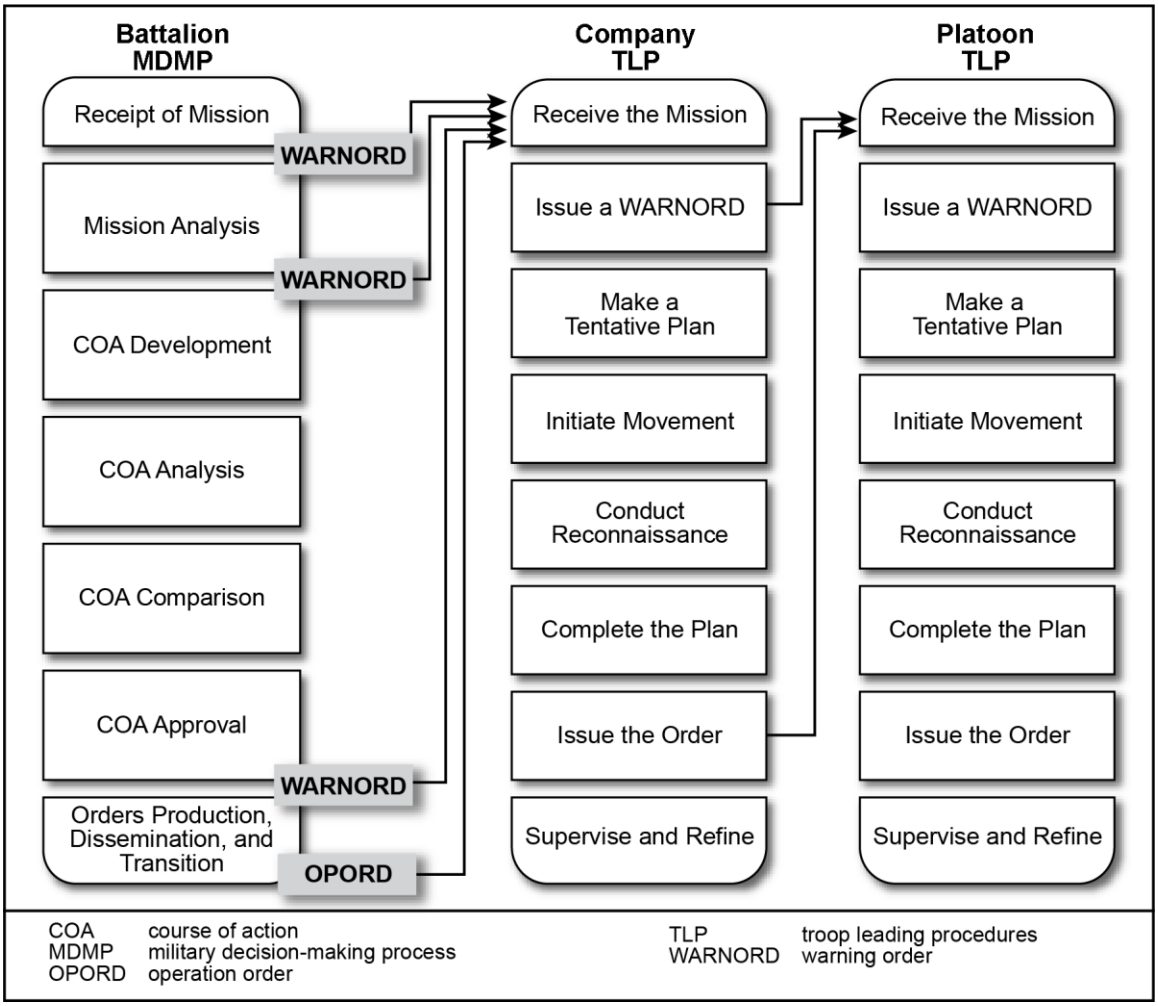


Figure 6-3. Troop leading procedures sequenced to the military decision-making process

Step 4—Initiate Movement

6-43. MI leaders may need to initiate movement while they are still planning or conducting reconnaissance. This step can occur at any time during the TLP.

Step 5—Conduct Reconnaissance

6-44. MI leaders, at a minimum, conduct a map reconnaissance and coordinate with the supported unit to review products (such as ground reconnaissance, geospatial information or imagery [including aerial photography], scout photographs, sketches) and to verify their terrain analysis, plan, and usability of routes. This step can occur any time during the TLP.

Step 6—Complete the Plan

6-45. MI leaders complete the plan based on reconnaissance and any changes in the situation and confirm the mission as received from the supported unit's WARNORD. This ensures the plan meets mission requirements and remains within the framework of the commander's intent.

Step 7—Issue the Order

6-46. MI leaders give final direction to their Soldiers and other personnel regarding the mission. Subordinate leaders should give a backbrief or confirmation brief to the responsible MI leader at the conclusion of the order to ensure specific tasks and purposes are understood. Designated personnel attend the mission brief, usually led by the maneuver element's mission leader.

Step 8—Supervise and Refine

6-47. All MI personnel/elements supporting the mission must attend all rehearsals, precombat checks, precombat inspections, and critical events conducted during planning. MI leaders ensure all supporting personnel adhere to the guidance, and all equipment, personnel, and vehicles are prepared for the mission.

PREPARE

6-48. *Preparation* is those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0). The prepare activity begins upon receipt of a plan or order, including a WARNORD. Intelligence operations begin once an order containing information collection tasks is received. For collection assets conducting intelligence operations, preparation activities include but are not limited to—

- Conducting the necessary coordination, as the situation requires, including logistics (by class of supply), maps, and medical evacuation procedures.
- Verifying fire support, casualty evacuation, fratricide avoidance, airspace coordination, spectrum management, and other coordination measures and procedures.
- Coordinating with the USAF SWO to determine weather effects on friendly and threat collection assets (platforms and sensors) and to determine time windows for optimal use based on their specific weather threshold sensitivities and current and predictive weather conditions in the OE.
- Refining plans, backbriefs, SOP reviews, and rehearsals, and coordinating products with various elements and organizations.

6-49. MI leaders should reconfirm and verify existing intelligence discipline reports for the target and share them with the supported commander. MI leaders should also review signal surveys, including the required technical data and the appropriate encryption, and inventory and test the signal equipment.

Perform Inspections

6-50. After acquiring all required equipment and support materials, MI leaders must conduct inspections to ensure unit personnel and sections are prepared to conduct their mission. Subordinate leaders conduct precombat checks of their personnel supporting the mission. Participating MI element leaders conduct precombat inspections before mission execution. It is crucial for MI leaders to verify that TTP, personnel, equipment, and services are in place and ready for mission execution.

Conduct Rehearsals

6-51. Rehearsals assist units in preparing for operations by either verifying that provisions and procedures are in place and functioning, or by identifying inadequacies that leaders and the staff must remedy. They allow operation participants to become familiar with and translate the plan into specific actions that orient them to their environment and other units when executing the mission. Rehearsals allow the MI element to integrate with and become familiar to the supported unit. It also allows the MI element to understand its role and scheme of maneuver within the larger mission objectives.

6-52. MI leaders conduct information collection rehearsals to ensure the correct information is collected, and Soldiers use the right techniques to support the mission. In a time-constrained environment, the information collection rehearsal may be combined with the combined-arms rehearsal or fires rehearsal.

EXECUTE

6-53. *Execution* is the act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0). MI leaders ensure their unit—

- Is properly staged with the supported unit and in the right order of movement.
- Monitors asset locations and supports and ensures force protection of these elements.
- Is on the right communications network and conducts communications checks.
- Reports technical, threat, and administrative information through the appropriate communications network (operations and intelligence) as specified in reporting guidelines established in Annex B (Intelligence) and unit SOPs.

ASSESS

6-54. *Assessment* is determination of the progress toward accomplishing a task, creating a condition, or achieving an objective (JP 3-0). Assessing allows the MI commander to determine the existence and significance of variances in the operation as envisioned in the initial plan. During execution, assessing an operation is an essential and continuous task. It is a deliberate comparison of previously templated outcomes to actual events, using the commander's criteria for success to judge operational success at any point during the operation. The MI unit commander assesses probable outcomes of the ongoing operation to—

- Determine whether changes are required to accomplish and complete the mission.
- React to threats.
- Take advantage of opportunities.

6-55. As the situation changes, MI leaders adjust the information collection plan to keep information collection tasks synchronized with the overall operation, optimize collection, and support future operational planning.

6-56. MI leaders assess intelligence operations by—

- Collaborating with collection managers to—
  - Identify if information requirements have been satisfied.
  - Evaluate the quality and accuracy of reported information.
  - Adjust the information collection plan based on the remaining information gaps.
- Requesting feedback from technical authorities (such as the G-2X) on the efficiency of information collection activities, and to identify the right collection activity to support the mission.
- Attending after action reviews with the supported commander and staff to assess how well the MI element integrated with and supported the unit during the mission. These after action reviews should include the—
  - Integration of the MI element into the larger mission plan.
  - Effectiveness of supporting the commander's information requirements.
  - Identification of equipment or personnel deficiencies.
  - Identification of lessons learned and emerging TTP that can better support the unit in the future.

TASK-ORGANIZING

6-57. The staff carefully considers the appropriate command or support relationship needed for each situation based on several factors, including proper intelligence authorities. The staff balances responsive support to the augmented unit with flexibility to distribute low-density, high-demand collection assets, as necessary, across the various echelons. The MI commander normally provides recommendations to the staff in matters of task-organizing collection assets and outlines the effects of the command and support relationships being considered. In coordination with supported units, the staff determines command and support relationships, as well as additional operational requirements (such as language support considerations [see appendix E]), along with the mission variables (METT-TC [I]) when developing plans and orders. The following discussion addresses factors to consider for intelligence operations. (See FM 5-0 for doctrine on task-organizing.)

Note. Understanding command and support relationships is important for the MI unit commander subordinating one unit to another, as appropriate.

COMMAND RELATIONSHIPS

6-58. Command relationships are used when the most responsive employment of augmenting MI units is required. Army command relationships are designated as either organic, assigned, attached, OPCON, or tactical control (TACON). Each relationship has inherent responsibilities associated with it. (See table 6-1.) All relationships, other than assigned, temporarily associate the augmenting MI unit with the gaining unit. Augmenting units return to their MI parent unit at the end of the operation, as specified in the plan or order directing the relationship, or when directed by a FRAGORD.

Table 6-1. Army command relationships

If the relationship is—	*Then the following are inherent responsibilities:*							
	Have command relationship with—	May be task-organized by—	Unless modified, ADCON responsibility goes through—	Are assigned position or AO by—	Provide liaison to—	Establish and maintain communications with—	Have priorities established by—	Authorities CDR can impose on gaining unit further command or support relationship of—
Organic	Organic HQ	Organic HQ	Organic HQ	Organic HQ	N/A	N/A	Organic HQ	Attached; OPCON; TACON; GS, GSR, R, DS
Assigned	Gaining HQ	Gaining HQ	Gaining HQ	Gaining HQ	N/A	N/A	Gaining HQ	Attached; OPCON; TACON; GS, GSR, R, DS
Attached	Gaining HQ	Gaining HQ	Gaining HQ	Gaining HQ	As required by gaining HQ	Unit to which attached	Gaining HQ	OPCON; TACON; GS; GSR; R; DS
OPCON	Gaining HQ	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ	Parent HQ	Gaining HQ	As required by gaining HQ	As required by gaining HQ and parent HQ	Gaining HQ	OPCON; TACON; GS; GSR; R; DS
TACON	Gaining HQ	Parent HQ	Parent HQ	Gaining HQ	As required by gaining HQ	As required by gaining unit and parent HQ	Gaining HQ	TACON; GS; GSR; R; DS

ADCON administrative control
AO area of operations
CDR commander
DS direct support
GS general support
GSR general support-reinforcing
HQ headquarters
N/A not applicable
OPCON operational control
R reinforcing
TACON tactical control

6-59. OPCON normally provides full authority to task-organize augmenting commands and forces and to employ those forces as the gaining commander considers necessary. It does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. A significant consideration in the OPCON relationship is that sustainment and other administrative control (ADCON) responsibilities remain with the parent MI unit unless the plan or order directing the relationship specifies otherwise. Normally, modifications to the inherent responsibilities are directed in the *Tasks to Subordinate Units* subparagraph of paragraph 3 (*Execution*) of the order.

6-60. TACON limits the gaining commander's authority to the detailed direction and control of maneuver/movement necessary to accomplish the missions or tasks assigned. TACON does not provide authority to change the organizational structure of the augmenting asset or direct administrative or logistics support.

SUPPORT RELATIONSHIPS

6-61. Commanders establish support relationships (table 6-2) when subordination of one unit to another is inappropriate, such as when limited MI collection capabilities must support multiple units. Support relationships provide the greatest flexibility to distribute collection assets across an AO. Support relationships are graduated from an exclusive supported and supporting relationship between two units—as in DS—to a broad level of support extended to all units under the control of the higher headquarters—as in general support (GS). Support relationships do not normally alter ADCON. Intelligence operations normally use two support relationships:

- *Direct support* is a support relationship requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance (FM 3-0).
- *General support* is support given to the supported force as a whole and not to any particular subdivision thereof (JP 3-09.3).

Table 6-2. Army support relationships

If the relationship is—	***Then the following are inherent responsibilities:***							
	Have command relationship with—	May be task-organized by—	Receive sustainment from—	Are assigned position or area of operations by—	Provide liaison to—	Establish and maintain communications with—	Have priorities established by—	Authorities CDR can impose on gaining unit further command or support relationship of
Direct support[1]	Parent HQ	Parent HQ	Parent HQ	Supported HQ	Supported HQ	Parent unit; supported HQ	Supported HQ	See note.
Reinforcing	Parent HQ	Parent HQ	Parent HQ	Reinforced HQ	Reinforced HQ	Parent HQ; reinforced HQ	Reinforced HQ; then parent HQ	N/A
General support-reinforcing	Parent HQ	Parent HQ	Parent HQ	Parent HQ	Reinforced HQ and as required by parent HQ	Reinforced HQ and as required by parent HQ	Parent HQ; then reinforced HQ	N/A
General support	Parent HQ	Parent HQ	Parent HQ	Parent HQ	As required by parent HQ	As required by parent HQ	Parent HQ	N/A

Note. Commanders of units in direct support may further assign support relationships between their subordinate units and elements of the supported unit after coordination with the supported commander.

CDR commander HQ headquarters N/A not applicable

6-62. In all support relationships, the parent unit is responsible for sustainment. Conditions may exist in which sustainment by the parent unit is not possible because of time, distance, or threats. In these cases, the plan or order directing the support relationship can direct the supported unit to provide sustainment for the supporting unit.

OTHER RELATIONSHIPS

6-63. Higher-echelon headquarters have established several other relationships with units that are not command or support relationships. These relationships are limited or specialized to a greater degree than command and support relationships, and they may be detailed in a command's implementing directives. Limited relationships are not used when tailoring or task-organizing Army forces. Using specialized relationships assists in clarifying certain aspects of OPCON or ADCON. Table 6-3 on page 6-16 lists other relationships.

Table 6-3. Other relationships

Relationship	*Operational use*	*Established by*	*Authorities and limitations*
TRO	The authority exercised by CCDRs over assigned RC forces when not on active duty. Through TRO, CCDRs shape RC training and readiness. Upon mobilization of RC forces, TRO is no longer applicable.	CCDRs identified in the Forces for Unified Commands memorandum ***Note.*** CCDRs normally delegates TRO to ASCCs.	TRO enables CCDRs to provide guidance on operational requirements and training priorities and review readiness reports and mobilization plans for RC forces. It is not a command relationship. ARNG forces remain under the C2 of their respective state AG until mobilized for federal service. USAR forces remain under the C2 of the CG, USARC, until mobilized.
TRA	The authority for a designated commander to give direction to an attached unit for leader development, individual and collective training, and unit readiness.	Higher commander	TRA includes responsibility for all facets of command that enable commanders to accomplish their mission. It does not include those installation command authorities vested in the Army senior commander.
DIRLAUTH	The authority to plan and direct collaboration between two units assigned to different commands, often based on anticipated tailoring and task organization changes.	The parent unit headquarters ***Note.*** This is a coordination relationship, not an authority through which command may be exercised.	DIRLAUTH is limited to planning and coordination between units.
Aligned	This is an Informal relationship to facilitate planning between a theater army and other Army units identified in operations and exercises in a specific combatant command.	Theater army and parent command	Normally establishes information channels for coordination between the gaining theater army and Army units that are likely to be committed to that area of responsibility.

AG	adjutant general	DIRLAUTH	direct liaison authorized
ASCC	Army Service component command	RC	Reserve Component
ARNG	Army National Guard	TRA	training and readiness authority
C2	command and control	TRO	training and readiness oversight
CCDR	combatant commander	USAR	United States Army Reserve
CG	commanding general	USARC	United States Army Reserve Command

TECHNICAL OVERSIGHT

6-64. 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 users. Commanders and staffs normally communicate through three channels: command, staff, and technical. (See ADP 6-0 and ATP 6-02.71.)

6-65. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess units' collection efforts. Technical channels involve translating information collection tasks into 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.
- Providing supporting technical data or databases.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized intelligence training.

6-66. Commanders and staffs ensure adherence to applicable laws, policies, and regulations, including but not limited to those listed in appendix D. They also ensure the proper use of doctrinal techniques and provide technical support and guidance. During intelligence operations, the intelligence staff ensures adherence to technical authorities through technical control.

6-67. *Technical authorities* are the applicable laws, policies, and regulations that guide and ensure the effective execution of the intelligence tasks, functions, and capabilities needed to meet the dynamic requirements of intelligence operations. Applicable laws and policies include all relevant U.S. laws, the law of war, international laws, ICDs, DOD directives, DOD instructions, and orders.

6-68. *Technical control*, in intelligence usage, refers to the application and oversight of the technical authorities that control the performance of intelligence functions and activities. While not a formal or support relationship, technical control is a critical function that ensures the collection asset has the required data and guidance to perform the mission.

6-69. Technical authority and technical control neither constitute nor bypass command authorities; rather, they serve as the mechanism for ensuring the effective execution of the intelligence tasks, functions, and capabilities needed to meet the dynamic requirements of operations. The commander and staff establish collection requirements for the asset, task the asset in accordance with the unit order or plan, and provide staff control of the asset during operations.

6-70. Technical authority and technical control are accomplished through intelligence technical channels. Establishing intelligence technical channels ensures oversight of and adherence to existing policies or regulations for information collection tasks within the information collection plan. In specific cases, regulatory authority is granted to national and DOD intelligence agencies for specific intelligence discipline collection and is passed through technical channels.

6-71. While intelligence technical channels are not part of command or support relationship channels, they are important to intelligence operations as they are the transmission paths between intelligence units (including sections) preforming a technical function that requires special expertise, oversight, or synchronization.

This page intentionally left blank.

PART THREE

Fighting for Intelligence

Fighting for intelligence requires leveraging national to tactical information collection, analytical capabilities, and PED capabilities to overcome challenges posed by threats within the OE. No one unit or echelon can collect all of the relevant information needed to identify and open windows of opportunity to continuously provide commanders and staffs situational understanding of the threat, especially during large-scale combat operations. Fighting for intelligence requires the G-2/S-2, in coordination with the G-3/S-3, other staff members, and the intelligence enterprise, to holistically portray the OE so friendly forces can gain and maintain situational understanding, present multiple dilemmas across domains, and deliver lethal capabilities.

Chapter 7

Intelligence at and Across Echelons

SECTION I – OVERVIEW

7-1. The Army portion of the intelligence enterprise, supported by an overarching Army intelligence architecture, facilitates intelligence support across echelons (for example, broadcast dissemination of higher-level collection) and at echelon as well as the synchronization of certain aspects of intelligence across echelons. However, to really understand Army intelligence support, intelligence professionals must understand intelligence support from national to battalion levels. Fundamentally, intelligence products, policy, and, in some situations, certain intelligence services flow down from the national level (along with partner nations) to joint headquarters and forces to theater army down (through the Army echelons) to the battalion level. This perspective provides a basic model. In some situations, intelligence also flows up from the tactical level to successive higher echelons—at times up to the national level—because of the unique access tactical-level intelligence can sometimes provide.

7-2. Figure 7-1 on page 7-2 provides a basic illustration of each echelon, including its intelligence staff and organic or supporting MI unit, to assist subsequent discussions of intelligence support at and across echelons.

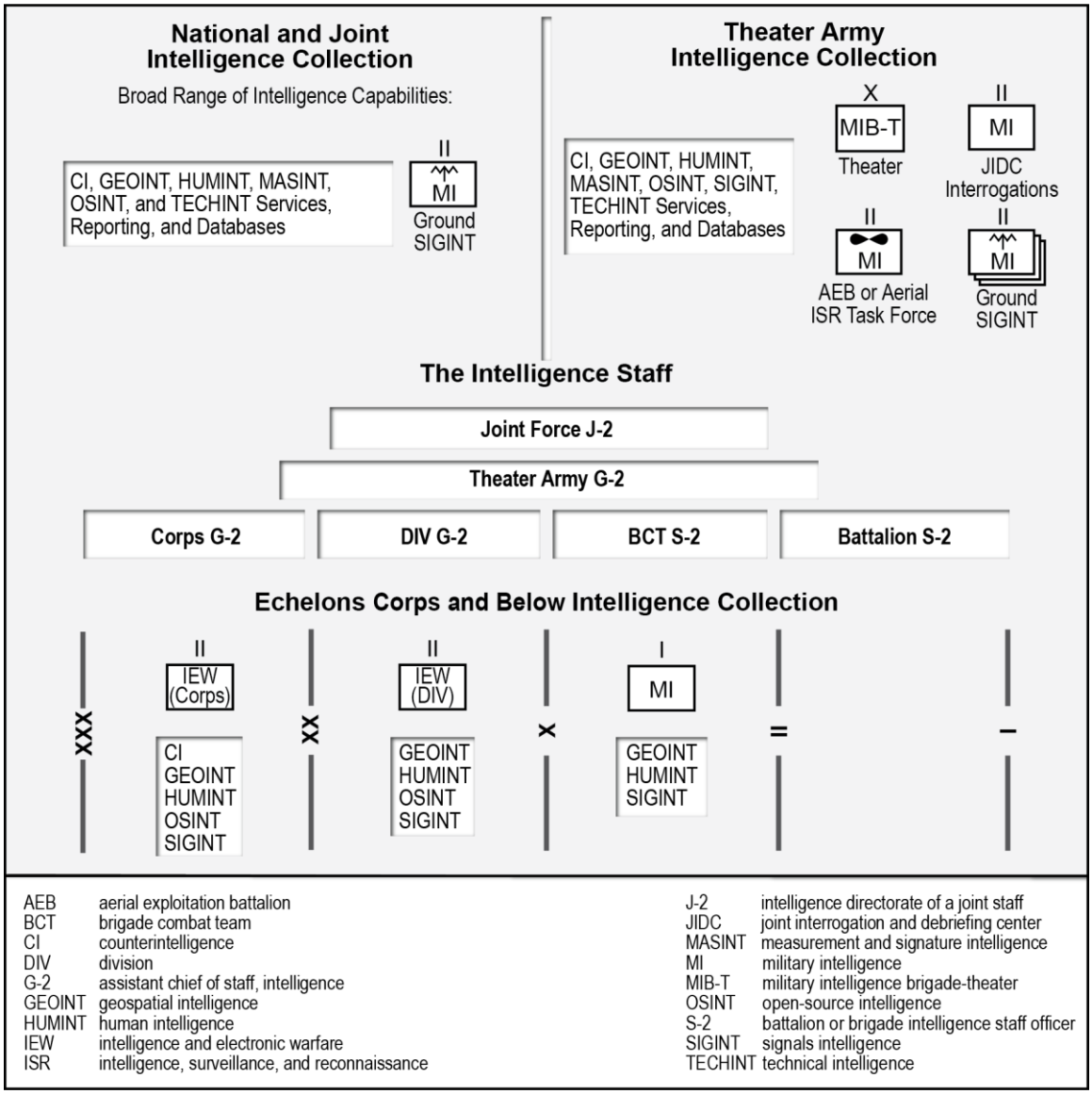


Figure 7-1. Intelligence across the echelons

THE INTELLIGENCE ENTERPRISE ACROSS ECHELONS

7-3. The scheme of intelligence assists in identifying how the intelligence warfighting function leverages capabilities across the intelligence enterprise to attain situational understanding of the OE. This is essential because each sensor, asset, unit, organization, agency, and allied partner within the intelligence enterprise assists in visualizing and understanding relevant characteristics of the OE that may impact operations. Information flow is not only downward to Army echelons but also from Army echelons to national organizations, agencies, and allied partners. This holistic approach of collaboration, integration and synchronization lessens the possibility of information gaps, information collection gaps, and the threat's ability to leverage a capability or adapt a COA not previously identified.

7-4. The value of the intelligence enterprise is the ability it provides to leverage information from all unified action partners (including access to national capabilities), nonintelligence information, larger volumes of information and intelligence, and specialized analysis. Collaboration is the central principle of conducting analysis. While there are many aspects to the intelligence enterprise, the most important element is the people that make it work. Army units provide accurate and detailed intelligence on the threats and relevant aspects

of the OE (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.

7-5. Collaboration, integration, and synchronization are central to the effectiveness of the national to tactical intelligence effort. When Army analysts collaborate with higher-level intelligence organizations, they create a more comprehensive and detailed assessment of the threat and OE (based on civil considerations and sociocultural factors across the domains and dimensions) to facilitate situational understanding.

INTEGRATED CAPABILITIES

7-6. To fully leverage intelligence enterprise capabilities, intelligence operations must integrate Service, special operations forces, theater, and national intelligence capabilities into a unified effort that surpasses any single organizational effort and provides the most accurate and timely information to commanders. Every intelligence organization provides pieces of information that support commanders' understanding, visualization, and decision making.

7-7. Intelligence integration occurs when intelligence sharing and collaboration occur at every level to develop an understanding of the threat's actions, activities, and anticipated steps. This facilitates the commander and staff's situational understanding and preparation for future operations. Information collection and intelligence activities must be coordinated vertically (for example, with higher/lower headquarters) and laterally (for example, with special operations forces, coalition, host-nation partner elements) and fully integrated into plans and operations. By using the appropriate procedures, foreign disclosure guidance, and established policy, intelligence leaders can provide information and intelligence support to multinational forces and vice versa. Having knowledge of and understanding the various echelons above corps and national intelligence organizations facilitate intelligence integration across every level.

SECTION II – NATIONAL, JOINT, AND U.S. ARMY INTELLIGENCE AND SECURITY COMMAND SUPPORT

7-8. Echelons above corps intelligence organizations encompass the national, joint, theater army, and field army (when established) portion of the intelligence enterprise. INSCOM is an example of an Army echelon above corps intelligence organization and key contributor to this effort. Echelons above corps intelligence organizations provide support at all levels of warfare. (See ADP 5-0.) They employ specialized and dedicated personnel and capabilities to collect information about threats, events, and national intelligence requirements. They leverage national and joint capabilities to allocate and prioritize collection assets to lower echelons operating at the tactical level. Therefore, Army commanders and staffs must understand the intelligence warfighting function across each echelon in addition to the intelligence capabilities of higher organizations.

7-9. An *Army Service component command* is command responsible for recommendations to the combatant commander on the allocation and employment of Army forces (JP 3-31). Army Service component commands (ASCCs) are the Army forces designated by the Secretary of the Army to support combatant commands. An ASCC has an intelligence staff that assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units. Some ASCCs receive support from several INSCOM units—ranging from directly aligned MIB-Ts to globally aligned functional intelligence brigades. INSCOM comprises 17 major subordinate commands categorized as—

- **MIB-Ts:** There are seven INSCOM MIB-Ts (six INSCOM MIB-Ts and one USAR [United States Army Military Intelligence Readiness Command (MIRC)] MIB-T), each tailored for the combatant command it supports. MIB-Ts provide collection, processing, analysis, and dissemination support to the ASCCs, CCDRs, and the U.S. IC.
- **Functional commands:** These functional commands, while not regionally aligned, work in coordination with INSCOM's MIB-Ts to create an integrated (national to tactical) intelligence architecture. INSCOM functional commands have missions and capabilities typically focused on a single intelligence discipline and operational function.

NATIONAL AND JOINT INTELLIGENCE SUPPORT

7-10. National intelligence organizations employ specialized resources and dedicated personnel to maintain situational understanding about potential adversaries, events, and other worldwide intelligence requirements across the competition continuum. National intelligence organizations routinely provide support to JFCs while continuing to support national decision makers. However, the focus of these national intelligence organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements. During large-scale combat operations against a peer threat, intense competition for intelligence resources at every level requires the efficient use and availability of Army information collection units and capabilities. (See ATP 2-19.1-1.)

7-11. The Army must posture itself as part of the joint force to effectively support and achieve national objectives. The intelligence warfighting function is the Army's contribution to national intelligence. As part of the joint intelligence effort, the Army's intelligence warfighting function must assist in achieving those objectives. INSCOM, as a direct reporting unit to the DA G-2, conducts and synchronizes worldwide intelligence collection across all disciplines and all-source analysis activities.

7-12. Table 7-1 lists and describes national and joint intelligence collection capabilities.

Table 7-1. National and joint intelligence collection capabilities

National and joint collection capabilities
• **CI:** Counterespionage investigations, CI collection, technical services and support, strategic CI operations, and CI analysis and production. **Disseminated/Broadcast to lower echelons:** Intelligence information reports and investigative reporting on shared databases. • **GEOINT:** National and commercial overhead collection and theater airborne collection. **Disseminated/Broadcast to lower echelons:** Operational intelligence ground station, TGS, Global Broadcast System, Integrated Broadcast Service, shared imagery library, reports, and shared databases. • **HUMINT:** Source operations (recruited, nonrecruited, debriefing), interrogations, collection support activities (HUMINT screening, liaison, HUMINT targeting, HUMINT support to DOMEX). **Disseminated/Broadcast to lower echelons:** Reports and shared databases. • **MASINT:** Overhead warning intelligence. **Disseminated/Broadcast to lower echelons:** Operational intelligence ground station, TGS, Global Broadcast System, and Integrated Broadcast Service, reports, and shared databases. • **OSINT:** Regional analytic products across many areas. **Disseminated/Broadcast to lower echelons:** OSINT reports, tactical OSINT reports, shared-product library. • **SIGINT:** National collection, theater airborne collection, and theater ground collection. **Disseminated/Broadcast to lower echelons:** Operational intelligence ground station, TGS, Global Broadcast System, reports, and shared databases. • **TECHINT:** Strategic support to the development community and detailed information and data on threat equipment and systems. **Disseminated/Broadcast to lower echelons:** Report and shared databases.

CI	counterintelligence	OSINT	open-source intelligence
DOMEX	document and media exploitation	SIGINT	signals intelligence
GEOINT	geospatial intelligence	TECHINT	technical intelligence
HUMINT	human intelligence	TGS	tactical intelligence ground station
MASINT	measurement and signature intelligence		

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

7-13. As the Army's operational intelligence force provider, INSCOM provides forces to ASCCs and the combat support agencies: National Security Agency, National Geospatial-Intelligence Agency, and DIA. INSCOM provides a ground intelligence production center to support the Army and the DIA federated production program and conducts TECHINT and forensics to support acquisition and operations. INSCOM's commander also provides Title 50, USC, National Intelligence Program support to the U.S. IC, combatant commands, and Army organizations.

7-14. The Army, in response to validated requirements, may direct INSCOM to provide many different types of capabilities to multiple echelons and joint forces with intelligence capabilities resident within INSCOM. INSCOM also delivers linguist support as well as intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, and unified action partner forces and the U.S. IC. INSCOM's MIB-Ts and functional commands may provide DS, GS, or GS-reinforcing to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force. (See ATP 2-19.1-2.)

7-15. INSCOM's functional commands and major subordinate commands include the following:

- The 116th MI Brigade (Aerial Exploitation) provides aerial intelligence collection platforms, associated PED, the Army Open-Source Center, and C2 at forward locations. The Army Open-Source Center is an OSINT organization that provides intelligence reach and supplementary support to Army major commands and units worldwide, coalition forces and JTFs, and other Services.
- The U.S. Army CI Command conducts the full range of CI functions (operations, investigations, collection, analysis and production, and technical services and support activities).
- The Army Operations Group conducts global, full range HUMINT operations.
- The National Ground Intelligence Center provides all-source intelligence and GEOINT on foreign ground forces, S&TI, general MI, and I2 on foreign ground forces. The Army GEOINT Battalion, as a National Ground Intelligence Center and INSCOM battalion, is the Army's lead force for GEOINT readiness and joint support to targeting. The Army GEOINT Battalion—
  - Conducts GEOINT to support worldwide military operations and national-level requirements.
  - Provides GEOINT support to joint targeting contingency planning and foundational MI.
  - Provides national-level representation for Army GEOINT collection.
  - Enables Army intelligence readiness through GEOINT Foundry mission and exercise support.
- The Cyber Military Intelligence Group, 780th MI Brigade, and other major subordinate commands (704th MI Brigade, 706th MI Group, the European Cryptologic Center, and the Expeditionary Operations Support Group) provide worldwide focus on threat analysis and emerging technologies (some in the cyberspace domain) with a goal of maintaining pace with ever-changing technologies and thereat advancements.

Army Intelligence and Security Enterprise

The AISE provides critical and unique assistance to the Army's national to tactical intelligence effort. The enterprise includes the following INSCOM offices, which assist in enabling Army cryptology, CI, GEOINT, HUMINT, and OSINT:

- Army Cryptologic Office (also known as ACO).
- Army GEOINT Office (also known as AGO).
- Army HUMINT Operations Center (also known as AHOC).
- Army OSINT Office (also known as AOO).
- Army Security Office (also known as ASO).
- Army Trojan Management Office (also known as ATMO).
- DA Intelligence Information Services (also known as DA IIS).

See ATP 2-19.1-2 for more information on the AISE offices.

SECTION III – FIGHTING FOR INTELLIGENCE ACROSS ECHELONS

7-16. Fighting for intelligence at echelon is difficult; fighting for intelligence across echelons is vastly complex. For national and joint levels, INSCOM, and at each Army echelon, there are so many varied capabilities performing many different roles across the intelligence enterprise. Different aspects of the intelligence enterprise include—

- Authorities, authorizations, and oversight.
- Different collection capabilities.
- All-source analytic centers, organizations, and units.
- Supporting enterprises across most of the intelligence disciplines.

7-17. Army capabilities at echelon perform different functions that vary with the type of unit, the organization of the theater or joint operations area, the nature of the conflict, and the number and types of friendly forces committed to the effort. At each echelon, a commander or leader task-organizes available capabilities to accomplish the mission. The use of capabilities is carefully planned, to include performing risk management. When fighting for intelligence at echelon during each strategic context, the G-2/S-2 considers several factors, including but not limited to—

- The commander's intent.
- The arrangement of friendly units and their capabilities across the OE.
- Synchronizing the intelligence effort across echelons to present multiple dilemmas to the threat across domains.
- Threat strengths, vulnerabilities, organizations, equipment, capabilities, intentions, and tactics.
- Considering threat capabilities residing in each domain and dimension.
- National, joint, and allied-partner capabilities available.
- Friendly capability vulnerabilities and limitations.
- Timely information is needed for decision making.

7-18. Army intelligence supports unified action at all echelons. Higher headquarters actively assist their subordinate formations in their fights, not simply attaching them to or assigning them with additional capabilities. Commanders and staffs actively avoid becoming so narrowly focused on their echelon's roles and responsibilities that they allow their subordinate formations to fail. Likewise, the G-2/S-2 must be able to visualize and synchronize intelligence operations across echelons during each strategic context to ensure optimal support across the entirety of the battlefield. MI unit structures and capabilities differ significantly across theaters and echelons. For example—

- Each theater army MIB-T has different capabilities and varying internal task organization.
- The corps expeditionary-military intelligence brigade (E-MIB) is the lowest level with organic HUMINT units that can support detainee facility interrogations and CI teams.
- Theater armies, corps, and BCTs have MI units—MIB-Ts, E-MIBs, and MI companies, respectively—but divisions and battalions do not have organic MI units.

Note. Combatant commands have OPCON of MIB-Ts and usually place them either under OPCON or TACON of the ASCC. Some corps E-MIBs can be task-organized to support divisions or even some BCTs.

7-19. 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; the number and complexity of the requirements; and the time available to answer those requirements. Generally, 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 must often depend on higher echelons 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. Figure 7-2 is a notional depiction of echelon roles and responsibilities in time, space, and purpose.

7-20. As a strategic context shifts from crisis to armed conflict, a good example of echelon interdependencies is setting and opening the theater and deploying intelligence staffs and MI units into the theater. Deployment comprises activities and processes required to prepare and move forces, supplies, and equipment to a theater. Planning for and executing the activities and processes necessary to deploy intelligence staffs and MI units occur from the theater army G-2 and intelligence staff level down to the MI unit platoon level. This also exemplifies the need for collaborative planning across echelons, as every echelon has a role in deployment. While the theater army G-2, intelligence staff, and MIB-T are responsible for setting the theater, once the E-MIB is set in theater, the theater army often tasks the E-MIB commander and staff to assist in setting the theater. The E-MIB is often tasked to support the deployment of subsequent MI units into the theater, especially in the reception, staging, onward movement, and integration (RSOI) of those units. (For more doctrine on Army deployments, see ATP 3-35.)

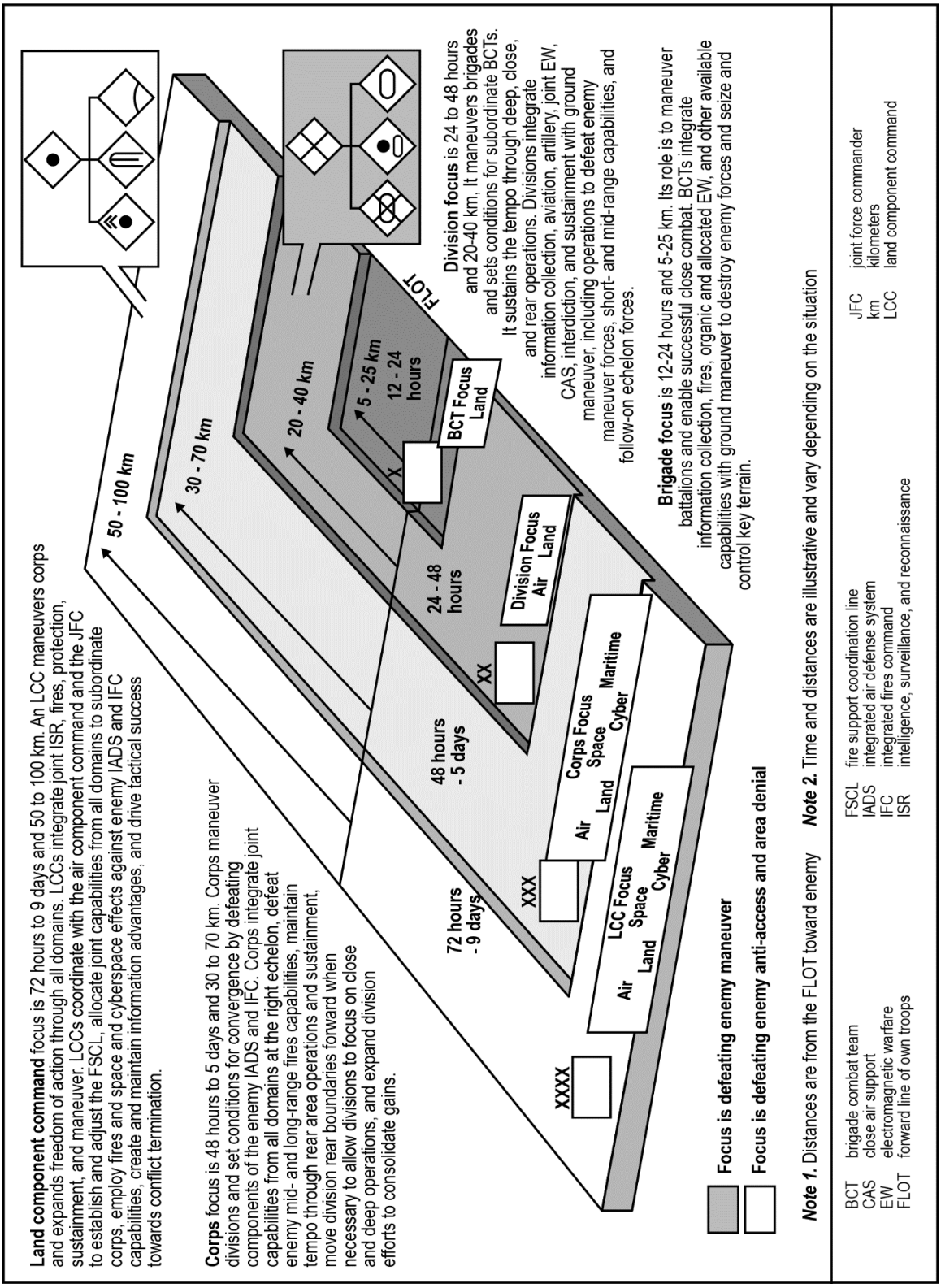


Figure 7-2. Notional roles/responsibilities in time, space, and purpose at different echelons

7-21. Another example of echelon interdependencies is intelligence support to targeting. Echelons above corps organizations are critical in building target folders during competition and then disseminating them to land force commanders. Currently, MIB-Ts and aerial exploitation battalions provide the Army's organic deep collection assets, which are essential to collecting information relevant to targeting. MIB-Ts have the data storage and data transport necessary to connect ground units at echelons corps and below to joint target folders and other theater-level targeting materials. As such, echelons above corps intelligence organizations support targeting from competition to armed conflict.

SECTION IV – THEATER ARMY

7-22. The ASCC of a combatant command can be a theater army. The Army contributes organizational elements and capabilities to JFCs to conduct unified action across the range of military operations. Theater army headquarters, operating from CPs with their associated theater-enabling commands and functional brigades, can control Army or joint forces for smaller-scale contingency operations. (See ATP 3-93.)

7-23. The theater army maintains an AOR-wide focus, providing support to Army and joint forces across the region, in accordance with the combatant command's priorities of support. Depending on the region and the combatant command's priorities, the relative emphasis that the theater army places on its operational and administrative responsibilities can vary greatly, to include—

- Shaping the AOR to improve positions of relative advantage held by U.S. forces and their allies.
- Protecting against threat actions outside of the operational area.
- Preventing the expansion of conflict unintended by friendly decision makers and senior commanders.
- Detecting and striking enemy capabilities that reside outside of a joint operations area.

7-24. The theater army enables the CCDR to employ landpower anywhere in the AOR across the range of military operations. It commands Army forces in the region until the CCDR attaches selected Army forces to a JFC. When that happens, the theater army divides its responsibility between the Army Component in the joint operations area and Army forces operating in other parts of the AOR. Each theater army synchronizes with unified action partners and employs the instruments of national power to fulfill policy aims within the assigned theater to support the national strategy. (See FM 3-0.)

7-25. Theater army intelligence operations are continually conducted to provide information and intelligence used to support land forces, including allied and partner-nation forces, in order to extend the capacity and capabilities of those forces and improve intelligence support to U.S. forces. Results from these operations provide guidance on plans and policies and strategic guidance. For the Army's corps, divisions, and BCTs, theater army intelligence operations provide information used in IPOE, support to targeting, support to information advantage activities, situation development, and protection; they also provide warning intelligence.

7-26. The theater army headquarters has a G-2 who assists the commander in processing, analyzing, and disseminating information and intelligence provided by higher, subordinate, and adjacent units. (See ATP 2-19.1-1.)

THEATER ARMY G-2

7-27. The theater army G-2 is the commander's principal assistant who advises, plans, and coordinates actions of the intelligence warfighting function. The theater army G-2 is the chief of the intelligence cell, theater army's senior intelligence officer, and principal intelligence advisor to the theater army commander.

7-28. The theater army G-2 is equipped with intelligence systems and processors that connect to all required networks. These systems are interoperable with the Army's C2 suite of systems and can share data with Army organizations at all echelons and organizations within the U.S. IC. Using these systems, the theater army G-2 provides the authoritative intelligence estimate of enemy units and intent through the shared CIP, providing the foundation for lower echelons.

7-29. The theater army G-2 and its supporting ACE provide regionally focused intelligence overwatch. Regionally aligned, assigned, and designated forces must thoroughly coordinate with the supporting MIB-T. This allows regional forces to access theater intelligence, infrastructure, and training opportunities, as well as leverage expertise resident in the theater. Organizations can also interact with INSCOM functional commands to focus organic intelligence capabilities and enhance situational awareness and mission readiness.

7-30. The theater G-2 coordinates with the USAF SWO to—

- Provide weather forecasts and effects on operations and capabilities (friendly and threat).
- Ensure the weather portion of the running estimate remains current.
- Ensure weather products are published according to the commander's stated requirements and the command's battle rhythm.
- Ensure weather products are tailored for the area and include specific weather forecasts for specific theater weather conditions.

THEATER ARMY INTELLIGENCE CELL

7-31. The theater army intelligence cell is responsible for integrating and synchronizing Army intelligence operations throughout the combatant command's AOR. The cell's staff elements either embed or coordinate with other CP cells to facilitate this synchronization. Specifically, the theater army intelligence cell performs the following tasks:

- Provides recommendations to the theater army commander regarding the theater intelligence collection posture and task organization.
- Plans, programs, manages, evaluates, oversees, and integrates all intelligence activities.
- Provides functional oversight of assigned or attached intelligence personnel and units.
- Establishes the theater intelligence architecture.
- Manages theater army intelligence collection, production, dissemination, disclosure, and CI requirements.
- Coordinates for national intelligence support and executes intelligence engagement and theater security cooperation, as required.
- Provides intelligence support to land-based air and missile defense.
- Distributes established transliteration guidance for intelligence and operational consistency.

Building a Collaborative Environment

The theater army G-2 and intelligence cell provide the guidance, resources, and access to the intelligence enterprise that, in turn, promotes a collaborative and flexible environment to ensure effective collection management and intelligence operations from theater army to battalion levels. A top-down collaborative approach assists each successive echelon in dealing with the dynamic challenges that the threat presents to friendly forces. This publication has previously emphasized the importance of close collaboration between echelons as well as between the G-3/S-3, G-2/S-2, collection manager, and MI unit commander. The theater army has an important role in promoting that collaboration.

7-32. The intelligence cell in the theater army CP provides regionally focused intelligence support to Army and joint forces operating in the combatant command's AOR. It is organized as a planning staff that assists the theater army commander in developing the plans required to support the combatant command's operations.

7-33. The theater army intelligence cell depends on the MIB-T for intelligence collection, single-source analysis, and all-source intelligence to meet the theater army's intelligence needs. Additionally, the theater army intelligence cell depends on the JFC information planning cell for analysis and intelligence about the cyberspace domain and information dimension. With augmentation, the intelligence cell can conduct operational intelligence collection and analysis to support theater army operations or operate in DS of a corps or other subordinate headquarters.

MILITARY INTELLIGENCE BRIGADE-THEATER

7-34. MIB-Ts are assigned to combatant commands and may be OPCON or TACON to the theater army by the CCDR. Both the MIB-T commander and the G-2 use a memorandum of understanding to identify OPCON, TACON, or ADCON responsibilities. As the theater army's permanently assigned ground intelligence organization, the MIB-T can deploy scalable and tailorable intelligence capabilities to meet combatant command, ASCC, and JTF intelligence requirements. However, it is likely that MIB-Ts will be OPCON to the theater army; therefore, this publication discusses MIB-Ts as OPCON to the theater army. (See ATP 2-19.1-2.)

7-35. MIB-Ts—

- Provide regionally focused collection and analysis to support theater army daily operation requirements and specific joint operations in the AOR.
- Provide the theater army with its foundational capabilities to set the theater for the intelligence warfighting function. As such, MIB-Ts serve as theater-level intelligence focal points through the theater army G-2 for deploying forces.
- As focal points, provide intelligence system and intelligence personnel support related to combatant command specific OEs.
- Provide expertise on joint ISR and Army information collection, intelligence resources, cultural knowledge of the theater, and the threat, as well as access to theater and national intelligence architectures and data that support intelligence operations.
- Perform important tasks to support the theater army G-2's effort in opening the theater.
- Assist the E-MIB with RSOI, when needed.
- Provide overarching planning for the RSOI of subsequent MI units.

SUPPORT AND ENABLING SERVICES

7-36. Deployed MIB-T forces leverage secure communications networks to access nondeployed MIB-T, higher-echelon Army, joint, and U.S. IC capabilities through intelligence reach. MIB-Ts can provide or coordinate the following support and enabling services to ground forces deploying to, operating in, or otherwise supporting the theater:

- **Intelligence:**
  - Intelligence assessments.
  - COPs, CIPs, and intelligence graphic products.
  - Persistent intelligence overwatch (for example cultural, language, area subject matter experts).
  - Federated intelligence production and coordination on behalf of the ASCC G-2.
- **Integration:**
  - Information technology integration.
  - Data services (COPs, CIPs, and intelligence pictures; theater geospatial database; data sharing; access to the combatant command's distributed integrated backbone [also called DIB]; knowledge management; and the USAF Weather Virtual Private Cloud).
  - Data ingest services (data push and pull, data formatting, and the intelligence analysis systems-to-C2 systems population).
  - Architecture management services (Secret, sensitive compartmented information, and multinational communications networks; regionally aligned forces intelligence analysis system connectivity; standard and shareable geospatial foundation, theater geospatial database, and geospatial data and information across all network classification domains; and data routing services provided or coordinated by Ground Intelligence Support Activity information technology operations).
- **Training:** Live environment training, mobile training teams, and subject matter expertise.

BASELINE DESIGN

7-37. The organization and capacity of each MIB-T differ in relation to enduring theater requirements and relative prioritization within the Defense Planning Guidance. Although tailored to the unique circumstances of the theater to which it is assigned, a MIB-T's standard baseline design is—

- A multicomponent brigade headquarters that includes Active Component, USAR, and aligned ARNG elements.
- An operations battalion that serves as the theater army G-2's ACE. This battalion may also be task-organized as a theater intelligence center. The battalion may also send a task-organized intelligence support element as part of the forward deployment of a theater army headquarters CP/element and/or other ground intelligence forces.
- A forward collection battalion that may possess CI, HUMINT, and SIGINT collection and analysis capabilities.
- A USAR MI battalion-theater support (known as a theater support battalion)—assigned to the MIRC but regionally aligned to the theater—that can mobilize to provide surge and an extension of intelligence capability and capacity to the MIB-T to support ground-force requirements in theater.
- An ARNG-aligned linguist battalion that provides CI, HUMINT, and SIGINT regionally aligned linguist Soldiers.

Note. The MIB-T, reinforced by INSCOM's functional commanders and major subordinate commands, provides support to regionally aligned force/global response force units at all levels to assist in integrating them into the theater enterprise before, during, and after deployment. Through MIB-T focal points and functional commands, INSCOM, along with the MIRC, brings intelligence capabilities to supported operational- and tactical-level commands to ensure they have the necessary intelligence to conduct expeditionary operations.

INTELLIGENCE COLLECTION CAPABILITIES

7-38. Table 7-2 lists and describes theater army-level intelligence capabilities, which are divided into organic and supporting collection capabilities. However, since every theater and specific operation are different, the theater army G-2 builds an intelligence architecture, receives augmentation and higher-level support, and task-organizes organic intelligence units based on the specific operation. The intelligence architecture reflects how many MI capabilities are employed forward as well as the capabilities provided through intelligence reach.

Note. Generally, at each echelon there are more requirements than intelligence analytical and collection capacity.

Table 7-2. Theater army organic and supporting intelligence collection capabilities

Theater army organic collection capabilities
MIB-T[1]: The MIB-T serves as the theater-level intelligence focal point through the theater army G-2, and as such for deploying, regionally aligned, and global response forces. It is the geographic combatant command's ground intelligence organization. Each MIB-T has the same organic baseline collection capabilities but with varying levels of capacity. USAR theater support battalions are regionally aligned and provide support in coordination with MIB-Ts. Each MIB-T is augmented with capabilities and capacity from the INSCOM during contingencies. MIB-T systems differ by theater. During competition and crisis, MIB-Ts are only sourced with their organic capabilities and capacity; during armed conflict, MIB-Ts draw additional support. MIB-T collection capabilities include any combination of— • **CI:** CI investigations, CI collection analysis, CI cyber, technical CI, polygraph support, CI operations, and technical services and support. • **GEOINT:** Leverages the following national and joint capabilities: collection of national imagery, full-motion video, and moving target indicator. • **HUMINT:** Source operations (recruited, nonrecruited, debriefing), interrogations, collection support activities (HUMINT screening, liaison, HUMINT targeting, HUMINT support to document and media exploitation). • **MASINT:** (No organic collection capability) Leverages national and joint capabilities to identify and characterize signatures. • **OSINT:** Publicly available information collection and population sentiment assessments.

Table 7-2. Theater army organic and supporting intelligence collection capabilities (*continued*)

Theater army organic collection capabilities (continued)
• **SIGINT:** (Mission- and theater-dependent capabilities) Leverages theater and national SIGINT collection as well as organic collection capabilities available in some MIB-Ts. • **TECHINT:** (No organic collection capability) Leverages from USAR. Limited foreign materiel exploitation, technical assessments, and threat capability/vulnerability identification.
Theater army supporting collection capabilities
• During large-scale combat operations, the aerial exploitation battalion or an aerial ISR task force (from the aerial intelligence brigade) will most likely support the theater army or corps echelon based on the mission variables. • Limited national, joint, and INSCOM units and organizations provide theater-specific and special intelligence capabilities, as required, during normal operations and can provide surge capabilities when required.
Notes. A theater army may receive intelligence and information from Army space control companies in the theater MDTF's multidomain effects battalion and from the 1st Space Brigade, including reconnaissance and the characterization of adversary space domain activities. Operational conditions may restrict the use of organic systems. The communications infrastructure, the threat, and the tempo may affect the ability to employ or emplace collectors and collection platforms. [1] In highly contested, lethal environments where enemies employ effective long-range fires and other capabilities, it is imperative to identify windows of opportunity to deploy national, joint, and theater collection capabilities.

CI	counterintelligence	MDTF	multidomain task force
G-2	assistant chief of staff, intelligence	MIB-T	military intelligence brigade-theater
GEOINT	geospatial intelligence	OSINT	open-source intelligence
HUMINT	human intelligence	SIGINT	signals intelligence
INSCOM	United States Army Intelligence and Security Command	TECHINT	technical intelligence
ISR	intelligence, surveillance, and reconnaissance	USAR	United States Army Reserve
MASINT	measurement and signature intelligence		

ALL-SOURCE INTELLIGENCE CAPABILITIES

7-39. All-source intelligence support at the theater army level consists of robust and sophisticated capabilities focused on analyzing a broad range of operational and mission variables across the domains and dimensions. The analytical focus is at the strategic and operational levels. This all-source support occurs across all theater army CPs and is a key component of the intelligence architecture. All-source intelligence support includes the various elements of the theater army intelligence cell, the MIB-T operations battalion, and the regionally aligned USAR theater support battalion.

7-40. The primary all-source analytical element supporting the theater army is the ACE. Most theater army ACEs do not deploy forward. However, tailored analytical elements deploy forward to support the theater army CP structure. Table 7-3 describes theater army-level all-source intelligence capabilities.

Table 7-3. Theater army-level all-source intelligence capabilities

Intelligence support to—	*Analytical focus: Theater army*	*Analytical window*
Current operations	• **Analytical tasks:** Provide warning intelligence, perform situation development, and conduct collection management. • Perform specified analytical tasks to support theater army operations as directed. • Further refine intelligence products provided from future operations.	Current to 72 hours
Future operations	• **Analytical tasks:** Conduct pre-mission analysis of the OE for all theater army forces, provide theater army database support, perform IPOE, perform situation development, and conduct collection management. • Provide analytical support and address multidomain operation considerations for lower echelons. • Provide analytical support to the joint task force or joint force land component commander as required. • Provide regional expertise of enemy ground combat forces. • Develop IPOE products and mission analysis for the next operation. • Support the integration of regionally aligned forces into the theater OE. • Perform specified analytical tasks to support the theater as directed by the theater commander.	72 hours to 9 days **Echelon focus:** • Theater to division maneuver units. • Groupings of long-range fires, artillery, and rockets. • All specialty and supporting ground forces.
Targeting (for lethal and nonlethal effects)	• **Analytical tasks:** Participate in IPOE and situation development and provide support to targeting. • Emphasize defining and assessing target nominations, target validations, and comprehensive battle damage assessments at strategic and operational levels.	72 hours to 9 days
Note. Time windows are examples; actual time windows depend on the situation. All analysis thoroughly accounts for civil considerations, terrain, and weather forecasts and effects on capabilities.		

IPOE	intelligence preparation of the operational environment	OE	operational environment

COMPETITION

7-41. The theater army is the primary Army organization that plans, prepares, and oversees the execution of activities conducted by Army forces during competition and assesses the results of those activities. All theater army intelligence efforts during competition are accomplished within a larger national, joint, and coalition context. The theater army intelligence effort during competition focuses on the following:

- Providing support to set and maintain the theater.
- Providing intelligence support to theater security cooperation.
- Supporting the execution of the CCDR's daily operational requirements.
- Supporting contingency planning for crisis and armed conflict.
- Identifying events that may lead to crisis and armed conflict.
- Providing leaders and decision makers with the information necessary for a clear understanding.
- Conducting all-source intelligence analysis to support the ASCC or CCDR PIR.
- Providing support to force tailoring.
- Maintaining situational awareness across the theater.
- Providing continual support to target development.
- Maintaining the intelligence portion of the COP.
- Participating in the joint collection management board, which enables the JFC's decision making on the apportionment and allocation of ISR assets and updating the information collection plan.
- Maintaining the CIP.
- Serving as the theater army ACE for single-source intelligence, all-source intelligence analysis products and databases, and intelligence collection management.
- Leveraging the U.S. IC and joint/allied intelligence enterprise and integrating regionally aligned forces and global response forces.
- Conducting continuous information collection activities and intelligence analysis to provide early and accurate warning intelligence.

7-42. Competition activities enable the joint force to gain positions of relative advantage before combat operations. Operations during competition are characterized by actions to protect friendly forces and indicate the intent to execute subsequent phases of a planned operation. For this reason, it is critical for the theater army G-2, the MIB-T, and other regionally aligned forces to develop intelligence databases (across the domains and dimensions) during competition activities.

7-43. Additionally, the theater army G-2—

- Prepares for theater openings, to include planning the RSOI of MI staffs and units on the time-phased force and deployment list (TPFDL) to the OPLAN. The theater army G-2 may task other staffs or MI units to support the RSOI of subsequent MI units due to the time-intensive and detailed nature of RSOI—especially the full integration of MI units into operations and the intelligence architecture.
- Maintains, updates, and shares all information, including the enemy electromagnetic order of battle overlay with deploying units to ensure a common and current understanding of the threat.

7-44. The theater army G-2 participates in operational planning processes to identify intelligence support requirements in order to support theater plans and determine gaps in information and knowledge. This drives the development of the information collection plan. The G-2 analyzes the collected data and uses it to refine IPOE products. Additionally, the G-2 proposes PIRs for commander approval and identifies HVTs and HPTs for G-3 approval. The theater army G-2 conducts collection management with national, joint, and coalition partners to ensure adequate coverage of collection assets to meet the theater's needs.

7-45. The theater army G-2 builds relationships with partner nations through exercises and exchanges. Exercises strengthen relationships with—

- The U.S. IC, including the J-2 and combat support agencies (particularly the DIA, National Geospatial-Intelligence Agency, and National Security Agency), regionally aligned units, and units apportioned against an OPLAN.

- The USAR, including the MIRC and the MIB-T's USAR theater support battalion.
- The ARNG's 300th MI Brigade (Linguist), which provides language and intelligence support to the Army by mobilizing and deploying elements from its battalions.
- INSCOM, to include reinforcing support beyond what the MIB-T provides (for example, intelligence discipline or all-source support from INSCOM's functional brigades and groups).

7-46. MIB-Ts conduct MI C2, single-source and all-source analysis, and intelligence collection, and they coordinate for reach PED as directed by the information collection plan. Additionally, MIB-Ts reach out to and coordinate with assigned units (theater-assigned, rotational, regionally aligned) and units apportioned against OPLANs (either temporarily or permanently) to their theaters' mission, and then MIB-Ts begin the process of integrating MI Soldiers and capabilities into theater operations before deployment. This is accomplished through a standing memorandum of understanding between INSCOM and assigned units rotationally aligned to the specific theater. MIB-Ts also emphasize support to force protection and based on indications of how the theater is reacting to U.S. objectives.

7-47. The MIB-T's role in receiving deploying units includes ensuring these units can operate on theater-specific networks, such as the Combined Enterprise Regional Information Exchange System (CENTRIXS) and the United States Battlefield Information Collection and Exploitation System (US BICES), both of which are part of the mission partner environment. Furthermore, Army SIGINT activities, either through MIB-T SIGINT elements or by reach from the Army Technical Control and Analysis Element and the Army Cryptologic Office, can assist tactical SIGINT/EW units in accessing theater-specific databases and entering theater-specific SIGINT networks. Similarly, the theater J-2X provides guidance on integrating deploying CI and HUMINT forces.

Note. US BICES is an intelligence system that is the U.S. gateway to the 28-member nation battlefield information collection and exploitation system (also called BICES).

7-48. The theater army G-2, through the MIB-T, fulfills an important role in theater through CI and HUMINT operations. CI capabilities are integral to force protection operations OCONUS. Army forces permanently stationed OCONUS, such as those in the Republic of Korea and Europe, face a high threat from foreign intelligence entities; CI forces mitigate this threat.

CRISIS

7-49. The theater army intelligence effort during crisis focuses on—

- Maintaining situational awareness across the theater.
- MI force tailoring.
- Monitoring events that may cause a noncombatant evacuation operation event.
- Developing or revising the intelligence architecture.
- Providing support to warning intelligence.
- Providing support to information advantage.
- Providing support to protection.
- Providing continual support to target development.
- Maintaining the intelligence portion of the COP.
- Building and maintaining the CIP.
- Participating in the joint collection management board (which enables the JFC's decision making on the apportionment and allocation of ISR assets) and updating the information collection plan.
- Updating the planning for theater openings, to include placing MI staffs and units on the TPFDL and planning the deployment of those MI units—especially the overarching planning for RSOI.
- Maintaining, updating, and sharing all information, to include the enemy electromagnetic order of battle overlay, with deploying units to ensure a common and current understanding of the threat.

7-50. The MIB-T continues to conduct MI C2, single-source and all-source analysis, and intelligence collection, as well as coordinate for reach PED as directed by the information collection plan. However, there is more emphasis on support to force protection and on indications of how the theater is reacting to crisis.

ARMED CONFLICT

7-51. The theater army may provide the core of a land component command or may have a subordinate field army. The MIB-T's operations battalion forms the theater army ACE. The joint force J-2 federates production requirements with the theater army ACE responsible for maintaining the enemy ground COP and the CIP, which are used in various forums to update the JFC. In a combined environment, the theater army ACE conducts the bulk of its operations in combined workspaces and on combined networks while maintaining some unique U.S. only facilities or capabilities.

7-52. The theater army ACE has an important role in assessing the effectiveness of friendly operations through combat assessment that enables the JFC's decision making at key points in the OPLAN (such as the transition to armed conflict). Additionally, the theater army ACE conducts target development for the land component to support both JFC and land component commander targeting priorities. The theater battlefield coordination detachment assists the G-3 and G-2 in coordinating input into the joint prioritized integrated target list.

7-53. As a component of the joint force, the theater army represents subordinate Army forces in joint boards and planning cells. The most important of these for the G-2 is the joint collection management board, which enables the JFC's decision making on the apportionment and allocation of ISR assets. In turn, the theater army may establish a process to further allocate ISR assets to either a field army or subordinate corps headquarters to support daily combat operations. The battlefield coordination detachment maintains close coordination with the combined air operations center's ISR directorate duty officer and can assist in deconflicting ISR coverage issues generated by maintenance, weather, or changes in priority.

7-54. A key aspect of apportionment and allocation of ISR assets is the allocation of Army intelligence forces and Army special operations forces within the time-phased force and deployment data (TPFDD). This includes USAR forces such as interrogation battalions that support a joint interrogation and debriefing center. Furthermore, the theater army, based on the theater army G-2's recommendation, incorporates additional nonstandard and quick reaction intelligence capabilities into the theater army G-2, the MIB-T, or other subordinate units.

7-55. The theater army G-2 organizes the effort to ensure there is sufficient PED of all assigned or allocated collection assets through a combination of organic forces and intelligence reach capabilities. The theater G-2 also supports campaign planning to address major changes to the situation such as the transition from large-scale combat operations to stability operations.

SECTION V – CORPS

7-56. The corps is the Army's most versatile formation that employs organic and assigned units for operations. A corps headquarters is organized, trained, and equipped to control the operations of two to five divisions. The corps conducts large-scale combat operations as part of a joint campaign, employing divisions as its base. Corps are central to the conduct of large-scale combat operations as they are organized, trained, and equipped for the deep, rear, and close operations that enable success during close combat. In addition to divisional units, the corps may command BCTs and several types of multifunctional and functional brigades.

7-57. The corps is best positioned and resourced to achieve convergence with Army and joint capabilities. Corps integrate joint capabilities at the right echelon, defeat enemy long- and mid-range fires capabilities, maintain tempo, allow divisions to focus on close and deep operations, and expand division efforts to consolidate gains. When operating independently during large-scale combat, the corps may serve as the *ARFOR*—the Army component and senior Army headquarters of all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command (FM 3-94)—or as the JFLCC, but significant augmentation from joint and multinational forces is required to perform this role successfully.

7-58. A corps usually receives reinforcing capabilities and units from theater army, joint, or multinational echelons to conduct operations. There is no standard configuration for a corps, but it generally requires a maneuver enhancement brigade, a combat aviation brigade, an expeditionary sustainment command, a field artillery brigade, and an E-MIB to conduct large-scale combat operations. Corps commanders rely on E-MIBs, resources from higher echelons, and (in some situations) elements from subordinate units to conduct intelligence operations. (See ATP 2-19.3.)

Note. A *field army* is an echelon of command that employs multiple corps, divisions, multi-functional brigades, and functional brigades to achieve objectives on land (ADP 3-90). When a field army is not present, a corps is the nexus between the operational and tactical levels of warfare. The field army, when established, is simply a headquarters. Although it employs subordinate units during operations, these units are provided by external Army, joint, and multinational sources based on the situation, the field army's role, and its mission.

CORPS G-2

7-59. The intelligence warfighting function supports operations by assisting the commander to understand how enemy forces and other threats, terrain, weather, and civil considerations can affect the mission of these commands. The corps G-2, supported by the intelligence cell, advises the commander on how to leverage the intelligence warfighting function to support operations.

7-60. The corps G-2 advises the commander on intelligence, assists the commander in synchronizing intelligence operations, and supervises the intelligence cell. The following include key responsibilities:

- Act as principal intelligence advisor to the corps commander.
- Ensure the intelligence running estimate and CIP remain current.
- Ensure intelligence products are published and intelligence cell support is completed according to the commander's stated requirements and the command's battle rhythm.
- Provide analysis to enable the commander and decision maker's situational understanding.
- Provide warning intelligence.
- Perform situation development.
- Provide unique intelligence support to other types of activities.
- Provide intelligence support to information advantage activities.
- Provide intelligence support to targeting for lethal and nonlethal effects.
- Provide staff supervision of the intelligence training program.
- Provide staff supervision of assigned command security programs.
- Assist the commander in evaluating physical security vulnerabilities.
- Assist the rest of the staff in developing assessment criteria.
- Identify linguist requirements pertaining to intelligence support. (See appendix E.)
- Coordinate with the USAF SWO to provide weather forecasts and effects on operations and capabilities (friendly and threat), ensure the weather portion of the running estimate remains current, ensure weather products are published according to the commander's stated requirements and the command's battle rhythm, and provide weather support to targeting and other activities.

CORPS INTELLIGENCE CELL

7-61. The corps intelligence cell facilitates understanding the OE. The corps intelligence cell consists of three principal sections: intelligence operations, G-2 ACE, and G-2X, along with a USAF-provided SWO or staff weather team. These sections deploy to support the corps main CP and forward tactical CPs. The corps intelligence cell—

- Requests, receives, processes, and analyzes information from all sources and disseminates intelligence to support current and future operations.

- Disseminates intelligence products to support corps operations and the commander's situational understanding.
- Participates in information collection planning.
- Manages all requirements for information collection and collection assets under corps control.
- Focuses collection resources to provide information the commander requires to make decisions.
- Interfaces with the movement and maneuver cell to integrate intelligence products and intelligence operations activities into current operations.
- Ensures weather products and weather effects information are integrated into current operations.
- Recommends tasks to the corps G-3 for resources under corps control.
- Participates in the targeting process.
- Provides foundational geospatial information and services to all headquarters C2 systems to support visualization through the geospatial engineer team resident in the GEOINT cell.
- Assists in coordinating intelligence support to the various CPs and subordinate units.
- Advises the commander and staff on the employment of CI and HUMINT collection assets and interfaces with external organizations to synchronize and deconflict CI and HUMINT taskings and missions.
- Provides representatives to the COIC.

7-62. Each corps intelligence cell provides policies and procedures for conducting intelligence operations to subordinate echelon intelligence cells. These policies and procedures allow lower echelon intelligence staffs the freedom to conduct intelligence staff activities and intelligence operations more efficiently, as routine tasks can be executed without obtaining approval from higher echelons.

EXPEDITIONARY-MILITARY INTELLIGENCE BRIGADE

7-63. An E-MIB is the primary collection asset assigned or attached to the corps. The Active Component has three E-MIBs, the ARNG has two E-MIBs, and the USAR has two MI brigades (GS) to enhance the intelligence capability. ARNG E-MIBs provide the same capabilities as the Active Component IEW battalions (division); USAR MI brigades (GS) provide GS-surge CI, HUMINT, analysis, and PED capacity to theater armies and corps or GS-reinforcing CI, HUMINT, analysis, and PED capacity to MIB-Ts and E-MIBs. (See ATP 2-19.3.)

7-64. E-MIB units are designed to conduct intelligence operations to enable field army/corps/combined JTF and division operations during large-scale combat operations. E-MIBs conduct intelligence operations across multiple domains and dimensions; develop unique intelligence problem sets such as the identification of peer threat integrated fires complex, A2 and AD capabilities; and detect, locate, identify, and track threat combat and enabling formations. E-MIBs provide—

- Intelligence architecture establishment and maintenance.
- ISR management.
- C2 of MI assets (organic, assigned, and attached).
- PED.
- All-source analysis, including target development and BDA.
- Intelligence operations:
  - CI collection, analysis, production, and activities.
  - OSINT collection, analysis, production, and activities.
  - HUMINT collection, analysis, and production.
  - GEOINT collection, analysis, and production.
  - SIGINT collection, analysis, and production.
- EW and limited cyberspace operations.

7-65. E-MIB commanders are responsible for the training, readiness, and certification of their subordinate battalions. Additionally, the theater army may task the E-MIB, once the E-MIB is set in theater, to assist in conducting RSOI as subsequent MI units deploy. IEW battalions are assigned to E-MIBs and task-organized to a corps and division with a command or support relationship, as determined by the corps commander. IEW battalions are collocated with their supported corps or division headquarters and develop a habitual relationship with their supported corps/division G-2, providing intelligence support in garrison, during exercises, and when operationally deployed.

INTELLIGENCE COLLECTION CAPABILITIES

7-66. Table 7-4 lists corps-level intelligence capabilities, which are divided into organic and supporting collection capabilities. However, since every corps and specific operation are different, the corps G-2 builds an intelligence architecture, receives augmentation and higher-level support, and task-organizes organic intelligence units based on the specific operation. The intelligence architecture reflects how many MI capabilities are employed forward as well as the capabilities provided through intelligence reach.

Table 7-4. Corps organic and supporting intelligence collection capabilities

Corps organic collection capabilities	
E-MIB: E-MIB capabilities are task-organized within the corps to augment existing intelligence collection capabilities or to cover gaps. E-MIBs support corps and division operational requirements.	
Active Component E-MIB comprises—	
• 1x IEW battalion (corps), which comprises the following: ▪ Headquarters and headquarters detachment. ▪ Analysis and PED detachment. ▪ Multidomain MI detachment. ▪ Electronic warfare company. ▪ CI and HUMINT company.	
• 2x or more IEW battalions (division), which comprise the following: ▪ Headquarters and headquarters detachment. ▪ Analysis and PED detachment. ▪ Multidomain MI detachment. ▪ Electronic warfare company.	
ARNG E-MIB comprises—	**USAR MI brigade (GS)** comprises—
• 4x IEW battalions (division), which comprise the following: ▪ Headquarters and headquarters detachment. ▪ Analysis and PED detachment. ▪ Multidomain MI detachment.	• 2x MI battalions (GS), which comprise the following: ▪ Headquarters and headquarters detachment. ▪ CI detachment. ▪ HUMINT company. ▪ All-source and PED company.
Corps supporting collection capabilities	
Corps may be augmented by national intelligence support teams, as required—for example, from NGA for GEOINT support.	
Note. Operational conditions may restrict the use of organic systems. The communications infrastructure, the threat, and the tempo may affect the ability to employ or emplace collectors and collection platforms.	
ARNG Army National Guard CI counterintelligence E-MIB expeditionary-military intelligence brigade GEOINT geospatial intelligence GS general support HUMINT human intelligence	IEW intelligence and electronic warfare MI military intelligence NGA National Geospatial-Intelligence Agency PED processing, exploitation, and dissemination USAR United States Army Reserve

ALL-SOURCE INTELLIGENCE CAPABILITIES

7-67. All-source intelligence support at the corps level consists of organic analytical capabilities focused on analyzing specific operational and mission variables across the domains and dimensions within an assigned theater. The analytical focus executes operational-level and tactical-level intelligence analysis and production of the enemy ground forces' intent and capability to conduct future military operations within an OE. This all-source support occurs at corps main CPs and tactical forward CPs and is a critical part of the intelligence architecture to higher, adjacent, and subordinate units.

7-68. The primary all-source analytic element supporting the corps is the ACE. The ACE supports situation development, the threat characteristics database, and targeting analysis. Generally, the corps ACE analytical capability deploys to support the corps main and forward tactical CPs. Table 7-5 describes corps-level all-source intelligence capabilities.

Table 7-5. Corps-level all-source intelligence capabilities

Intelligence support to—	*Analytical focus: Corps*	*Analytical window*
Current operations	• **Analytical tasks:** Provide warning intelligence and perform situation development. • Perform specified analytical tasks to support corps and below target execution and collection management. • Further refine products received from future operations.	Current to 48 hours
Future operations	• **Analytical tasks:** Conduct pre-mission analysis of the OE for all corps forces, provide integrated database support, perform IPOE, perform situation development, and conduct collection management. • Provide analytical reach support and address multidomain operation considerations for lower echelons. • Perform specified analytical tasks to support the corps as directed. • Provide intelligence products to plans.	48 hours to 5 days **Echelon focus:** • Corps to brigade maneuver units. • Groupings of long-range fires, artillery, and rockets. • All specialty and supporting ground forces.
Targeting (for lethal and nonlethal effects)	• **Analytical tasks:** Participate in IPOE and situation development and provide support to targeting. • Emphasize defining and assessing target nominations, target validations, and comprehensive battle damage assessments at the operational and tactical levels.	48 hours to 5 days
Note. Time windows are examples; actual time windows depend on the situation. All analysis thoroughly accounts for civil considerations, terrain, and weather forecasts and effects on capabilities.		
IPOE intelligence preparation of the operational environment OE operational environment		

COMPETITION

7-69. During competition, corps, division, and brigade intelligence staffs focus primarily on planning along with individual, collective, and unit training and readiness. Echelons corps and below units participate in their assigned commands' training events, including mission rehearsal exercises, mission readiness exercises, and combat training center rotations; they also participate in annual theater events when directed. Additionally, MI Soldiers within echelons corps and below units leverage the Army Foundry Intelligence Training Program as well as other training opportunities (for example, live environment training) to maintain perishable technical skills and enhance tactical and technical proficiency (see AR 350-32).

7-70. Based on the time available, units may conduct certain theater-specific intelligence readiness training before deployment. This training is generally tasked through Army Forces Command orders based on theater guidance. It is often driven by material fielding to support the deployment but can include subjects such as threat awareness and theater reporting procedures. Once in theater, units, under the direction of theater representatives, may conduct additional intelligence training as part of the RSOI process.

CRISIS

7-71. During crisis, the corps headquarters may deploy into an operational area as a tactical headquarters with subordinate divisions and brigades. (See FM 3-0.) The corps headquarters is responsible for—

- Understanding the threat.
- Integrating information collection and intelligence analysis into the next higher echelon's processes and systems.
- Establishing liaison with its higher headquarters and planning reconnaissance of its initial assembly areas, routes, and forward assembly areas.
- Assigning AOs to subordinate units.
- Identifying multiple routes from the points of debarkation through assembly to staging areas.
- Establishing an initial concept of operations.
- Planning to consolidate gains.
- Coordinating cyberspace attack mitigation, including distributed denial of service, malicious software, or system intrusion.
- Planning and preparing for communications denial and degradation.
- Planning for the dispersion of subordinate units along routes and within assembly areas.

7-72. Corps, divisions, and BCTs prepare for movement into theater and accomplishing RSOI. Corps and divisions integrate their ARNG and USAR main CP operational detachments and fully integrate their activities into the theater army G-2 and MIB-T battle rhythm to participate in analysis and battle update briefs. The main CP operational detachments establish reach operations to maintain continuity and provide intelligence updates while the corps, division, and BCT headquarters are in movement. Corps, divisions, and BCTs send advanced parties forward, including G-2/S-2 representatives. These advanced parties consider the following (not all-inclusive):

- Understanding the threat (collaborating with theater, partners, allies, and host-nation forces).
- MI force tailoring.
- Information collection and analysis integration.
- Processes and systems.
- SOP review and update.

ARMED CONFLICT

7-73. The corps G-2 and intelligence staff have important roles in the planning and execution of various operations and decisive tasks such as forcible entry operations, corps and/or subordinate division attacks, joint suppression of enemy air defense, deep operations, and corps-level gap crossings.

7-74. The corps staff, led by the corps intelligence cell, performs IPOE to support all operational planning. As a result of IPOE, the staff produces a range of intelligence products, including the enemy situation template and the event template and its associated event matrix. These products assist in accomplishing tasks, including but not limited to sharing information across the staff, driving certain aspects of the corps war game, and generating requirements to drive the information collection effort. The corps collection manager uses IPOE products to develop and then submit requirements to higher headquarters through joint systems for validation at the theater level. Additionally, the collection manager works in conjunction with the G-3 to generate taskings for assigned or attached collection assets, Army aviation, and maneuver formations responsible for reconnaissance and security operations.

7-75. The corps establishes procedures to suballocate theater information collection capabilities to the division level. Additionally, the corps task-organizes the E-MIB to support the corps and subordinate commanders. The corps also integrates nonstandard or quick reaction capabilities into intelligence units or staffs.

7-76. The corps can conduct expeditionary PED with assets from the E-MIB and the operational intelligence ground station within the corps G-2. In most situations, the corps requires intelligence reach support for PED, but the expeditionary capability ensures some level of support when there is no network connectivity in either an austere or degraded/denied environment.

7-77. Synchronizing the corps analytical effort with information collection and intelligence operations is critical in providing the corps commander with the timely and accurate intelligence required to make decisions regarding armed conflict. The sheer magnitude of large-scale combat operations necessitates precise timing. Triggers to initiate armed conflict require precise and detailed intelligence reporting and assessments.

7-78. Shaping OEs by the corps sets conditions for division operations. Shaping OEs through lethal and nonlethal effects requires a thorough understanding of threat systems and critical vulnerabilities. The corps G-2 and intelligence staff ensure the information collection effort—

- Generates targetable data on key enemy systems to support shaping OEs.
- Supports combat assessment that provides the commander with the necessary intelligence to decide if conditions have been met to initiate armed conflict.

7-79. An example of synchronization at the corps level is coordination for joint ISR capabilities (with associated PED) to detect a moving enemy force (via SIGINT or a moving target indicator) and support the analytic assessment that triggers a commander's decision point. In turn, the decision point is synchronized with operations and fires (for example, joint fires or Army aviation) linked to a TAI.

7-80. The corps intelligence staff also supports corps campaign planning and future operations. The intelligence staff identifies changes in the situation that allow the commander to take advantage of windows of opportunity by making adjustments to the plan beyond current operations.

SECTION VI – DIVISION

7-81. The division is a formation that employs organic and assigned units for operations. As the tactical unit of action for a corps, a division's primary role is as a tactical headquarters commanding multiple brigades. Divisions are the lowest tactical echelon that employ capabilities from multiple domains to achieve convergence during large-scale combat operations. Divisions are central to the conduct of large-scale combat operations as they are organized, trained, and equipped for the deep, rear, and support operations that enable success during close combat. A division combines offensive, defensive, and stability operations in an AO assigned by its higher headquarters, normally a corps. It task-organizes subordinate forces to accomplish the mission. During large-scale combat operations, a division operates not only as a headquarters but also as a centralized tactical force.

7-82. During operations of limited scope and duration, the division can fulfill the ARFOR role. Under such conditions, the division may also form the nucleus for a small-scale JTF or JFLCC, although joint force augmentation is required to fulfill either role successfully. During operations to consolidate gains, the division primarily serves as an intermediate tactical command. When the situation is consolidated such that a field army or corps is no longer required to C2 operations, a division can assume the ARFOR or JFLCC role; either role also requires joint force augmentation.

7-83. The division primarily focuses on operational responsibilities. Unless it serves as the ARFOR, a higher echelon normally retains ADCON for all but the division's organic, assigned, and attached units. However, when warranted, a higher-echelon commander serving as the ARFOR may designate a division commander as the deputy ARFOR with prescribed responsibilities.

7-84. A division may receive reinforcing capabilities and units from a corps, theater army, joint, or multinational echelon to conduct operations. In addition to BCTs, a division may directly control several types of multifunctional and functional brigades. The standard organization for a division formation includes a division artillery, a combat aviation brigade, a sustainment brigade, a maneuver enhancement brigade, and three to five BCTs.

IEW Battalions (Division)

In most instances, the corps allocates the IEW battalion (division) from the E MIB to a division. However, these are not enough IEW battalions for each division. IEW battalions (division) are assigned to E-MIBs and task-organized to priority divisions with command or support relationships as determined by corps commanders. IEW battalions (division) are collocated with their supported division headquarters and develop a habitual relationship with their supported division. The division commander may task-organize an IEW battalion (division), as necessary, for specific operations.

7-85. The size, composition, and capabilities of the forces task-organized under a division may vary between divisions involved in the same campaign, and they may change from one operational phase to another. Operations during large-scale combat require a different mix of forces and capabilities from those required for the conduct of stability operations.

7-86. Division and higher-level intelligence operations collect information to support current and future operations. Detailed intelligence analysis drives information collection for the division and its higher headquarters. To collect the information needed for planning and decision making, the division staff integrates all tools at its disposal into an integrated and synchronized echelon information collection plan. (See ATP 2-19.3.)

DIVISION G-2

7-87. The intelligence warfighting function supports operations by assisting the commander in understanding how enemy forces and other threats, terrain, weather, and civil considerations can affect the mission of these commands. The division G-2, supported by the intelligence cell, advises the commander on how to leverage the intelligence warfighting function to support operations.

7-88. The division G-2 advises the commander on intelligence, assists the commander in synchronizing intelligence operations, and supervises the intelligence cell. Key responsibilities include the following:

- Act as principal intelligence advisor to division commanders.
- Ensure the intelligence running estimate and CIP remain current.
- Ensure intelligence products are published and intelligence cell support is completed according to the commander's stated requirements and the command's battle rhythm.
- Provide warning intelligence.
- Perform situation development.
- Provide unique intelligence support to other types of activities.
- Provide intelligence support to targeting.
- Provide staff supervision of the intelligence training program.
- Provide staff supervision of assigned command security programs.
- Assist the commander in evaluating physical security vulnerabilities.
- Assist the rest of the staff in developing assessment criteria.
- Identify linguist requirements pertaining to intelligence support. (See appendix E.)
- Coordinate with the USAF SWO to ensure the weather portion of the running estimate remains current, provide weather forecasts and effects on operations and capabilities (friendly and threat), and provide weather support to targeting and other activities.

DIVISION INTELLIGENCE CELL

7-89. The division intelligence cell coordinates activities and systems that assist commanders in understanding the enemy and other threats, terrain and weather, and civil considerations. Similar to the corps intelligence cell, the division intelligence cell has three principal staff sections that deploy to support the corps main CP and forward tactical CPs: intelligence operations, G-2 ACE, and G-2X, along with a USAF-provided SWO or staff weather team. Each staff section has several elements. The division intelligence cell provides an intelligence staff element to the COIC.

7-90. To support operations, the division intelligence cell—

- Receives, processes, and analyzes information from all sources to produce and disseminate intelligence.
- Provides intelligence to support current and future operation activities.
- Develops information collection requirements and synchronizes intelligence operations.
- Participates in the targeting process.
- Through the G-3, supports, tasks, and directs intelligence operations (for example, fire support and survivability coordination).
- Assesses information collection, including intelligence operations, and resynchronizes the information collection plan throughout operations.
- Plans, monitors, and analyzes CI and HUMINT activities.
- In coordination with the USAF SWO, provides weather forecasts and effects to support current and future operation activities, information collection management, the targeting process, fire support, and medical evacuation.
- Coordinates intelligence support with multifunctional brigade intelligence sections (aviation, intelligence, maneuver, fires, and division artillery).
- Provides foundational geospatial information and services to all headquarters C2 systems to support visualization.

INTELLIGENCE COLLECTION CAPABILITIES

7-91. Table 7-6 lists division-level intelligence capabilities, which are divided into organic and supporting collection capabilities. The division has no organic intelligence collection capabilities; however, it has limited information collection and target acquisition assets in the combat aviation brigade Gray Eagle company that contribute to the intelligence effort. The division G-2 builds an intelligence architecture, receives augmentation and higher-level support, and task-organizes supporting intelligence units based on the specific operation. The intelligence architecture reflects how many MI capabilities are employed forward as well as the capabilities provided through intelligence reach.

Table 7-6. Division organic and supporting intelligence collection capabilities

Division organic collection capabilities
The CAB/ARB Gray Eagle company is equipped with 12 MQ-1C Gray Eagle unmanned aircraft systems.[1]
Division supporting collection capabilities
• Corps expeditionary-military intelligence brigades augment and provide capabilities to divisions through IEW battalions. • Active Component and Army National Guard IEW battalions (division) provide— ▪ Multidiscipline intelligence analysis and PED to support the division intelligence staff officer. ▪ Intelligence analysis and targeting support, PED, open-source intelligence, and signals intelligence collection to support division targeting. ▪ Limited interrogation capability to the division. ▪ Counterreconnaissance capabilities for sensing and attack to support division and brigade combat team commanders' scheme of maneuver.
Note. Operational conditions may restrict the use of organic systems. The communications infrastructure, the threat, and the tempo may affect the ability to employ or emplace collectors and collection platforms. [1] The CAB/ARB Gray Eagle company is not an intelligence unit, but it provides an information collection and target acquisition capability. The division operation order assigns the appropriate mission, which can include information collection, to the CAB/ARB Gray Eagle company.
ARB attack reconnaissance battalion — IEW intelligence and electronic warfare CAB combat aviation brigade — PED processing, exploitation, and dissemination

ALL-SOURCE INTELLIGENCE CAPABILITIES

7-92. All-source intelligence support at the division level consists of organic analytical capabilities focused on analyzing tactical enemy ground forces. The analytical focus is on enemy ground forces' intent and capability to conduct future military operations within a corps or division boundary. All-source support occurs at the division main CP and forward tactical CPs and is a critical part of the intelligence architecture to subordinate commands.

7-93. The primary all-source analytical element supporting the division is the ACE, which supports situation development, the threat characteristics database, and targeting analysis. Generally, the division analytical capability within the ACE deploys to support the division main and forward tactical CPs. Table 7-7 describes division-level all-source intelligence capabilities.

Table 7-7. Division-level all-source intelligence capabilities

Intelligence support to—	***Analytical focus: Division***	***Analytical window***
Current operations	**Analytical tasks:** Provide warning intelligence, perform situation development, conduct collection management, and further refine intelligence products received from future operations.	Current to 24 hours
Future operations	• **Analytical tasks:** Conduct pre-mission analysis of the OE for all division forces, provide database support, perform IPOE, perform situation development, and conduct collection management. • Provide IPOE products and mission analysis for the next mission. • Provide basic analytical support based on higher-level analysis of multidomain operation considerations. • Perform specified analytical tasks to support the division as directed. • Provide intelligence products to plans.	24 to 48 hours **Echelon focus:** • Division to battalion maneuver units. • Grouping of artillery and rockets. • Division specialty and supporting ground forces.
Targeting (for lethal and nonlethal effects)	• **Analytical tasks:** Participate in IPOE and situation development and provide support to targeting. • Emphasize defining and assessing target nominations, target validations, and comprehensive battle damage assessments at the operational and tactical levels.	24 to 48 hours
Note. Time windows are examples; actual time windows depend on the situation. All analysis thoroughly accounts for civil considerations, terrain, and weather forecasts and effects on capabilities.		
IPOE intelligence preparation of the operational environment — OE operational environment		

COMPETITION

7-94. Corps, divisions, and BCTs plan and prepare for movement into theater and accomplishing the RSOI. Corps and divisions integrate their ARNG and USAR main CP operational detachments and fully integrate their activities into the theater army G-2 and MIB-T battle rhythm to participate in analysis and battle update briefs. The main CP operational detachments establish reach operations to maintain continuity and provide intelligence updates while the corps, division, and BCT headquarters are in movement. Corps, divisions, and BCTs send advanced parties forward, including G-2/S-2 representatives.

7-95. Once identified as part of the rotational force, echelons corps and below units coordinate with the designated MIB-T to begin their integration into theater intelligence operations. This includes predeployment leader, staff, and analyst coordination as well as theater-specific qualifications and certifications. Some of these qualifications and certifications can be accomplished through Foundry training while others may include live environment training opportunities. Echelons corps and below units may establish intelligence reach operations to reduce their forward or deployed Soldier presence and maximize nondeployed MI capabilities or expertise (for example, linguists, federated PED, and contract or civilian analysts).

CRISIS

7-96. Based on the time available, units may conduct certain theater-specific intelligence readiness training before deployment. This training is generally tasked through Army Forces Command orders based on theater guidance; it is often driven by material fielding to support the deployment but can include subjects such as threat awareness and theater reporting procedures. Once in theater, units (under the direction of theater representatives) may conduct additional intelligence training as part of the RSOI process.

7-97. The primary role of a division during crisis is demonstrating credible coercive force as a combined arms formation. (See FM 3-0.) During crisis, the division headquarters performs many of the same activities as the corps headquarters. The division headquarters fulfills its primary role as a tactical headquarters staffed, trained, and equipped to command two to five BCTs and other subordinate brigades and battalions. Corps and division intelligence leaders collaborate closely with INSCOM and the national agencies to tailor capabilities to the specific OE and integrate new or additional capabilities. During crisis, divisions should expect to conduct short-notice training exercises with multinational partners and perform other activities that demonstrate capabilities as part of a crisis response. (ATP 3-91 provides more information on division operations.)

ARMED CONFLICT

7-98. The division G-2 and intelligence staff have important roles in planning and executing offensive, defensive, and/or stability operations. The division employs organic and supporting collection assets to gain and maintain enemy contact, develop the situation, generate targeting data, and assess the effectiveness of division operations.

7-99. The corps task-organizes a portion of or a complete E-MIB's IEW battalion to support division operations and enable subordinate commanders. Further, the division supports subordinate operations by further allocating or task-organizing information collection capabilities in DS of a subordinate unit; information collection support is not limited to BCTs. Adequately resourcing division artillery and combat aviation brigade operations is very important. Further, information collection support is required in consolidating gains to identify enemy observers, bypassed enemy units, and unconventional forces.

7-100. The division intelligence staff must coordinate PED to support these efforts. The division has one tactical intelligence ground station at the division and BCT levels. When task-organized, the supporting E-MIB provides PED capabilities, including a tactical intelligence ground station-PED section that enables sensor data receipt and PED tools when network connectivity is limited or negated.

7-101. The division collection manager orchestrates the information collection effort. The collection manager generates the requirements necessary to support division operations. The division uses joint systems, also used by the corps, to request theater or national ISR support. Those requests are validated at higher echelons. The collection manager, working in conjunction with the G-3, generates taskings for organic and allocated information collection systems and those units assigned a reconnaissance or security mission.

7-102. The division intelligence staff supports targeting and combat assessment to identify and exploit enemy vulnerabilities. This enables commander's decision making to support additional shaping activities, initiating armed conflict, or shifting the main effort.

7-103. The division G-2 and intelligence staff synchronize information advantage activities, information collection, and combat assessment in a fluid and complex environment characterized by multiple BCT attacks, supporting combat aviation brigade operations, joint fires, and operations in deep, close, and rear areas. This synchronization allows the staff to identify windows of opportunities. Synchronization across the staff ties information collection to commander decision points with Army aviation and joint fires linked to the TAI.

7-104. Fleeting windows of opportunity are addressed by current operations within division CPs. Intelligence also supports future operations by identifying changes in the situation beyond the current operations that necessitate changes to the plan.

SECTION VII – BRIGADE COMBAT TEAM

7-105. A BCT is the Army's primary combined arms, close-combat force. BCTs maneuver against, close with, and destroy the enemy; conduct offensive, defensive, and stability operations; and are the principal ground maneuver units of a division. All BCTs include the following capabilities:

- Maneuver.
- Fires.
- Reconnaissance.
- Sustainment.
- Intelligence.
- Medical.
- Signal.
- Engineer.

7-106. The organizational flexibility inherent within the BCT allows it to function across the range of military operations; armored BCTs have combined arms battalions, and infantry and Stryker BCTs have infantry battalions.

7-107. Intelligence operations are normally weighted to support the main effort. The BCT intelligence structure has the flexibility to tailor its capabilities to meet the requirements of various types of operations and adapt to changing operational needs during execution. For each operation, the commander and staff create and refine requirements and develop a scheme of information collection that positions MI and maneuver collection assets where they can best satisfy those requirements. (See ATP 2-19.4.)

7-108. BCT intelligence assets from the MI company are employed to support C2 by meeting the BCT commander's information collection tasks. The BCT staff develops a scheme of information collection that employs maneuver and MI units based on the BCT's mission, PIRs, concept of operations, and the commander's intent. This scheme integrates intelligence operations with the BCT's overall operation. The MI company positions collection assets to—

- Satisfy SIRs.
- Expose threat vulnerabilities.
- Monitor key locations.
- Detect targets.
- Collect information for the assessment of lethal and nonlethal effects.
- Identify opportunities as they arise.

BRIGADE COMBAT TEAM S-2

7-109. The BCT S-2 is the principal intelligence advisor to the BCT commander. Additionally, the BCT S-2 supports security programs and oversees the BCT intelligence cell. Specific BCT S-2 responsibilities include but are not limited to—

- Situation development, target development, and support to lethal and nonlethal targeting, warning intelligence, assessment, and protection.
- Providing the commander and staff with assessments of enemy capabilities, intentions, and COAs as they relate to the mission.
- Identifying intelligence gaps and developing collection strategies.
- Disseminating intelligence products throughout the unit and to higher and subordinate headquarters.
- Answering RFIs from subordinate commanders, staffs, and higher and adjacent units.
- Coordinating the unit's information and intelligence requirements with supporting higher, lateral, and subordinate echelons.
- Overseeing BCT intelligence cell contributions to collection management.
- Supporting the S-3 during the MDMP.
- Leading the staff in performing IPOE.
- Coordinating with the USAF SWO to provide weather forecasts and effects on operations and capabilities (friendly and threat) and for weather information to support targeting.

BRIGADE COMBAT TEAM INTELLIGENCE CELL

7-110. The BCT intelligence cell is the intelligence organization in the CP that answers directly to the BCT S-2. Most intelligence staff Soldiers reside in the BCT intelligence cell in the main CP. Higher headquarters may augment this cell with additional capabilities to meet mission requirements. (See FM 6-0 for doctrine on CP organizations.)

7-111. The BCT intelligence cell performs several different functions, including but not limited to—

- Analyzing information from all intelligence disciplines and organizations to produce and disseminate intelligence products.
- Supporting current operations and planning.
- Supporting collection management.
- Providing technical control of intelligence discipline activities.
- Providing IEW systems integration and maintenance throughout the BCT.
- Augmenting intelligence analysis across the BCT by distributing intelligence support teams to subordinate units as a part of the overall task organization.

MILITARY INTELLIGENCE COMPANY

7-112. Most intelligence personnel within the BCT are assigned to the MI company. The BCT MI company provides intelligence and synchronized information collection support to the BCT commander, BCT staff, and subordinate units during the planning, preparation, and execution of operations. Based on operational requirements, the division commander may attach the BCT MI company to another division unit to provide an additional intelligence capability.

7-113. The BCT MI company provides a clear intelligence picture to assist maneuver commanders in making educated, tactical decisions on the battlefield. The BCT MI company integrates collection assets with maneuver units and the G-2/S-2 and supports the targeting effort. It deploys and provides single-source collection, tactical UAS capabilities, and collected intelligence processing capabilities. The BCT MI company is organized to accomplish specific intelligence activities to support BCT operational requirements.

7-114. When appropriate, the intelligence structure includes SIGINT and HUMINT augmentation to battalions or companies and analytical augmentation to battalion intelligence cells, creating an MI company (minus). The MI company (minus) represents those Soldiers remaining in the MI company after the task organization of the BISE, the USAF SWO element, and the intelligence collection platoon elements. Additionally, the tactical UAS platoon may be under the combat aviation brigade's ADCON, at home station, for aviation safety, standardization, and sustainment reasons while still providing GS as part of the MI company (minus).

BRIGADE INTELLIGENCE SUPPORT ELEMENT

7-115. There are several ways to task-organize the BISE, which provides BCT commanders the flexibility to tailor the force based on mission requirements. The BISE provides the BCT S-2 with some PED, all-source analysis and production, intelligence reach, and dissemination capabilities. The BISE—

- Receives collected enemy and civil considerations information.
- Tracks enemy movement.
- Assesses enemy capabilities and some other significant aspects of the OE.
- Creates graphic and textual products that depict intelligence analysis results.

7-116. The BISE collaborates and disseminates its information, intelligence products, and analytical conclusions with the rest of the BCT intelligence cell elements, the subordinate battalion intelligence cells, and higher- and lateral-echelon intelligence organizations.

INTELLIGENCE COLLECTION CAPABILITIES

7-117. Table 7-8 lists BCT-level intelligence capabilities, which are divided into organic and supporting collection capabilities. The organic intelligence collection capability is the MI company. MI company assets may provide downward reinforcement to maneuver battalions or maneuver companies. Since every BCT and specific operation are different, the BCT S-2 builds an intelligence architecture, receives augmentation and higher-level support, and task-organizes organic intelligence units based on the specific operation. The intelligence architecture reflects how many MI capabilities are employed forward as well as the capabilities provided through intelligence reach.

Table 7-8. Brigade combat team organic and supporting intelligence collection capabilities

BCT organic collection capabilities
• **MI company:** MI company capabilities generally support the BCT, but they may be task-organized to other units across the BCT to cover gaps. MI companies contain the following collection capabilities: ▪ 1x tactical UAS platoon contains UAS operators and repairers (4x tactical UASs). ▪ 1x intelligence collection platoon contains 3x SCTs and 3x HCTs. • **Cavalry squadron.**
BCT supporting collection capabilities
May be augmented by the E-MIB depending on the commander's requirements and priorities. Possible augmentation includes— • 2x CI teams. • 1x SCT. • 1x HCT. • Upon request, MQ-1C Gray Eagle UASs from the CAB/ARB Gray Eagle company.
Note. Operational conditions may restrict the use of organic systems. The communications infrastructure, the threat, and the tempo may affect the ability to employ or emplace collectors and collection platforms. While not an intelligence collection capability, the cavalry squadron conducts reconnaissance and security operations as part of the BCT information collection effort.

ARB	attack reconnaissance battalion	HCT	human intelligence collection team
BCT	brigade combat team	MI	military intelligence
CAB	combat aviation brigade	SCT	signals intelligence collection team
CI	counterintelligence	UAS	unmanned aircraft system
E-MIB	expeditionary-military intelligence brigade		

ALL-SOURCE INTELLIGENCE CAPABILITIES

7-118. All-source intelligence support at the BCT level is very basic and focuses on ground operations. The other domains are only addressed based on how they affect BCT operations. All-source support is organized to meet BCT requirements across main and tactical forward CPs. Table 7-9 describes BCT-level all-source intelligence capabilities.

Table 7-9. Brigade combat team-level all-source intelligence capabilities

Intelligence support to—	*Analytical focus: BCT*	*Analytical window*
Current operations	**Analytical tasks:** • Provide warning intelligence. • Perform situation development of enemy tactical ground element forces. • Conduct collection management. • Further refine intelligence products received from future operations.	Current to 12 hours
Plans	• **Analytical tasks:** Conduct pre-mission analysis of the OE for BCT and adjacent forces, provide tactical inputs to intelligence database support to higher and lower echelons, perform tactical IPOE, perform situation development, and conduct collection management. • Provide IPOE products and mission analysis for the next mission. • Provide analytical support to the BCT commander's MDMP requirements. • Provide intelligence products to current operations.	12 to 24 hours **Echelon focus**: • Division to battalion maneuver units. • Groupings of artillery and rockets. • Follow-on ground units.
Note. Time windows are examples; actual time windows depend on the situation. All analysis thoroughly accounts for civil considerations, terrain, and weather forecasts and effects on capabilities.		
BCT brigade combat team IPOE intelligence preparation of the operational environment		MDMP military decision-making process OE operational environment

COMPETITION

7-119. BCTs focus on perfecting tactical tasks to execute OPLANs for large-scale combat operations. Forward deployed BCTs assess and improve protection measures against adversary capabilities and promote interoperability with host-nation tactical units. For BCTs that are not forward deployed, BCT S-2s and MI company leaders plan and prepare for movement into the theater and accomplishing RSOI. While most of the rotational brigade's training occurs in CONUS and does not involve partner-nation forces, brigades anticipate and plan how to integrate with host-nation forces. (See FM 3-0 and FM 3-16.)

7-120. The BCT S-2 and MI company collaborate to train intelligence teams across the BCT. Specifically, BCT and MI company leaders collaborate to develop individual Soldier skills, crew drills, and battle drills, and refine tactical SOPs. Each set of tactical SOPs must be tailored to address theater-specific TTP and integrate new or additional capabilities required to operate in the designated joint operations area. New or additional capabilities can include materiel (quick reaction capabilities, system upgrades) and personnel (military or contract linguists, PED platoons, CI teams, additional HUMINT and SIGINT teams).

CRISIS

7-121. During crisis, brigades provide strategic leaders and JFCs with an alternative to deploying a corps or division. (See FM 3-0.) If strategic leaders or JFCs require a credible and rapidly deployable deterrent during an escalating crisis, they may decide to deploy a BCT, functional brigade, multifunctional brigade, or a combination thereof as part of a flexible deterrent option or flexible response option. MI forces may be included within the flexible deterrent option or flexible response option to provide capabilities to support deterrent and response options to prevent further escalation.

7-122. When BCTs provide support during crisis, they further tailor tactical SOPs to address theater-specific TTP. BCT intelligence leaders, granted with direct liaison authorized permissions by higher headquarters, collaborate closely with INSCOM and the national agencies to tailor capabilities to the specific OE and integrate new or additional capabilities, which can include materiel (such as quick reaction capabilities, hardware or software upgrades) and additional personnel (such as military or contract linguists). BCTs also establish communications and liaisons, as necessary.

ARMED CONFLICT

7-123. The BCT S-2 and intelligence staff support BCT operations from planning through execution. The BCT S-2 performs basic IPOE to support operations, such as an attack to penetrate an enemy defensive belt, a river crossing, or an envelopment. The information collection effort—

- Confirms or denies templated obstacles and enemy fighting positions, enemy reserves, and enemy attack positions.
- Generates targeting data and supports target detection.
- Supports both physical and functional damage assessments when it is a specific PIR.

7-124. The BCT S-2 or designated representative, working in conjunction with the S-3, generates taskings for assigned, attached, and supporting intelligence assets. Additionally, the S-2 develops NAIs or requirements tasked by the S-3 to units assigned a reconnaissance, surveillance, or security mission.

7-125. The MI company is tasked-organized to support BCT operations. It may receive and integrate E-MIB assets based on the situation. The MI company tactical intelligence ground station team provides limited PED capability to support the BCT Shadow UAS platoon or receive a moving target indicator from an airborne platform through the common data link. The S-2 coordinates additional PED requirements through the division. In addition to organic assets, the BCT integrates supporting assets into the information collection plan.

7-126. The BCT S-2 and intelligence staff synchronize intelligence with operations to ensure overmatch in the close fight. (See figure 7-3.) For example, SIGINT or EW coverage is synchronized with a friendly attack to detect enemy repositioning or enemy counterattack through either the EMS or by a moving target indicator. This synchronization allows the commander to visualize windows of opportunity and take advantage of these windows before they close.

Priority Intelligence Requirement	Indicators	Specific Information Requirements	NAI	ETIOV	LTIOV	Units and Capabilities														Decision Point	Target Area of Interest
						Brigade							Echelons Above Brigade								
						1st BN	2d BN	3d BN	1-1 CAV	Shadow	Prophet/LLVI	HCT	COMINT	ELINT	OSINT	HUMINT	GEOINT	CI	MASINT		
1. Where are the reconnaissance elements between PL Red and PL Blue?	1.1. Presense of 5 to 7 man teams	1.1.1. Report antenna relay arrays on hilltops	3001	H-2	H+2	C	TA	C	TP						R		R			1	10
			3006	H-1	H+3										R					3	11
		1.1.2. Report location of camouflage netting	3001	H-1	H+2	TP	TA								R		R			1	10
			3006	H-1	H+3										R		R		R	3	11
		1.1.3. Report communications of reconnaissance assets	3001	H-1	H+1	C	TA	C	TP	TA	TP	TA	R							1	10
			3006	H	H+2								R							3	11
	1.2. Presence of 1 or more BRDMs	1.2.1. Report visual location 4-wheeled armored vehicle	3001	H-4	H+2	C	TA	C	TP	TA	TP	TA			R		R			1	10
			3006	H-4	H+3										R		R			3	11
		1.2.2. Report presence of threat radars	3001	H-1	H+1									R	R					1	10
			3006	H	H+1		TA		TP	TA	TP			R	R					3	11
	1.3. Presence of suspected proxy forces vicinity OBJ Scorpio	1.3.1. Report activities of newly arrived personnel	3001	H-12	H+3	C	TP			TA	TP				R					1	10
			3006										R		R			R		3	11

BN battalion
BRDM Boyevaya Razvedyvatelnaya Dozornaya Mashina
C capable
CAV cavalry
CI counterintelligence
COMINT communications intelligence
ELINT electronic intelligence
ETIOV earliest time information is of value
GEOINT geospatial intelligence
HCT human intelligence collection team
H-hour specific hour at which a particular operation commences
HUMINT human intelligence
LLVI low-level voice intercept
LTIOV latest time information is of value
MASINT measurement and signature intelligence
NAI named area of interest
OBJ objective
OSINT open-source intelligence
PL phase line
R requested
TA tasked as alternate
TP tasked as primary

Figure 7-3. Information collection matrix example

SECTION VIII – BATTALION

7-127. The role of a battalion is closing with and destroying enemy forces using fires, movement, and shock effect, or repelling the enemy's assault by fire and counterattack. The battalion combines the efforts of its companies to execute tactical missions as part of the BCT or when augmenting another BCT. Amassing the combat power of these companies quickly, while integrating and synchronizing supporting and sustaining multipliers, is the key to victory. Combined arms battalions are organized to fight and win, but they are equally capable of executing stability and defense support of civil authorities (DSCA) operations as part of a JTF.

7-128. The manning of the intelligence staff and intelligence cell at the battalion level within the BCT varies with the type of battalion. The analytical and production capacity across the five types of battalions that are organic to a BCT varies according to the size of the intelligence staff and intelligence cell. For operational considerations, such as weighting the main effort, the BCT may task-organize intelligence support teams from the MI company, CI teams, HUMINT teams, or SIGINT teams to support a battalion. Additionally, a battalion may use remote sensors for defense or information collection purposes. (For doctrine on battalion intelligence activities, see ATP 2-19.4.)

BATTALION S-2

7-129. The battalion S-2 provides timely, accurate intelligence analysis and products to support the commander, staff, and subordinate units. The battalion S-2—

- Acts as the principal intelligence advisor to the battalion commander.
- In conjunction with the S-3, supervises and coordinates the collection, processing, production, and dissemination of intelligence.
- Plans and manages information collection tasks in coordination with the S-3 and fires cell.
- Evaluates the enemy in terms of doctrine, threat characteristics, HVTs, capabilities, and vulnerabilities.
- In conjunction with the S-3, coordinates the battalion staff's recommendations for specific PIRs to be designated as CCIRs.

BATTALION INTELLIGENCE CELL

7-130. The battalion intelligence cell contains the battalion S-2, an assistant S-2, and one or more all-source intelligence analysts. The cell makes analytical predictions on when and where actions will occur. It also provides analysis on the effects of relevant aspects of the OE on friendly and enemy COAs and capabilities. The intelligence cell integrates staff input to IPOE products for staff planning, decision making, targeting, and combat assessment. A battalion intelligence cell is also responsible for—

- Attending all MDMP and targeting meetings.
- Proposing new PIRs to the commander.
- Providing the staff with a detailed projection of possible enemy COAs for the next 24 to 72 hours, based on all enemy, terrain, and weather factors.
- Creating and maintaining the intelligence running estimate, which provides the commander and staff with current assessments of the situation in the AO, based on enemy activities and other relevant aspects within the AO.
- Integrating reporting into intelligence cell products.
- Leveraging the brigade GEOINT capability, as appropriate.
- Coordinating with the USAF SWO assigned to the BCT to provide—
  - Weather forecasts and effects on operations and capabilities (friendly and threat) and enemy COAs, based on current and predictive weather conditions in the OE, for integration into the MDMP and targeting process.
  - The weather estimate, weather portion of the running estimate, or updated weather estimate.

INTELLIGENCE COLLECTION CAPABILITIES

7-131. Table 7-10 lists maneuver battalion-level intelligence capabilities. Organic BCT MI company intelligence assets may downward reinforce maneuver battalions or maneuver companies. Close coordination and an adequate lead time are required to ensure the effective flow of information and intelligence.

Table 7-10. Battalion organic and supporting intelligence collection capabilities

Battalion organic collection capabilities
Small UASs and scout platoon[1]. Unmanned ground systems and snipers[1].
Battalion supporting collection capabilities
May be augmented by the BCT MI company depending on the commander's requirements and priorities. Possible augmentation includes 1x SCT and 1x HCT.
Note. The communications infrastructure, the threat, and the tempo may affect the ability to employ or emplace systems or sensors to their full potential. [1] Small UASs, scout platoon, unmanned ground systems, and snipers (when in the MTOE, resourced, and equipped) are not intelligence systems, but they provide an important information collection capability.

BCT	brigade combat team	MTOE	modified table of organization and equipment
HCT	human intelligence collection team	SCT	signals intelligence collection team
MI	military intelligence	UAS	unmanned aircraft system

ALL-SOURCE INTELLIGENCE CAPABILITIES

7-132. All-source intelligence supports the commander's tactical requirements, which focus on enemy tactical forces operating within a short window of action. Table 7-11 describes maneuver battalion-level all-source intelligence capabilities.

Table 7-11. Battalion-level all-source intelligence capabilities

Intelligence support to—	***Analytical focus: Maneuver battalion***	***Analytical window***
Current operations	**Analytical tasks:** Provide warning intelligence, perform situation development, and conduct collection management.	Current to 12 hours
Future operations	• **Analytical tasks:** Conduct pre-mission analysis of the OE for the battalion, perform tactical IPOE, and perform tactical situation development to the battalion. • Provide analytical support to the battalion commander's MDMP and collection requirements. • Provide support to targeting.	12 to 24 hours **Echelon focus:** Brigade to company/battery maneuver artillery units.
Note. Time windows are examples; actual time windows depend on the situation. All analysis thoroughly accounts for civil considerations, terrain, and weather forecasts and effects on capabilities.		

BCT	brigade combat team	MDMP	military decision-making process
IPOE	intelligence preparation of the operational environment	OE	operational environment

This page intentionally left blank.

Chapter 8

Fighting for Intelligence During Large-Scale Combat Operations

SECTION I – OVERVIEW

8-1. Fighting for intelligence during large-scale combat operations (armed conflict) is very different than fighting for intelligence during competition and crisis. Before large-scale combat operations and deployment, friendly forces have been under continuous enemy observation and influence. Enemy influence has occurred through the information dimension (including through social media, telecommunications, human interaction, and other forms of communications and contact) with the intent to shape the perceptions, behaviors, and decision making of the United States and allied and partner nations. However, with the onset of large-scale combat operations and deployment, the amount, intensity, and lethality of enemy actions increase drastically.

8-2. During large-scale combat operations, operational success requires a successful intelligence effort. Intelligence success during large-scale combat operations requires aggressive preparations during competition and crisis. Intelligence architecture planning and revising, joint TSA, regional expertise, intelligence databases, threat signatures, threat characteristics and models, and intelligence and language training must all be developed or conducted before large-scale combat operations; the intelligence warfighting must not begin a large-scale combat operation as a *cold start*.

8-3. Building on chapters 1 through 7, this chapter focuses on the tactical aspects of large-scale combat operations. All echelons are important to operations; theater army and corps echelons, as joint land component commands, play pivotal roles in successful large-scale combat operations. However, this chapter discusses corps (not as a joint land component command), division, and BCT echelons.

SECTION II – CHALLENGES

8-4. There are many challenges to effective intelligence support during large-scale combat operations. Staff integration, operational planning, and information collection plans are not foolproof and can become ineffective. Army forces compete with a determined and adaptive enemy; therefore, perfect planning and information collection seldom occur. Intelligence is not perfect, information collection is not easy, and a single collection capability (or even all collection at a single echelon) is not persistent and accurate enough to provide all the answers. Conducting information collection requires focused intelligence requirements, thorough and creative planning, aggressive execution, and adjustments based on the operational situation to inform the commander's situational understanding and support decision making and targeting.

8-5. The commander and staff must understand the doctrinal fundamentals of fighting for intelligence and maintain proficiency in integrating the intelligence warfighting function into operations. Conducting realistic staff and intelligence training and building effective relationships are vital to successful intelligence support during the rigors and stresses of combat operations. This section discusses some of the many challenges of a contested deployment and the conduct of operations and intelligence support after RSOI.

CONTESTED DEPLOYMENT

8-6. Threat information warfare operations can have a global reach and hamper friendly military deployments. With sufficient scale or precision, they have the potential to completely halt effective unit deployment operations. Targeted disinformation and threats delivered via social media to the Family members of every Soldier in a unit can be potentially devastating without prior planning, preparation, and trust building.

8-7. Commanders and their staffs must understand the potential effects of adversarial disinformation operations on units and leaders. Targeted adversary or enemy activities in the information dimension can rapidly degrade Soldiers' performance, impacting their readiness. These activities can also degrade civilian performance and affect the critical infrastructure they manage. Leaders combat this through—

- Public communications, both before and during deployment operations.
- Coordination with relevant public affairs personnel.
- Soldier and Family preparation, which can include incorporating response strategies for disinformation dissemination into exercises and other training.

8-8. As friendly forces transition from competition and crisis to armed conflict, threat actors increase the intensity and lethality of their tactics. This can include infrastructure sabotage by pre-positioned agents, a broad scope of cyberspace or information attacks (such as targeting an oil pipeline supplying a large region rather than only a specific port), or long-range precision strikes using a variety of munitions. Concurrently, threat actors posture for, and may eventually escalate through, nonlethal and lethal actions of increasing intensity to improve standoff and prevent power projections from the U.S. homeland and other basing and staging areas. Threat actors may also strike transport vessels along sea lines of communications while these vessels are enroute to a seaport of debarkation.

8-9. Peer threats may choose to support proxy forces or influence unwitting groups, including irregular forces, saboteurs, sympathetic civil organizations, and criminals. These groups may be used to prevent timely deployment operations by denying access to roads or facilities with crowds, protests, or looting. Using these forces may also allow for direct action against U.S. targets while masking the responsible nation or group. Threat actors may design these activities to affect the economy and global trade in addition to the political-military balance in the United States or overseas. Additionally, other state and nonstate actors may exploit the situation with attacks to pursue their own objectives. These attacks may be conducted within the United States or allied nations, in the theater where Army forces are preparing to deploy, or in other, unrelated regions.

8-10. Leaders anticipate adversary activities in all domains while preparing for or conducting deployment operations. Disruptions may not be preventable. They can, however, be mitigated through intelligence support, training, preparation, and coordination with unified action partners. Effective mitigation in planning, preparation, and execution ensures the Army provides the required forces to CCDRs and other JFCs.

8-11. FM 3-0 discusses how deployments comprise various movements and activities—fort to port, port to port, and RSOI—all of which involve unique intelligence considerations. (See appendix C and FM 3-0.) Most subsequent discussions in this chapter address actions after friendly force RSOI. Following RSOI, there may be challenges for the intelligence warfighting function based on the loss of or delay in receiving intelligence personnel or the loss, delay, or damage to intelligence systems.

Fluid Reception, Staging, Onward Movement, and Integration Operations

As part of peer threat A2 and AD, long-range strike capabilities mean that sanctuary to conduct unimpeded RSOI operations in rear areas can no longer be assumed; it is likely that strikes by peer threats will degrade or destroy port and other transportation infrastructure vital to U.S force projection. This can cause Army forces to arrive in a disaggregated manner and disrupt RSOI operations. While integrating U.S. forces in theater can be challenging, Army planners must consider host-nation requirements for logistics infrastructure. The host nation's response to an attack on its infrastructure, including its military mobilization, can affect freedom of movement for U.S. forces. These challenges may require JFCs to alter their operational plans or remain defensively postured until sufficient combat power is built to enable offensive operations.

The theater army has primary responsibility for conducting RSOI operations for the entire joint land force. Once the E-MIB is set in theater, the theater army may task the E-MIB commander and staff to assist in conducting RSOI as subsequent MI units deploy. However, executing RSOI is primarily a unit responsibility. The deploying unit must conduct detailed planning and proper coordination before deploying. Planning must include mitigation actions in the event systems are damaged or destroyed and MI Soldiers are injured or killed during deployment.

Army equipment may arrive haphazardly across numerous ports. Commanders must establish secure communications, allowing staff coordination for unit personnel to meet their equipment and facilitate ship offloading. Units provide port support teams with the right personnel and capabilities, such as licensed vehicle operators and communications, to expedite port operations. This assists in ensuring ports of debarkation are not congested with disabled equipment or frustrated cargo. If some unit equipment is lost in transit due to the destruction of transport vessels, some tactical unit personnel may be held temporarily at theater facilities to facilitate re-equipping efforts, or they may be retasked by the combatant command or theater army commander.

OPERATIONAL CHALLENGE

8-12. As friendly forces flow into the theater, they will be faced with the intensity, lethality, and brutality of large-scale combat operations, which create complex, chaotic, fearful, violent, fatiguing, and uncertain conditions. 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, systems warfare, and information warfare. Activities in the information dimension will often be inseparable from ground operations.

8-13. Conflicts encompassing large-scale combat operations are more intense and destructive than limited contingencies. During large-scale combat operations, peer threats will mass effects across multiple domains and dimensions at speeds that will significantly impact ongoing operations. Peer threats will employ many highly lethal and sophisticated capabilities, such as information warfare, cyberspace attacks, counterspace measures, long-range massed fires, IADSs, EW, deception, reconnaissance, and counterreconnaissance, to deny and degrade friendly force maneuver, communications, information collection, and targeting capabilities, particularly when they are static.

8-14. Large-scale combat operations typically entail—

- High-resource consumption, high casualty rates, and an incredible level of stress on all aspects of sustainment. Flexibility and adaptability at all echelons are critical.
- The deliberate and imaginative use of capabilities within and across all domains synchronized to create effects across all dimensions to gain and exploit positions of relative advantage.
- The ability to effectively provide the joint force with important capabilities and employ joint capabilities when they are allocated.
- Focusing operational and mission variables through the sequence of planning and execution necessary to apply combat power on threat defeat mechanisms.

- The execution of campaigns and effective tactical transitions between offensive, defensive, and stability operations.
- Tactical actions that in some cases can have strategic impacts to an international audience.
- Eventual negotiations, peace talks, and other political considerations.

8-15. Successful large-scale combat operations defeat enemy-armed forces while establishing control over land and populations to achieve strategic and operational objectives. They may capitalize on superior military capability to quickly overwhelm a weaker enemy and consolidate gains as part of a rapid campaign. Large-scale combat operations against more capable enemy forces are likely to be of longer duration, lasting months or longer. When operating against a peer threat, commanders aggressively and simultaneously conduct offensive, defensive, and stability operations to seize, retain, and exploit the initiative. Army operations must orchestrate many simultaneous actions in the most demanding OEs. Figure 8-1 illustrates the scope, complexity, and lethal nature of large-scale combat operations.

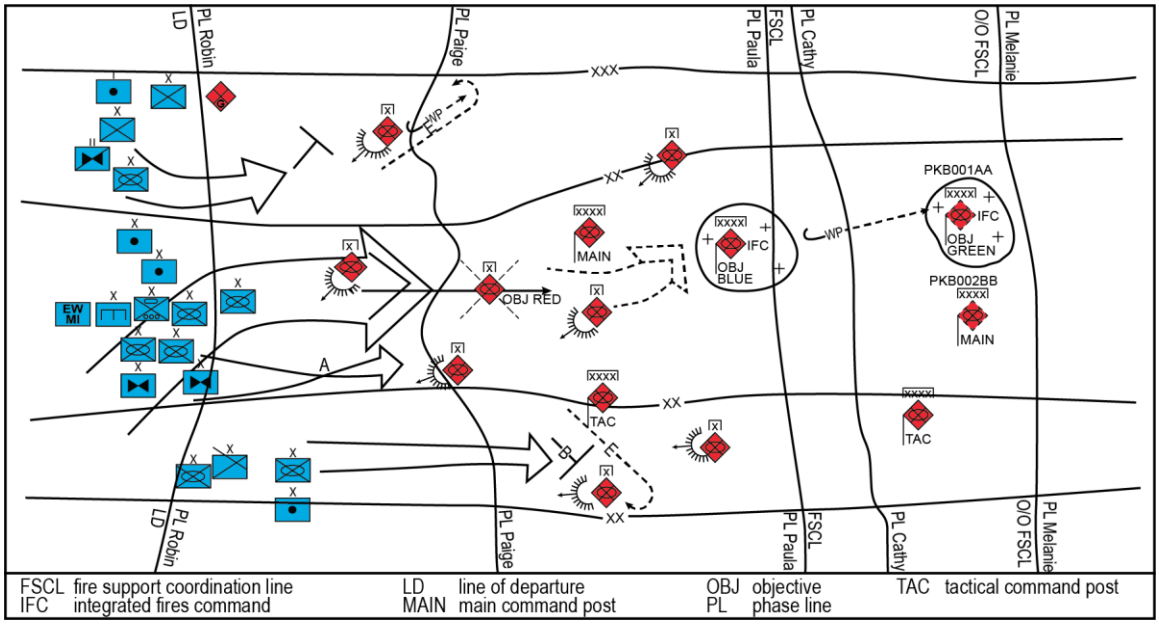


Figure 8-1. Large-scale combat operations (offensive action) (example)

INTELLIGENCE CHALLENGE

8-16. The fluid and chaotic nature of large-scale 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 OE. The challenges to information collection include IADSs, long-range fires, counterreconnaissance, cyberspace and EW operations, and camouflage, concealment, and deception. The enemy's ability to create a denied, disrupted, intermittent, and limited (DDIL) communications environment can have major impacts on intelligence support.

8-17. Despite these challenges, commanders and staffs must have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations. This is essential when determining how best to mitigate sophisticated threat A2 and AD systems, IADSs, deception, information warfare, EW operations, UAS swarms, robotics, and long-range fires capabilities. Additionally, there are many unique requirements to account for civil considerations and support sustainment operations and friendly activities within the various rear areas.

8-18. IPOE and information requirements differ significantly during large-scale combat operations and often require detailed analysis. IPOE and information requirements, in supporting warning intelligence (which indicates changes in the likelihood of threat actions against friendly forces or developments likely to cause harm to friendly forces), are especially important in protecting the force. IPOE and information requirements also differ significantly based on the defensive or offensive operation, the specific situation, and unique requirements for concurrent supporting operations such as deep and rear operations. During both friendly defensive and offensive operations, there are consolidating gains 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. Example IPOE and information requirements are listed throughout section III for the operational framework and various types of operations.

8-19. Although large-scale combat operations considerations span the intelligence process, three areas of particular importance to intelligence include—

- The intelligence architecture.
- PED.
- Information collection.

INTELLIGENCE ARCHITECTURE

8-20. During competition, the intelligence architecture is developed well before any deployments based on future planning and assumptions regarding the employment of intelligence capabilities. During crisis and into a large-scale combat operation, intelligence leaders must carefully plan for revisions to the existing intelligence architecture and expand it as tactical units arrive in or move within a theater.

8-21. During competition or crisis, no matter how well-planned, the friction of deployment and then large-scale combat operations can adversely affect the use and tactical extension of the intelligence architecture. For example—

- The TPFDL may have execution flaws when situations arise that demand changes. This, in turn, delays transport and arrival in theater of key intelligence architecture components.
- Damage to equipment essential to the intelligence architecture during transit from garrison to the port of debarkation may delay the integration and employment of that equipment into the intelligence architecture.
- Friction at the port of debarkation, along forward movement routes, and at intermediate staging bases in theater, especially during contested deployments, can multiply RSOI challenges, which may impact the arrival and integration of intelligence architecture components.

8-22. Friendly actions and conditions can also challenge establishing the intelligence architecture. For example—

- U.S. forces may have to operate on a theater-specific network such as CENTRIXS or US BICES.
- Receipt in theater of unanticipated Army, joint, and multinational reinforcing units adds requirements that stress the capabilities of the intelligence architecture.
- Receipt in theater of new or unanticipated information collection or foundational capabilities stresses the ability to integrate these capabilities into the intelligence architecture when time available is limited and interoperability is less than optimal.
- Greater congestion (more intelligence nodes than in peacetime) and greater volumes of transported data and information strain the intelligence architecture.

PROCESSING, EXPLOITATION, AND DISSEMINATION

8-23. Deployment and then large-scale combat operations can also cause the highest level of stress on the conduct of intelligence PED activities. Leaders and Soldiers must anticipate, plan, and train for intelligence PED in conditions closely resembling the strenuous conditions of large-scale combat operations. Although these high stress levels cannot be replicated in training environments, CP exercises, or field training exercises, leaders and Soldiers must exercise flexibility, adaptability, and creativity in performing intelligence PED tasks during large-scale combat operations.

Note. Intelligence PED capabilities and activities depend on intelligence architectures; therefore, they incur the same challenges and risks that intelligence architectures must face and overcome in large-scale combat operations.

INFORMATION COLLECTION GAPS

8-24. After RSOI, as tactical units start information collection, there may be significant challenges based on enemy capabilities and risks to Soldiers. The inability to collect at certain locations and ranges without a high degree of risk to organic, attached, assigned, and supporting collection capabilities is considered a collection gap. Section IV discusses mitigating collection gaps.

8-25. Information collection gaps often occur due to the following:

- Threat capabilities, including countermeasures limiting or preventing friendly collection.
- Insufficient networks, systems, or personnel/linguists.
- Lack of technical capabilities.
- Inadequate collection ranges.
- Movement in preparation for operations.
- A high tempo and constant maneuver.
- Unfavorable terrain.
- Unacceptable risk for the employment of specific assets.
- National technical means, when available, focus on national priorities. Even when aligned against joint force command priorities, these means may not meet tactical-level requirements.
- Collection may not be authorized due to international borders, existing agreements, or areas that are not part of a joint operations area.
- Most of the other Service ISR systems do not focus on ground requirements unless they are allocated to Army forces.
- Most theater-level intelligence collection assets and sensors are employed to answer theater intelligence requirements.
- Collection factors can significantly impact intelligence operations from theater army to BCT levels. The intelligence cell and MI unit must consider these factors during planning. Collection factors include—
  - The impact of enemy IADS on aerial collection.
  - Limits on the range of ground collection.
  - Geography.
  - Technical aspects of collection capabilities.
  - Threat signatures.
  - The specific operational and tactical situation.

SECTION III – DEFENSIVE AND OFFENSIVE OPERATIONS (FRIENDLY)

8-26. Corps and division commanders are directly concerned with those enemy forces and capabilities that can affect their current and future operations. Successful corps and division operations may depend on intelligence and successful joint interdiction operations, including those operations to isolate the battle or weaken the enemy force before the battle is fully joined.

8-27. Corps and divisions execute defensive, offensive, and stability operations, of which offensive and defensive operations comprise most of the activities. Commanders must focus and use intelligence to explicitly understand the lethality of large-scale combat operations to preserve their combat power and manage risk. Commanders must also use ground maneuver and other land-based capabilities to enable maneuver in the other domains.

8-28. BCTs and subordinate echelons concentrate on performing defensive and offensive operations and necessary enabling operations, such as reconnaissance, security, or passage of lines. During large-scale combat operations, they only perform those minimum-essential stability operations tasks (paragraph 8-49) necessary to comply with the laws of land warfare and applicable international standards. These requirements create an even greater challenge for the intelligence warfighting function because operations to consolidate gains require a dynamic intelligence effort to maintain positive momentum and achieve additional gains.

FUNDAMENTALS OF DEFENSIVE AND OFFENSIVE OPERATIONS

8-29. The effective application of tactics creates multiple dilemmas for the enemy, allowing the friendly commander to prevail in combat operations. Successful tactics also require synchronizing all elements of combat power. The intelligence warfighting function fuses information collected from the primary tactical tasks of reconnaissance, surveillance, security operations, and intelligence operations. These complementary and reinforcing effects contribute to effective defensive and offensive operations. For the intelligence warfighting function to be successful during large-scale combat operations, intelligence professionals must understand the doctrinal fundamentals of defensive and offensive operations as well as the forms of contact; deep, close, and rear operations; and enabling operations.

FORMS OF CONTACT

8-30. Commanders consider all forms of contact possible with enemy forces and visualize their AOI as the situation develops, including effects of enemy influence and disinformation and misinformation. During IPOE, the G-2/S-2, in coordination with other staff members, determined how capabilities can be leveraged against friendly forces using the nine forms of contact. During the MDMP, the commander and staff determine how to leverage the nine forms of contact within the OE.

8-31. Tactics assist the G-2/S-2, in conjunction with the commander and staff, in determining the best form of contact to engage enemy forces. *Contact* is an interaction between two or more forces. The nine forms of contact describe the method of interaction that positively identifies the location or activity of a force:

- **Direct:** Interactions from line-of-sight weapons systems (small arms, heavy machine guns, and antitank missiles) in any domain.
- **Indirect:** Interactions from non-line-of-sight weapons systems (cannon artillery, mortars, rockets).
- **Nonhostile:** Neutral interactions (civilians on the battlefield) that may degrade military operations.
- **Obstacle:** Interactions from friendly, enemy, and natural obstacles (minefields and rivers).
- **CBRN:** Interactions from friendly, enemy, and civilian CBRN effects (chemical, nuclear, and biological attacks; industrial accidents; and toxic/hazardous industrial materials).
- **Aerial:** Interactions from air-based combat platform effects (attack helicopters, armed UASs, and close air support).
- **Visual:** Interactions from acquisition via the human eye, optical, or electro-optical systems (ground reconnaissance telescopic, thermal, and infrared sights on weapons and sensor platforms such as UASs and satellites).
- **Electromagnetic:** Interactions via systems used to acquire, degrade, or destroy using select portions of the EMS (radar systems, jamming, cyberspace, space-based systems, and electromagnetic pulse).
- **Influence:** Interactions through the information dimension (social media, telecommunications, human interaction, other forms of communications and contact) intended to shape the perceptions, behaviors, and decision making of people relative to a policy or military objective.

DEEP, CLOSE, AND REAR OPERATIONS

8-32. Within assigned areas, commanders organize their operations in terms of time, space, and purpose by synchronizing deep, close, and rear operations. An echelon's focus in time, space, and purpose—not necessarily the echelon's physical location—determines whether the echelon conducts deep, close, or rear operations. The deep. close, and rear operations model assists commanders and staffs in synchronizing capabilities that reside outside of their unit's assigned area (for example, from air, space, cyberspace), with

operations inside their assigned areas. Intelligence support to deep, close, and rear operations involves close coordination with the operations staff to determine how the intelligence warfighting function can best support operations at any given time. Although deep, close, and rear operations are distinctly different, aspects of each may overlap; likewise, at times intelligence operations in each may comprise similar activities.

8-33. Typically, corps and divisions assign CPs to enable control of deep, close, and rear areas. At echelons brigade and below, differentiating between deep, close, and rear areas may have less utility during large-scale combat operations because of the high tempo, narrow focus, and short planning horizons. However, at every echelon, commanders must understand the relationship among these operations and their combined impact on mission accomplishment. (See FM 3-0 and FM 3-94 for doctrine on deep, close, and rear operations.)

8-34. Intelligence synchronization across deep, close, and rear operations is required to ensure the unity of support and unity of effort. This mitigates the dynamic nature of the OE. Operations in each area will cause effects, impacting threat, neutral and friendly forces. These impacts must be continuously monitored to ensure commanders and staffs have the most updated and accurate assessments from which to make decisions. For example, information regarding bypassed enemy forces in the close area must be received by units in the rear and deep areas to assist in deep and rear area assessments.

8-35. Commanders, G-2/S-2s, and the staff must ensure analytical sections in deep, close, and rear areas are manned, able to assess threat activities in each area, and have access to an architecture to share information across these areas. During large-scale combat operations, analytical elements in the three areas must collaborate to ensure threat monitoring is maintained as the unit maneuvers through their AORs and communicate that information to subordinate elements.

8-36. The fusion of information and intelligence from the deep, close, and rear areas provides commanders and staffs with a holistic picture, from which to build assessments of current operations and subsequently provide the relevant information to determine future operations. G-2/S-2s must maintain communications with higher, subordinate, and adjacent echelons to ensure all relevant information regarding the OE is assessed, considered, and incorporated into operations. Figure 8-2 illustrates the variety of activities across the operational framework and how they interrelate.

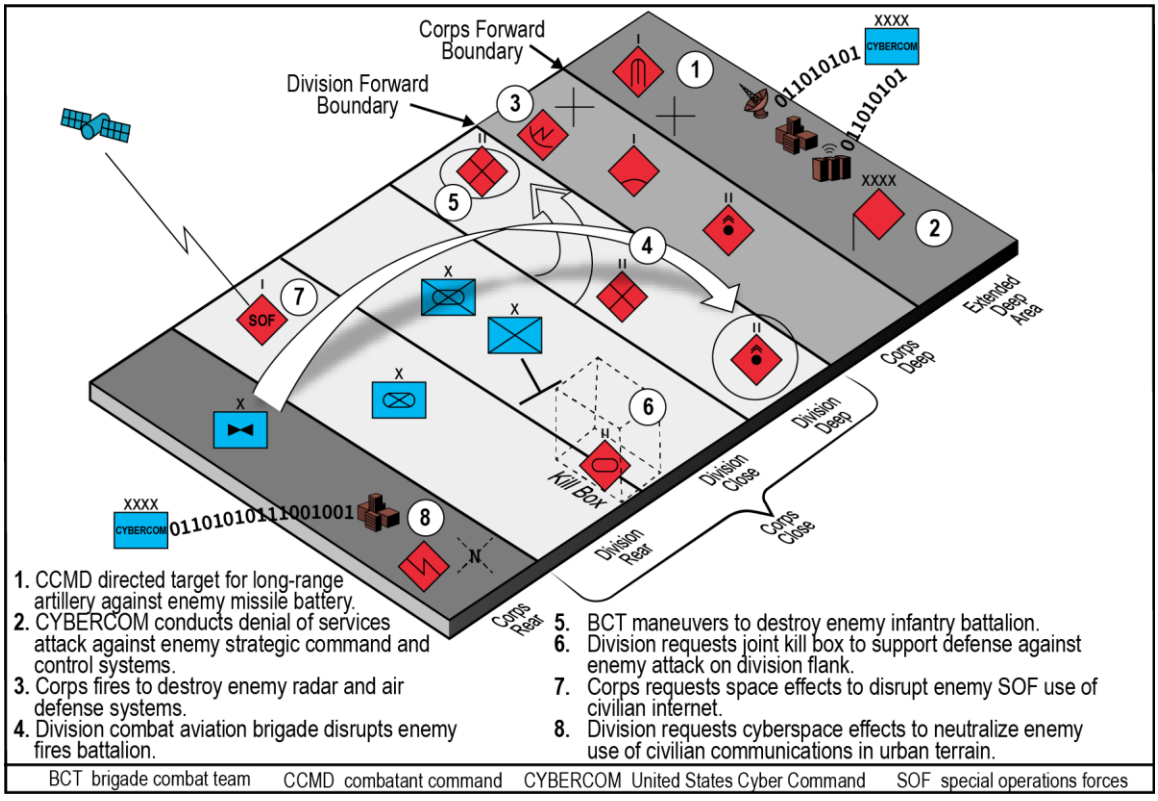


Figure 8-2. Notional operational framework during offensive operations

Deep Operations

8-37. At the operational level, deep operations influence the timing, location, and enemy forces involved in future battles; at the tactical level, deep operations set conditions for success during close operations and subsequent engagements. The principal effects of deep operations focus on an enemy force's freedom of action and the coherence and tempo of their operations. (See ATP 3-94.2 for doctrine on deep operations.)

8-38. Deep operations 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. The following activities are typically conducted as part of deep operations either singly or in combination:

- Deception.
- Information collection and target acquisition.
- Interdiction (by ground or air fires, ground or aerial maneuver, cyberspace forces, special operations forces, or any combination of these).
- Long-range fires against enemy IADSs, sustainment nodes, fires capabilities, and echeloned follow-on maneuver formations.
- EW.
- Information advantage activities.
- Offensive cyberspace operations.
- Space operations.
- Military information support operations.

8-39. Not all activities focused forward of the line of contact are deep operations. For example, counterfire primarily supports close operations although the targets attacked may be located at great distances from the forward line of troops.

8-40. Deep operations focus on the enemy vulnerabilities and capabilities most dangerous to the next close operation. These operations 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. Attacks must employ enough combat power to achieve the desired result. This is critical when—as is frequently the case—maintaining momentum in close operations depends on the successful prosecution of deep operations.

8-41. Intelligence support to deep operations is an inherent part of intelligence support to targeting. IPOE and information requirements related to deep operations include—

- Gaining and maintaining threat activities and intentions, which focus on—
  - Locating the enemy reserve.
  - Locating enemy forces capable of impacting the close fight.
  - Locating long-range fires capabilities and other A2 and AD capabilities.
  - Locating C2 nodes.
  - Locating logistics nodes.
  - Disrupting enemy recruiting activities.
  - Enemy intentions during friendly transitions.
- Key and decisive terrain associated with the deep operation.
- Enemy indicators that allow the commander to identify time windows to conduct deep operations.
- HPTs and target system components vulnerable to attack as well as the most effective method of attack.
- BDA to determine if the correct target was attacked, the results of that attack, if reattack is required, and the impact of the attack on enemy COAs.

- Information gaps in deep operations intelligence and developing collection strategies to fill those gaps.
- Support to protection activities.
- Support to security activities.
- Activities to consolidate gains.
- Integrating intelligence, civil information, military information support operations, cyberspace, and electromagnetic activities.
- The convergence of capabilities from multiple domains to isolate, penetrate, and disintegrate an enemy's integrated fires commands and IADSs.

Close Operations

8-42. Until enemy forces are defeated or destroyed in close operations, they retain the ability to fight and hold ground. Close operations include the deep, close, and rear operations of their subordinate maneuver formations. For example, divisions and separate brigades conduct corps close operations. BCTs are the primary forces conducting division close operations. (See FM 3-0.) Due to the relationships of these operations, intelligence activities must be synchronized across the operational areas. G-S/S-2s at all echelons must ensure the intelligence effort is synchronized and unified, lessening the possibility for gaps in information collection coverage.

8-43. Close operations occur in the *close area*—the portion of the commander's area of operations where the majority of subordinate maneuver forces conduct close combat (ADP 3-0). The close area contains the current battles and engagements of its major maneuver units. For example—

- A field army's close area is where its committed corps and divisions conduct operations.
- A corps' close area includes the deep, close, and rear areas of its committed divisions and separate maneuver brigades.
- A division's close area is primarily where BCTs operate.

8-44. Speed and mobility are essential to close operations to exploit windows of opportunity by rapidly concentrating overwhelming combat power at the right time and location. Close operations comprise the following activities:

- Maneuver of subordinate formations (including counterattacks).
- Close combat (including offensive and defensive operations).
- Indirect fire support (including counterfire, close air support, EA, and offensive space and cyberspace operations against enemy forces in direct physical contact with friendly forces).
- Information collection.
- Sustainment support of committed units.

8-45. Intelligence activities in close operations (corps and division) focus on—

- Continuous monitoring of threat activities in corps and division deep areas.
- Gaining and maintaining information concerning threat activities and intentions:
  - Locating and targeting HPTs.
  - Locating and targeting bypassed forces.
  - Locating enemy reserve forces.
  - Identifying and exploiting windows of opportunity across all domains and dimensions.
  - Locating threat capabilities that may impact sustainment operations.
- Considering flexibility when planning information collection.
- Achieving relative advantages across relevant domains and dimensions.
- Synchronizing the use of intelligence handover lines.
- Activities to consolidate gains.
- Support to security operations.
- Protecting critical infrastructure and key lines of communications for future operations.
- Ensuring continuous updates to the CIP.

8-46. Intelligence activities in close operations (BCT) focus on—

- Gaining and maintaining information concerning threat activities and intentions:
  - Locating and targeting HPTs.
  - Providing support to branches and sequels.
  - Locating and targeting bypassed forces.
  - Locating reserve forces.
  - Locating present/planned obstacles, including the use of obscuration and chemical weapons.
  - Threat's use of denial and deception.
  - Threat's use of EW.
  - Threat's use of misinformation and disinformation in population centers.
  - Threat's use of UASs, including drone swarms.
- Activities to consolidate gains.
- Support to security activities.
- Support to protection activities.

Rear Operations

8-47. The rear area is that area in a unit's AO extending forward from its rear boundary to the rear boundary of the area assigned to the next lower level of command. Operations in this area facilitate movement, extend operational reach, and maintain the desired tempo. Rear operations support close and deep operations. At the operational level, rear operations sustain current operations and prepare for the next phase of the campaign or major operation. At the tactical level, they enable the tempo of combat, assuring friendly forces have the agility to exploit any opportunity.

8-48. Rear operations typically include efforts that consolidate gains to make conditions created by deep and close operations more permanent. Corps and division rear CPs are generally responsible for rear operations. Rear operations typically include five broad activities:

- Positioning and moving reserves.
- Positioning and repositioning aviation, fire support, and air and missile defense units.
- Conducting support area operations.
- Securing sustainment and C2 nodes.
- Controlling tactical-unit movement between corps and divisions or rear boundary and units conducting close operations.

8-49. There are several considerations for conducting rear operations:

- C2.
- Information collection activities to detect enemy forces.
- Establishing and maintaining routes.
- Terrain management.
- Movement control.
- Protecting critical friendly capabilities.
- Information activities.
- Infrastructure repair and improvement.
- Defeating bypassed forces and continuing to consolidate gains.
- Minimum-essential stability operations tasks:
  - Establish civil security, which requires Army units to protect the population from violence and restore public order.
  - Provide immediate needs, which requires Army units to ensure the population has food, water, shelter, and emergency medical treatment.
- Coordinating with host-nation and multinational governmental organizations.

- Adjusting to shifts in the unit and subordinate rear boundaries.
- Integrating new units into corps and divisions.

8-50. Intelligence support to rear operations focuses on ensuring operational and tactical gains achieved during operations are not lost and the tempo of operations in close and deep areas is maintained. IPOE and information requirements related to sustainment operations include but are not limited to—

- Gaining and maintaining information concerning threat activities and intentions such as—
  - Threat capabilities that may impact sustainment operations.
  - Bypassed forces that may impact rear operations.
  - Threat capabilities that may impact freedom of maneuver for friendly forces through the AO.
  - Threat long-range fires capabilities.
- Support to security activities.
- Support to protection activities.
- Activities to consolidate gains.
- Support to developing and implementing stability mechanisms.
- Key and decisive terrain associated with rear operations.
- Support to echelons conducting consolidating gains activities.
- Support to protection and security operations.
- Support to information advantage activities.
- Information gaps in rear operations intelligence and developing collection strategies to fill the gaps.

SETTING CONDITIONS: ENABLING OPERATIONS

8-51. There are many important aspects of offensive and defensive operations, including enabling operations. An *enabling operation* is an operation that sets the friendly conditions required for mission accomplishment (FM 3-90). The nine types of enabling operations are—

- Reconnaissance.
- Security operations.
- Troop movement
- Relief in place.
- Passage of lines.
- Countermobility.
- Mobility.
- Tactical deception.
- Linkup.

8-52. Reconnaissance and security operations are the enabling operations most important to the intelligence warfighting function. In combat, seizing the initiative involves conducting reconnaissance, maintaining security, conducting defensive and offensive operations at the earliest possible time, forcing the enemy to culminate offensively, and setting the conditions to prevail.

Reconnaissance

8-53. Commanders normally assign reconnaissance objectives, which can be a specific geographic location, a specific enemy activity to be confirmed or denied, or a specific enemy unit to be located and tracked. Reconnaissance objectives can focus on any operational or mission variable about which the commander wants to obtain additional information. Therefore, every reconnaissance is different and there is no general list of information requirements. The following are the five types of reconnaissance operations:

- *Zone reconnaissance* is a form of reconnaissance operation that involves a directed effort to obtain detailed information on all routes, obstacles, terrain, and enemy forces within a zone defined by boundaries (FM 3-90). Commanders assign a zone reconnaissance when they need additional information on a zone before committing other forces.
- *Area reconnaissance* is a form of reconnaissance operation that focuses on obtaining detailed information about the terrain or enemy activity within a prescribed area (FM 3-90). This area may consist of a single location, such as a town, a ridgeline, a forest, an airhead, a bridge, an installation, or any other critical operational feature such as obstacles.

- *Route reconnaissance* is a form of reconnaissance operation to obtain detailed information of a specified route and all terrain from which the enemy could influence movement along that route (FM 3-90). The route may be a road, highway, trail, mobility corridor, AA, or axis of advance. The reconnaissance effort provides new or updated information on route conditions, such as obstacles and bridge classifications, and enemy, adversary, and civilian activity along the route.
- *Reconnaissance in force* is a form of reconnaissance operation designed to discover or test the enemy's strength, dispositions, and reactions or to obtain other information (FM 3-90). Battalion-sized task forces or larger organizations usually conduct a reconnaissance in force. Commanders assign this operation when an enemy force is operating within an area, and they cannot obtain adequate information about the enemy force by other means.
- *Special reconnaissance* is reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces (JP 3-05). Special reconnaissance provides an additional capability for commanders and supplements other conventional reconnaissance and surveillance actions.

8-54. Table 8-1 shows the echelon/type of unit that can conduct the types of reconnaissance operations.

Table 8-1. Types of reconnaissance operations and dedicated reconnaissance units

Type of reconnaissance	*Scout platoon*	*Troop or company*	*Air cavalry*	*Cavalry squadron*	*BCT*	*Division*	*SOF*
Zone	X	X	X	X	X		
Area	X	X	X	X	X		
Route	X	X	X				
Reconnaissance in force				X (if reinforced)	X	X	
Special							X

BCT brigade combat team SOF special operations forces

8-55. Reconnaissance is a focused collection effort. During any type of reconnaissance, the commander may require information about a specific aspect of the AO. To obtain this information the commander may direct a specific focus task that typically requires using an organization uniquely trained and equipped for the mission. The following include focus tasks:

- *Electromagnetic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-85). Electromagnetic reconnaissance supports information collection at brigade and higher echelons using assigned EW personnel and capabilities. Information obtained through electromagnetic reconnaissance assists the commander with situational understanding and can support SIGINT activities. Electromagnetic reconnaissance may result in EP modifications or lead to an EA against enemy capabilities. Regarding the EMS, commanders use electromagnetic reconnaissance assets to identify enemy attempts to regain the initiative, readjust targeting priorities and fire support plans, and keep adversaries on the defensive. (See FM 3-12.)
- *Engineer reconnaissance* includes missions to obtain information about the infrastructure, terrain, or threat. This may include data on obstacles, gap crossing sites, airfields, bridges, tunnels, roads, and trails. Engineer units do not have designated reconnaissance teams. Engineer reconnaissance is directed and task-organized based on mission requirements using assets that would otherwise support other engineer missions. (See ATP 3-34.81.)
- *CBRN reconnaissance* includes missions to obtain information on suspected or confirmed CBRN threats and hazards in an assigned area. CBRN reconnaissance identifies indicators of enemy CBRN production or employment, and indicators related to civilian or industrial facilities that could be weaponized or produce hazards when damaged or destroyed. (See ATP 3-11.37.)
- *Civil reconnaissance* is a targeted, planned, and coordinated observation and evaluation of specific civil aspects of the environment such as areas, structures, capabilities, organizations, people, or events (JP 3-57). Civil reconnaissance verifies or refutes civil information, supports OE assessments, and detects and monitors changes in the civil component. It is conducted over time through routine engagements and patterned civil observations using active and passive sensors, virtual sensors, and other means. (See FM 3-57.)

Security Operations

8-56. The main difference between conducting security operations and reconnaissance is that security operations orient on the force or facility being protected while reconnaissance orients on the enemy and terrain. Security operations aim to protect a force from surprise and reduce the unknowns in any situation. Commanders conduct security operations to the front, flanks, or rear of their forces, which may be moving or stationary. Their goal is to determine the enemy's COA and assist the main body in defeating enemy forces. For security operations, economy of force is often considered during planning. The following are the four types of security operations:

- *Area security* is a type of security operation conducted to protect friendly forces, lines of communications, installation routes and actions within a specific area (FM 3-90). The security force may be protecting the civilian population, civil institutions, and civilian infrastructure within a unit's assigned area.
- *Cover* is a type of security operation done independent of the main body to protect them by fighting to gain time while preventing enemy ground observation of and direct fire against the main body (ADP 3-90). A force tasked to cover may do so offensively or defensively.
- *Guard* is a type of security operation done to protect the main body by fighting to gain time while preventing enemy ground observation of and direct fire against the main body (ADP 3-90). Units performing a guard cannot operate independently. They rely on fires and functional and multifunctional support assets of the main body. A force tasked to guard may do so offensively and defensively.
- *Screen* is a type of security operation that primarily provides early warning to the protected force (ADP 3-90). Screens provide less protection than guards or covers. Screen missions are defensive in nature and accomplished by establishing a series of observation posts and patrols to ensure observation of the assigned area. The screen force gains and maintains enemy contact consistent with the OPORD and destroys or repels enemy reconnaissance units by conducting counterreconnaissance.

8-57. Main body commanders designate the size of the security force and its mission. This designation determines the limit of the security forces' responsibilities to perform screen, guard, cover, and area security operations. Table 8-2 shows the typical sizes of security forces at various echelons in relation to their missions. The limited capabilities of most maneuver platoons prohibit them from having a mission separate from their parent company; scout platoons are the exception to this rule.

Table 8-2. Typical security force echelon for a given mission and echelon

Echelon	***Security mission***			
	Screen	Guard		Cover
		Advance	Flank or rear	
Echelons above corps (joint force land components or numbered Army)	CAB, armored BCT, Stryker BCT	Reinforced corps or division	CAB, armored BCT, or Stryker BCT	Reinforced corps or division
Corps	CAB, combined arms battalion, battalion task force	Division, armored BCT, Stryker BCT	Division, armored BCT, Stryker BCT, combined arms battalion, battalion task force	Reinforced division or armored BCT
Division	Cavalry squadron, combined arms battalion, or battalion task force	Reinforced cavalry squadron or BCT	Reinforced cavalry squadron, combined arms battalion, or battalion task force	Reinforced BCT
BCT	Company team	Battalion task force	Reinforced combined arms battalion, or battalion task force	
Battalion task force	Scout platoon			

BCT brigade combat team CAB combat aviation brigade

DEFENSIVE OPERATIONS (FRIENDLY)

8-58. Enemy commanders conducting offensive operations identify probable enemy objectives and possible enemy avenues of approach (AAs) to achieve them. The G-2/S-2 must understand enemy capabilities in all domains; this is critical to devising the most effective friendly defensive schemes. Identifying enemy limitations assists in determining opportunities to exploit friendly advantages. Enemy forces employ reconnaissance, EW, information warfare, and other capabilities during offensive operations. Figure 8-3 depicts a notional enemy offensive operation.

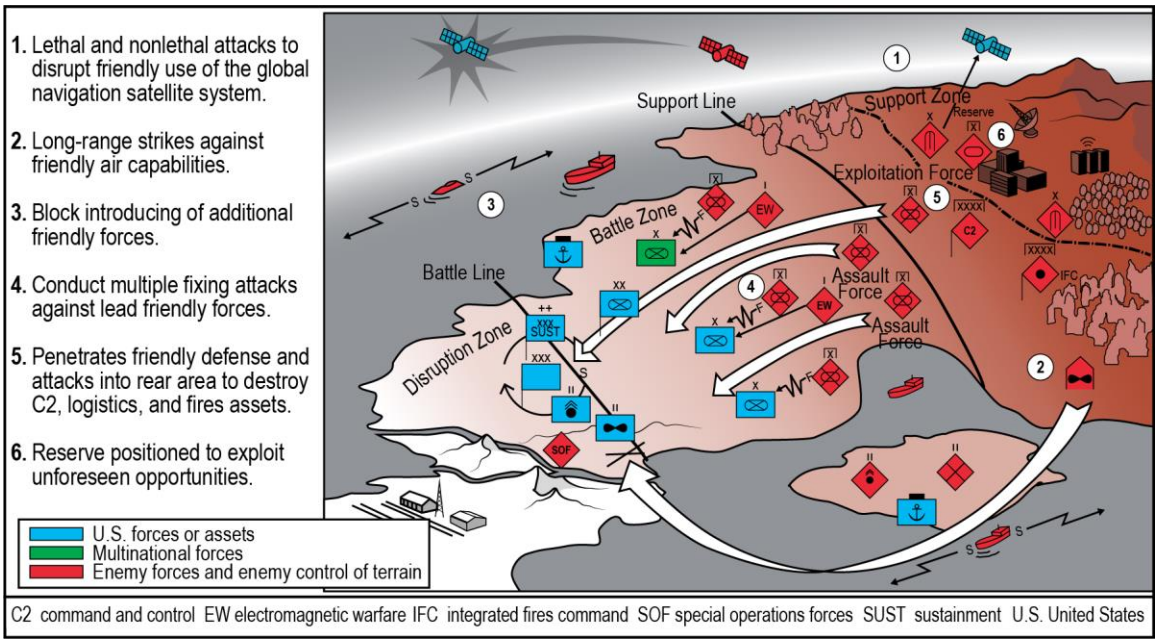


Figure 8-3. Notional enemy offensive operation

8-59. During friendly defensive operations, enemy forces employ precision fires, other long-range fires, and nonlethal capabilities (such as cyberspace and EW) to attack friendly C2 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. Successful defenses apply the following characteristics (see ADP 3-90):

- Disruption—deceiving or destroying enemy reconnaissance forces, breaking up combat formations, separating echelons, and impeding an enemy force's ability to synchronize its combined arms.
- Flexibility—developing plans that anticipate a range of enemy actions and allocate resources accordingly.
- Maneuver—achieving and exploiting a position of physical advantage over an enemy force.
- Mass and concentration—creating overwhelming combat power at specific locations to support the main effort.
- Depth—engaging multiple enemy echelons, enemy long-range fires, sustainment, and C2.
- Preparation—preparing the defense before attacking enemy forces arrive.
- Security—conducting security, protection, information activities, OPSEC, and cyberspace and EW tasks.

AREA DEFENSE

8-60. *Area defense* is a type of defensive operation that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright (ADP 3-90). Area defense can occur at the tactical and operational levels of warfare. The area defense focuses on retaining terrain where the bulk of a defending force positions itself in mutually supporting, prepared positions. Units maintain their positions and control the terrain between these positions. The operation focuses fires into engagement areas, possibly supplemented by a counterattack. Commanders can use their reserve to reinforce fires, add depth, block, or restore a position by counterattack; seize the initiative; and destroy enemy forces. Units at all echelons can conduct an area defense. (See FM 3-90 for the advantages and disadvantages of using a defense in depth and a forward defense during the conduct of an area defense.)

MOBILE DEFENSE

8-61. *Mobile defense* is a type of defensive operation that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force (ADP 3-90). Mobile defense is more often associated with the operational level of warfare. The mobile defense focuses on defeating or destroying an enemy by allowing enemy forces to advance to a point where they are exposed to a decisive counterattack by a *striking force*—a dedicated counterattack force in a mobile defense constituted with the bulk of available combat power (ADP 3-90). A *fixing force*—a force designated to supplement the striking force by preventing the enemy from moving from a specific area for a specific time (ADP 3-90)—supplements the striking force by holding attacking enemy forces in position to help channel attacking enemy forces into ambush areas and to retain areas from which to launch the striking force.

8-62. A mobile defense requires an AO with considerable depth. Commanders shape their battlefields, causing an enemy force to overextend its lines of communications, expose its flanks, and dissipate its combat power. Commanders move friendly forces around and behind an enemy force to cut off and destroy them. A division or higher echelon normally executes a mobile defense. BCTs and maneuver battalions participate in a mobile defense as part of a striking force or fixing force.

RETROGRADE

8-63. *Retrograde* is a type of defensive operation that involves organized movement away from the enemy (ADP 3-90). A retrograde can take place at the tactical or operational levels of warfare. An enemy may force these operations, or a commander may execute them voluntarily. The higher echelon commander of a force executing a retrograde must approve the retrograde before its initiation. A retrograde is a transitional operation. It is not conducted in isolation. It is always part of a larger scheme of maneuver designed to regain the initiative and defeat the enemy.

8-64. The following are the three forms of the retrograde:

- *Delay* is when a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on enemy forces without becoming decisively engaged (ADP 3-90). In delays, units yield ground to gain time while retaining flexibility and freedom of action to inflict the maximum damage on an enemy.
- *Withdraw* is to disengage from an enemy force and move in a direction away from the enemy (ADP 3-90). Withdrawing units, whether all or part of a committed force, voluntarily disengage from an enemy to preserve the force or release it for a new mission.
- *Retirement* is when a force out of contact moves away from the enemy (ADP 3-90).

8-65. In each form of retrograde, a force not in contact with an enemy moves to another location, normally by a tactical road march. In all retrograde operations, firm control of friendly maneuver elements is a prerequisite for success.

INTELLIGENCE SUPPORT TO DEFENSIVE OPERATIONS

8-66. Before a battle, commanders at all echelons require intelligence and combat information. IPOE and information requirements may include—

- The composition, equipment, intent, strengths, vulnerabilities, and scheme of maneuver of the attacking enemy force.
- The location, direction, and speed of enemy reconnaissance elements.
- The location and activities of enemy units and reserves.
- Enemy C2 and communications facilities.
- The location of enemy fire support and air defense systems with associated C2 networks.

8-67. The G-2 uses the operations process' prepare activity to complete information collection integration and synchronization. Corps and divisions rely on joint and national systems to detect and track targets beyond their limited organic capabilities. The corps headquarters employs available collection assets to refine its knowledge of the terrain, weather, and civil considerations within the area of influence. Collection assets identify friendly vulnerabilities and key defensible terrain. The division headquarters conducts periodic information collection of any unassigned areas to prevent the enemy from exploiting those areas to achieve surprise.

8-68. Commanders continuously refine the enemy portion of the COP throughout their AOIs as part of deep operations. They focus their information collection efforts on key geographical areas and enemy capabilities of particular concern using NAIs. Figure 8-4 depicts a situation template of enemy forces in an offensive operation; the friendly forces in figure 8-4 provide context.

8-69. Surveillance of the AOIs and effective reconnaissance are necessary to acquire targets and to verify and evaluate potential enemy COAs and capabilities. Information collection efforts focus on validating when, where, and with what strength the enemy will attack. This allows commanders to identify opportune times to conduct spoiling attacks and reposition forces.

8-70. Intelligence supports friendly force efforts to protect the force, disburse 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.

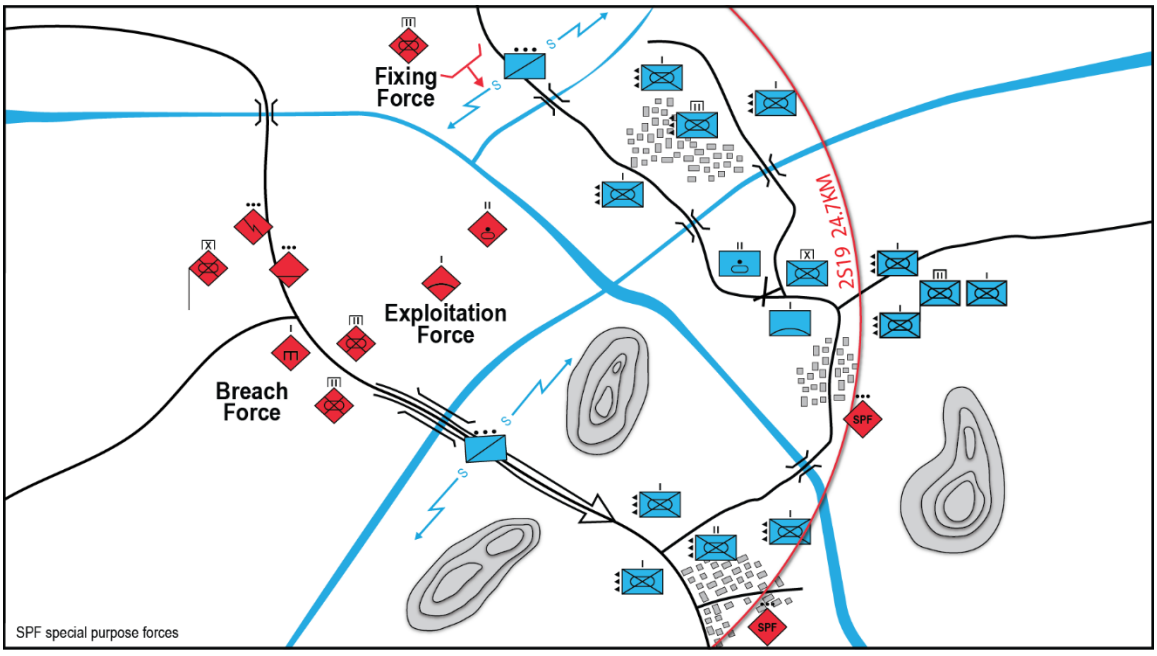


Figure 8-4. Situation template depicting enemy forces in the offense (example)

8-71. Table 8-3 depicts IPOE and information requirements generally associated with friendly defensive operations.

Table 8-3. IPOE and information requirements associated with defensive operations (friendly)

Determine the likely purpose (for example, terrain- or force-oriented) and type of enemy offense.
Determine the likely enemy end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy offensive operations: • Favorable ground corridors and air avenues of approach (including for the use of drone swarms and drone delivered munitions). • Areas with significant concealment and/or cover. • Terrain, including subterranean, that allows forces to bypass obstacles and friendly positions. (See ATP 3-21.51.) • Infiltration routes. • Landing zones (manned and unmanned aircraft systems). • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for friendly systems relative to enemy systems. • Favorable weather for the use of obscuration or chemical weapons.
Identify military aspects of terrain (OAKOC) and weather effects that support friendly defensive operations: • Terrain that allows friendly forces to tie obstacles to existing terrain features to supports friendly defensive positions. • Favorable air and ground avenues of approach for a counterattack. • Terrain that canalizes enemy attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems relative to friendly systems.
Identify the location of enemy assembly areas, ammunition and logistics nodes, forward aviation locations, and likely movement routes into the friendly area of operations.
Template and track the composition, disposition, likely routes, and time phase lines of reconnaissance and surveillance, security, advanced engineering, infiltrating, and air assault units (most include intelligence handover lines).
Template and track the composition, disposition, likely routes, and time phase lines of advance guard, main body, antitank, reserve, and second echelon units.
Template and track specific locations where the enemy will conduct key maneuver tasks, such as occupying support by fire positions and dismounting infantry, or where friendly units may be isolated in defensive positions due to enemy use of artillery scatterable mines.
Determine the likely use and template the location of enemy command and control nodes, long-range fires, artillery and rocket units, air defense systems, attack helicopter units, close air support, engineer units, CBRN units, electromagnetic warfare assets, and special operations forces.
Determine the likely use of enemy information warfare, cyberattacks, and denial and deception operations; likely impacts to friendly, threat, and neutral forces; and impacts of misinformation and disinformation on local, regional, and international audiences.
Determine the impact of significant civil considerations on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, criminal activity, and the housing and feeding of a displaced population.
ATP Army techniques publication CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

8-72. Table 8-4 depicts IPOE and information requirements generally associated with each of the three types of friendly defensive operations.

Table 8-4. IPOE and information requirements associated with each defensive operation type

Area defense
The intelligence staff leads the rest of the staff in identifying when, where, with what strength, and how the enemy will attack across domains and potentially engaging one or more dimensions. This allows the commander to identify opportune times to conduct spoiling attacks and reposition forces. The entire staff also identifies threats to support and rear areas, such as enemy special purpose forces and irregular activities, which may interfere with control of the defense. Besides the IPOE and information requirements identified in table 8-3, conducting area defense operations includes considering the following requirements: • Identify the location of natural lines of resistance, well-defined avenues of approach, intervisibility lines, cover and concealment, and other terrain features that support area defense. (See ATP 2-01.3.) • Determine whether the terrain better supports a forward defense or a defense in depth. • Consider cyberspace, space, information advantage activities, and EW capabilities that enable friendly defensive operations while also defending against those same threat capabilities.
Mobile defense
Besides IPOE and information requirements, conducting mobile defense operations includes considering the following requirements: • Likely locations where the threat can employ fire support coordination measures to turn or block friendly forces executing the mobile defense. • Likely locations where the enemy can expose its flanks and dissipate its combat power. • Likely times when and locations where the friendly commander can launch a spoiling attack. • Where and when friendly force combat power is greater than enemy force combat power. • Likely locations where the commander can employ striking and fixing forces based on the enemy's scheme of maneuver.

Table 8-4. IPOE and information requirements associated with each defensive operation type (*continued*)

Retrograde
The intelligence staff leads the rest of the staff in analyzing the terrain, including ground and air avenues of approach, to determine the best routes for both the friendly force retrograde and the likely enemy exploitation or pursuit operation. Besides IPOE and information requirements, conducting a retrograde operation includes considering the following requirements: • Identify possible routes friendly forces can use to conduct retrograde operations. • Identify possible hasty defensive positions in zone that facilitate attrition of the enemy. • Identify possible pursuit routes enemy forces may use. • Identify blocking points enemy forces may use to prevent the retrograde. • Determine how enemy forces can exploit friendly retrograde operations (consider local, regional, and international audiences).
ATP Army techniques publication IPOE intelligence preparation of the operational environment

OFFENSIVE OPERATIONS (FRIENDLY)

8-73. The enemy employs two types of defenses:

- A maneuver defense trades terrain for the opportunity to destroy portions of an opponent's formation and render the opponent's combat system ineffective.
- In an area defense, the enemy denies key areas to friendly forces.

8-74. In most situations against a peer or superior opponent, enemy forces are willing to surrender terrain to preserve their major combat forces since the loss of those forces threatens the survival of the enemy's state or regime. Figure 8-5 depicts a notional enemy maneuver defense.

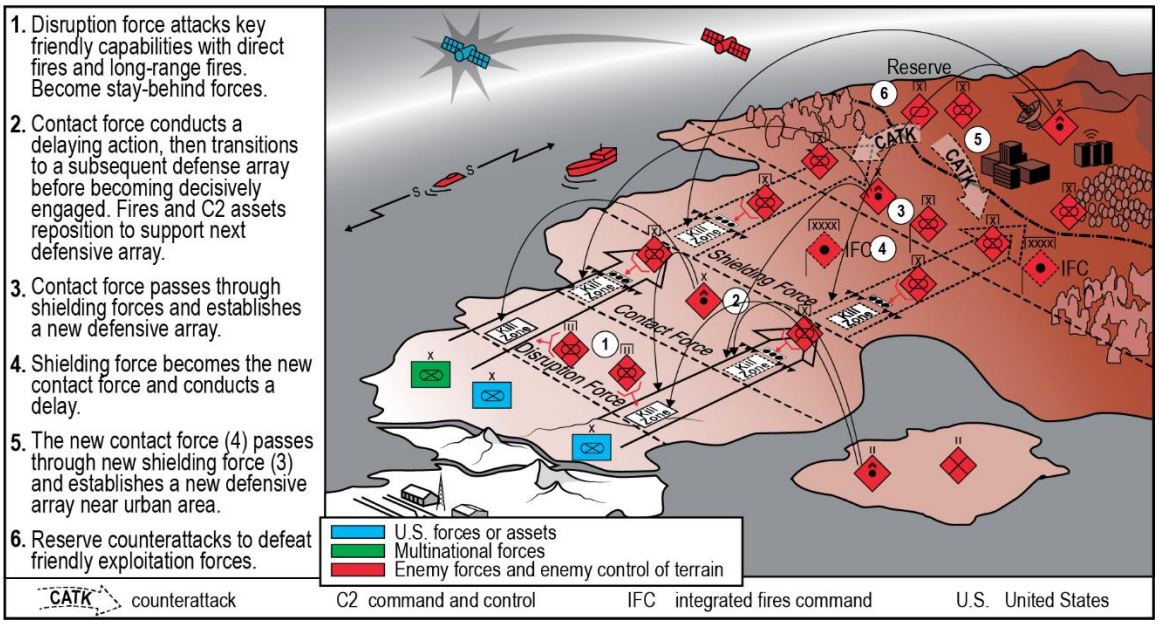


Figure 8-5. Notional enemy maneuver defense

8-75. During friendly offensive operations, enemy forces in the defense attempt to disrupt friendly activities by employing precision fires, other long-range fires, and nonlethal capabilities (like cyberspace 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 are movement to contact, attack, exploitation, and pursuit. Successful offenses apply the following characteristics (see ADP 3-90):

- Audacity—the ability to assume risk to create opportunity with bold action.
- Concentration—orchestrating forces or effects to create and exploit opportunity. (Concentrating effects is referred to as *mass*.)

- Surprise—taking action that catches enemy forces off guard.
- Tempo—maintaining a pace of operations that is faster than the enemy's but not so fast that it cannot be sustained for as long as necessary to achieve all assigned objectives.

MOVEMENT TO CONTACT

8-76. *Movement to contact* is a type of offensive operation designed to establish or regain contact to develop the situation (FM 3-90). Commanders conduct a movement to contact when an enemy situation is vague or not specific enough to conduct an attack. The goal of a movement to contact is to make initial contact with a small element while retaining enough combat power to develop the situation and mitigate the associated risk. A movement to contact employs purposeful and aggressive reconnaissance and security operations to gain contact with the enemy main body and develop the situation. The movement to contact force defeats enemy forces within its capability and creates favorable conditions for subsequent tactical actions. If the movement to contact force meets a superior force that it is unable to defeat, the movement to contact force conducts the security or defensive operations necessary to develop the situation further. A movement to contact may result in a meeting engagement. Once an enemy force makes contact, the friendly commander has five options: attack, defend, bypass, delay, or withdraw. Subordinate forms of a movement to contact include search and attack, and cordon and search operations.

ATTACK

8-77. An *attack* a type of offensive operation that defeats enemy forces, seizes terrain, or secures terrain (FM 3-90). Attacks incorporate coordinated movement supported by fires. A commander may describe an attack as hasty or deliberate, depending on the time available for assessing the situation, planning, and preparing. A commander may decide to conduct an attack using only fires (including EW, offensive cyberspace operations, and information advantage activities), based on an analysis of the mission variables. An attack differs from a movement to contact because in an attack, commanders know at least part of an enemy's dispositions. This knowledge enables commanders to better synchronize and more effectively employ combat power. Subordinate forms of the attack have special purposes. They include the tasks of ambush, counterattack, demonstration, feint, raid, and spoiling attack. The commander's intent and the mission variables determine which of these forms of attack to employ. Commanders conduct each of these forms of attack, except for a raid, as either a hasty or a deliberate operation.

EXPLOITATION

8-78. An *exploitation* is a type of offensive operation following a successful attack to disorganize the enemy in depth (FM 3-90). An exploitation seeks to disintegrate enemy forces, so they have no alternative but to surrender or retreat. Exploitations take advantage of tactical opportunities. Division and higher headquarters normally plan exploitations as a branch or sequel.

PURSUIT

8-79. A *pursuit* is a type of offensive operation to catch or cut off a disorganized hostile force attempting to escape, with the aim of destroying it (FM 3-90). A pursuit normally follows a successful exploitation. However, if enemy resistance breaks down and the enemy begins fleeing the battlefield, any offensive operation can transition into a pursuit. Pursuits entail rapid movement and decentralized control. Bold action and calculated initiative are required in the conduct of a pursuit.

INTELLIGENCE SUPPORT TO OFFENSIVE OPERATIONS (FRIENDLY)

8-80. The information collection effort assists commanders in deciding when and where to concentrate combat power. Collection assets answer the corps or division commander's intelligence requirements, which flow from IPOE and the war-gaming process. Important IPOE and information requirements may include—

- Enemy centers of gravity or decisive points.
- Location, orientation, and strength of enemy defenses.
- Location of enemy reserves, fire support, and other attack assets to support defensive positions.

- Enemy air AAs and likely enemy engagement areas.
- Key terrain, AAs, and obstacles.

8-81. The G-2 identifies threats to corps and division support and rear areas, such as enemy special purpose forces, enemy bypassed conventional forces, and irregular activities that may interfere with corps or division support and rear activities.

8-82. The G-2 integrates and synchronizes unified action partner capabilities into the collection effort. The G-2 recommends specific reconnaissance tasks for corps- or division-controlled reconnaissance forces, realizing the commander may task these forces to conduct offensive operations or other tactical enabling tasks. A focused approach to allocating collection assets maximizes the capability of the limited number of assets available to corps or divisions.

8-83. The G-3 synchronizes information collection operations with combat operations to ensure all corps and division information collection provides timely information to support operations. The G-3 tasks collection assets to support the targeting process. Collection assets locate targets identified in the AGM and call for fires. The fires cell may engage targets to achieve lethal and nonlethal effects.

8-84. MI units and systems conduct intelligence operations to locate enemy units and systems. SIGINT and EW systems usually operate with the covering force and flank guard. The covering force commander directs EW against enemy C2 and fire support networks. The commander may use electromagnetic deception to deceive the enemy as to the location of the main body. Space-based and cyberspace systems and activities also support the security force in locating and determining the presence of enemy disruption forces, contact forces, and shielding forces.

8-85. Intelligence identifies when and where the enemy will concentrate combat power, find gaps and vulnerabilities in enemy defenses, and predict how the enemy will conduct counterattacks and other tactics across the domains and dimensions. 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. Figure 8-6 depicts a threat template of enemy forces in the defense.

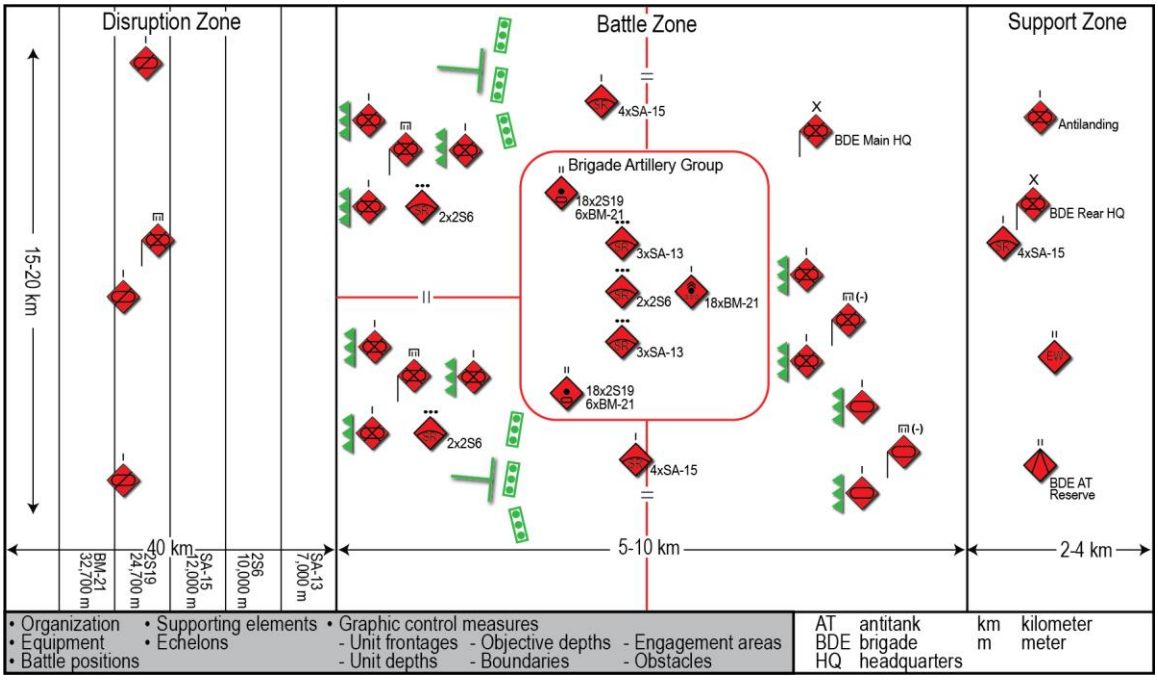


Figure 8-6. Threat template of enemy forces in the defense (example)

8-86. Table 8-5 depicts IPOE and information requirements generally associated with friendly offensive operations.

Table 8-5. IPOE and information requirements associated with offensive operations (friendly)

Determine the likely purpose and type of enemy defense: area defense, mobile defense, or retrograde.
Determine the likely enemy's likely end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver. Synchronize efforts to gain and maintain relative advantages and maintain tempo.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy defensive operations: • Terrain that allows reconnaissance and security outposts to be arranged in depth along choke points and terrain features that canalize friendly forces to attrite our forces and diminish our combat power in depth. • Terrain, including subterranean, that allows the enemy to tie obstacles to existing terrain features to support enemy defensive positions. (See ATP 3-21.51.) • Favorable air and ground avenues of approach for an enemy counterattack (including for the use of drone swarms and drone delivered munitions). • Terrain that canalizes friendly attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems relative to friendly systems.
Identify terrain military aspects of terrain (OAKOC) and weather effects that support friendly offensive operations: • Favorable ground and air mobility corridors. • Areas with significant concealment and/or cover. • Terrain that allows forces to bypass obstacles and enemy positions. • Infiltration routes. • Landing zones (manned and unmanned aircraft systems). • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for friendly systems relative to enemy systems, and favorable weather for using obscuration or chemical weapons.
Identify the location and orientation of enemy counterreconnaissance and security units, obstacles, engagement areas, main battle areas, reserve units, and likely counterattack routes (most incorporate intelligence handover lines).
Within each enemy defensive area, identify specific primary, secondary, tertiary locations of enemy infantry, armor, antitank, mortar, and other units and systems, and the potential use of camouflage.
Determine the likely use and identify the location of enemy command and control nodes, reconnaissance and surveillance assets, long-range fires, artillery and rocket units, air defense systems, rotary aviation units, close air support, engineer units, ammunition and logistics nodes, CBRN units, electromagnetic warfare assets, and special operations forces.
Determine the likely use of enemy information warfare, cyberattacks, and denial and deception operations; likely impacts to friendly, threat, and neutral forces; and impacts of misinformation and disinformation on local, regional, and international audiences.
Determine the impact of significant civil considerations on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, criminal activity, and the housing and feeding of a displaced population.
ATP Army techniques publication CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

8-87. Table 8-6 depicts IPOE and information requirements generally associated with each of the four types of friendly offensive operations.

Table 8-6. IPOE and information requirements associated with each offensive operation type

Movement to contact	
A thorough IPOE 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. Besides the IPOE and information requirements identified in table 8-5, movement to contact includes considering the following requirements:	
• Intent and likely locations for enemy reconnaissance and security forces. • Likely observation post locations. • Likely enemy defensive locations with close obstacles and engagement areas. • Likely enemy activities in friendly rear areas.	• Likely enemy use of a feint or deception. • Indications that the enemy is still conducting movement. This could turn the operation into a meeting engagement or cause friendly forces to employ a hasty defense. • Likely electromagnetic warfare, cyberspace, and space targets as well as the type and disposition of sensors in each domain.
Attack	
Besides IPOE and information requirements, attack includes considering the following requirements: • Known and likely enemy defensive locations with likely purpose and use of close obstacles and engagement areas. • Known and likely enemy command and control and communications nodes and systems. • Known and likely electromagnetic warfare, cyberspace, and space targets.	
Exploitation	
Besides IPOE and information requirements, exploitation includes considering the following requirements: • Likely locations where friendly forces can interdict enemy reinforcements or second echelon forces through fires and subsequent operations. • Enemy reserve or second echelon and logistic units. • Enemy long-range artillery, missile systems, and associated fires units.	

Table 8-6. IPOE and information requirements associated with each offensive operation type (*continued*)

Pursuit
Any rapid decision making to support a pursuit uses IPOE planning and products from the original offensive operation and the appropriate branch or sequel planning. Besides IPOE and information requirements, pursuit includes considering the following requirements: • Identify ground and air avenues of approach to determine the best routes for retreating enemy forces. • Identify locations that second echelon enemy forces may reinforce retreating enemy forces.
IPOE intelligence preparation of the operational environment

SECTION IV – INTELLIGENCE SUPPORT: DEVELOPING THE SITUATION

Note. This section focuses on tactical intelligence support during a large-scale combat operation from completion of RSOI through a series of tactical engagements. The discussion assumes familiarity with the doctrinal content in chapters 1 through 7 and sections I through III of this chapter.

8-88. From RSOI to the first engagement (often in the form of close combat), the commander and staff may largely focus on countering threat capabilities, preserving combat power, and protecting friendly units as friendly forces set conditions for the first engagement—preferably from a position of relative advantage. Friendly forces are under continuous threat observation and contact, and the threat has several means to disrupt and desynchronize friendly operations. Theater army and corps collection assets are likely in contact with enemy forces. These echelons provide intelligence support to tactical echelons throughout deployment and the completion of RSOI. However, tactical echelons should not assume they will receive perfect intelligence support; it is important for them to quickly gain and maintain contact, in terms of information collection, with the enemy. Gaining contact is each echelon's first step in developing the situation to strive for situational understanding and attempt to find a position of relative advantage.

8-89. Key aspects of developing the situation within the intelligence warfighting function include the following:

- Effective staff integration.
- Effective intelligence requires the extension of the intelligence architecture to tactical units as they move and prepare for their first engagement.
- A thorough understanding of threat TTP, capabilities, vulnerabilities, and limitations is crucial.
- An understanding of time and space and their relationship to the employment of friendly and threat capabilities.
- A thoroughly developed and flexible information collection plan.
- 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, phased, continuous, and aggressive information collection plan.

8-90. During this period, tactical echelons may potentially face a high tempo, many unit movements, and the need to conduct planning within a relatively short time. They may resort to using the RDSP and overlay orders or a series of FRAGORDs with a plan for multiple branches and sequels, depending on the tempo. The commander indicates when, in what format, and the focus of the different staff products; it is vital for tactical echelons to remain focused on meeting the commander's needs.

8-91. When facing these pressures, it is crucial to apply operational and intelligence doctrinal fundamentals to execute the operations process. Although there are means of abbreviating the different intelligence processes and tasks, intelligence personnel must ensure they conduct each step of these processes and tasks—even if abbreviated. Staff collaboration and integration, accounting for the mission variables, and thoughtful war-gaming are more important than producing every operational and intelligence product to the highest standard.

8-92. The entire intelligence process applies in providing tactical intelligence support during a large-scale combat operation; however, the rest of this section focuses on three important aspects of tactical intelligence: thoroughly integrated planning, intelligence synchronization and effective information collection, and producing focused and tailored intelligence. (See figure 8-7 on page 8-24.)

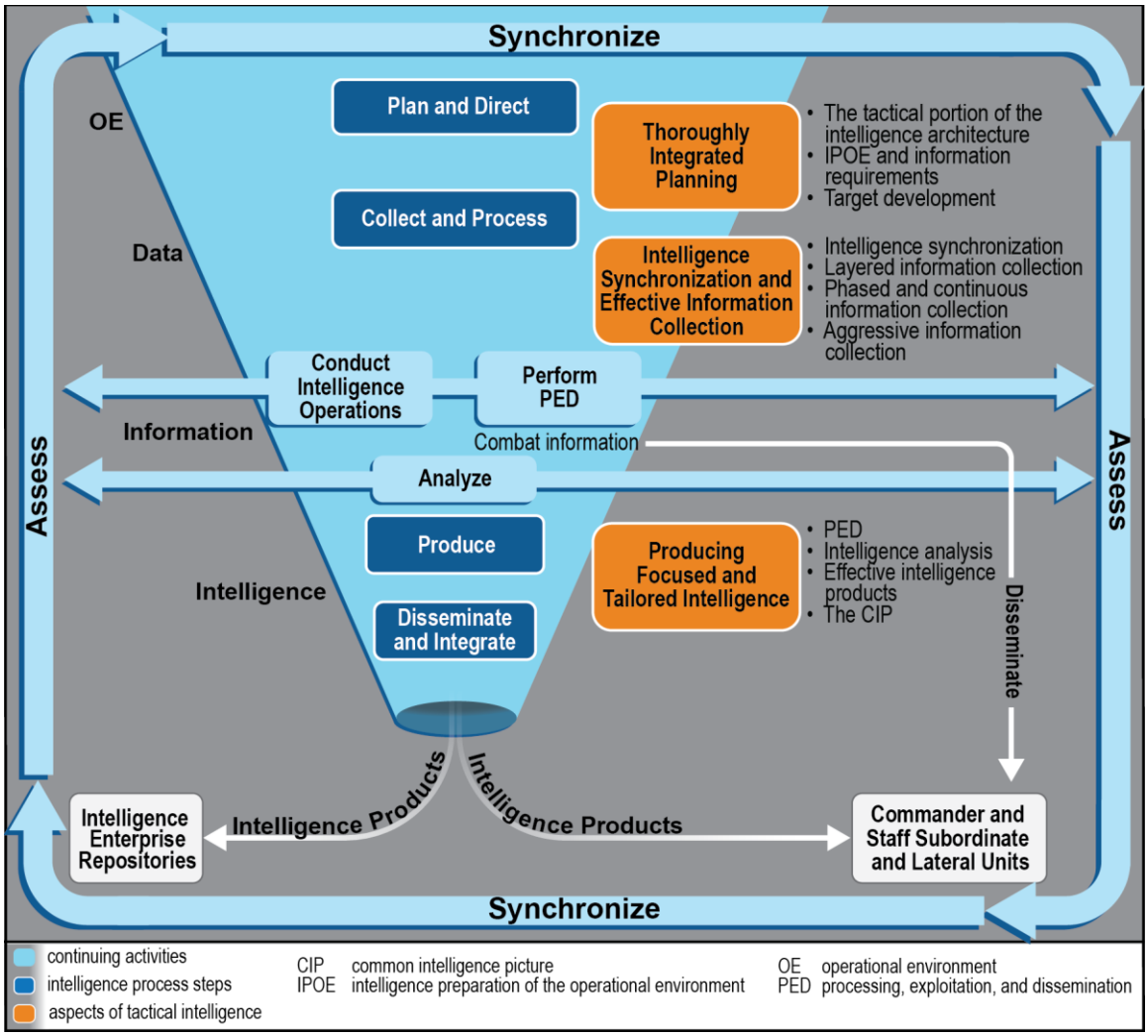


Figure 8-7. Key aspects of tactical intelligence

THOROUGHLY INTEGRATED PLANNING

8-93. As much as possible, planning before deployment and at higher echelons reduces the pressure imposed on tactical units about to move to their first engagement. For the intelligence warfighting function, IPOE and participation in the MDMP are important, but there is more to intelligence planning than IPOE. Staff teamwork and collaboration are critical to intelligence planning, especially during this difficult phase of operations. Thoroughly integrated planning focuses on—

- The tactical portion of the intelligence architecture.
- IPOE and information requirements.
- Target development.

TACTICAL PORTION OF THE INTELLIGENCE ARCHITECTURE

8-94. Conditions from RSOI through close combat degrade a Soldiers' and units' abilities to revise the existing intelligence architecture and extend the tactical portion of the architecture. The lethal, fluid, and chaotic nature of combat causes the greatest stress on the intelligence architecture. This level of stress cannot be replicated in training environments, CP exercises, or field training exercises; therefore, leaders and Soldiers must exercise flexibility, adaptability, and creativity to establish and revise the intelligence architecture during operations. These traits must be reflected in tactical intelligence architectures.

8-95. Frequent CP movements with short halts challenge units' abilities to reestablish the intelligence architecture. Integrating new personnel—for example, when personnel arrive as replacements for lost or undeployable personnel—can challenge. These personnel may require unit-oriented training or specified network certifications not previously received, and they must quickly familiarize themselves with local SOPs.

8-96. Adverse weather and terrain conditions in the AO can negatively affect Soldiers' and units' abilities to establish and revise an intelligence architecture. Weather, such as extreme temperatures (hot and cold), extreme winds, and dust can adversely affect equipment performance and impede Soldiers' abilities to perform intelligence architecture related tasks in exposed conditions. Restrictive terrain can also adversely affect the intelligence architecture. For example, line-of-sight communications blocked by intervening terrain or limited space available for locating a CP may force units to locate intelligence systems in inconvenient locations.

8-97. Enemy and threat actions against U.S. and multinational partner communications can threaten and adversely affect intelligence architecture operations. Spare parts and replacement systems may not be available to maintain components or replace damaged or destroyed physical components of the intelligence architecture. Enemy cyberspace attacks and EAs can also degrade the intelligence architecture.

8-98. These conditions and situations that can occur during operations are not all-inclusive. When planning the intelligence architecture during ongoing operations, the G-2/S-2 and intelligence staff must consider these factors as well as—

- Developing, managing, and revising the intelligence architecture as mission requirements change.
- The survivability and resiliency of systems and networks.
- The redundancy of systems and networks.
- Contingencies and PACE planning in the event of the physical destruction of systems and networks.
- DDIL communications environments.

8-99. Planning as well as practiced unit drills can anticipate the integration of new units once in theater. Contested communications environments require active, aggressive communications security measures and activities. Flexible, adaptive, and creative thinking and actions can mitigate many of the challenges and risks to intelligence architectures. For example—

- Creatively using systems to reroute data and information can overcome transport obstacles and challenges in a DDIL communications environment.
- Prioritizing and tailoring data and information to the right point at the right time can ease transport congestion.
- Ensuring noncommissioned officers are trained as trainers and have effective, practiced training plans can assist in integrating new Soldiers, especially once the unit is deployed in theater.

Note. The G-2/S-2 must articulate how the intelligence architecture supports the commander's objectives and desired end state. Successful tactical operations depend on the commander's understanding of the intelligence warfighting function (including the intelligence architecture) and integration of intelligence into operations.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT AND INFORMATION REQUIREMENTS

8-100. For the commander and staff, IPOE is critical to understanding the OE and setting the conditions for successful operations. Pre-mission analysis of the OE facilitates effective IPOE. During the MDMP, the intelligence staff leads IPOE and conducts continuous intelligence analysis to understand the OE and the options it presents to friendly and threat capabilities. For example, threat databases and signatures developed during pre-mission analysis of the OE assist in assessing threat capabilities and vulnerabilities during IPOE. This information facilitates operational planning during the MDMP and provides a common understanding of the OE.

8-101. Developing detailed and effective threat characteristics, threat models, and joint TSA and other target development products during competition and crisis allows tactical units to quickly start effective IPOE as early as RSOI. Early IPOE is crucial because the commander and staff must quickly gain a significant amount of knowledge focused to the mission variables (which account for all domains and dimensions). At this stage in operations, IPOE assists the commander and staff in identifying significant aspects of the OE within the AO and AOI and in developing indicators of threat activities, intentions, and objectives. The need to continuously update key intelligence products cannot be overstated through the analytical continuum of pre-mission analysis of the OE, IPOE, and situation development. While IPOE is critical, it may be necessary to conduct an abbreviated IPOE, still accounting for all four steps, through cross-staff collaboration, which is critical to operations. The situational understanding provided by accurate and timely IPOE products permits commanders and units to maintain a high tempo and execute the RDSP, when necessary, to achieve freedom of action and identify and exploit relative advantages across one or more domains and dimensions. (See ATP 2-01.3 for IPOE doctrine.)

8-102. The entire staff considers gaps in intelligence during the MDMP to develop often detailed information requirements, which in turn can go forward as potential intelligence requirements. However, these generic requirements lack the specifics of a particular tactical situation. Full consideration of every aspect of a tactical situation is necessary to develop information and intelligence requirements during operations. Intelligence and information collection are driven by the commander's intelligence requirements. The intelligence warfighting function must be very focused on intelligence requirements during large-scale combat operations. Together, IPOE and intelligence requirements drive information collection, subsequent intelligence analysis, and targeting.

TARGET DEVELOPMENT

8-103. Target development in a tactical situation requires continuous collaboration between all staff sections, but, at a minimum, it must include the targeting team, operations staff, CEMA cell, and the intelligence staff. Effective targeting is supported by accurate situational understanding. Without accurate situational understanding and detailed IPOE, effective targeting is unlikely.

8-104. The analysis associated with target development includes analyzing threat systems, unless this analysis already exists. Additionally, target development also includes deconfliction, aim point recommendations, target materials production, and collateral damage estimation. Target development generally results in products such as target intelligence folders, information collection requirements, and target briefs. Detailed analysis should characterize the function, criticality, and vulnerabilities of each target, linking them back to targeting objectives and measures of effectiveness. Target development includes target vetting and target validation. (See FM 3-60.)

8-105. The intelligence section must account for adequately supporting targeting, to include BDAs across multiple CPs. Accomplishing this at a high tempo against a peer threat is difficult. The D3A targeting methodology must consider—

- Threat deception, camouflage, cover, and dispersion.
- Threat counterreconnaissance and EW capabilities.
- Threat counterfire capabilities.
- Any issues, damages, destruction, or delays based on the deployment of fire support capabilities.
- Friendly fire support planning, including logistics; movement following RSOI; and displace and emplace requirements following fire missions.

INTELLIGENCE SYNCHRONIZATION AND EFFECTIVE INFORMATION COLLECTION

8-106. Thoroughly integrated planning occurs as several important aspects of intelligence synchronization occur. Tactical units must transition from depending on higher echelons for information collection and leveraging the intelligence enterprise for their intelligence to fully employing their intelligence warfighting function and conducting information collection. Intelligence synchronization ensures intelligence analysis and PED are enabled for operations, to include using intelligence analysis systems, reestablishing communications and access to intelligence databases, and optimizing the tactical portion of the intelligence architecture.

INTELLIGENCE SYNCHRONIZATION

8-107. Synchronizing adjustments to the intelligence architecture, information collection, PED, intelligence analysis, and the dissemination and integration of intelligence products is integral to develop the situation and reach situational understanding. The G-2/S-2 and intelligence staff, in cooperation with the MI unit commander and staff, synchronize intelligence, ensuring the intelligence process is effective and intelligence support to operations and targeting are effective and flexible. Intelligence synchronization requires an effective relationship with the commander and staff, especially the G-3/S-3, as well as cooperation across echelons and with lateral units. Critical aspects of intelligence synchronization include but are not limited to—

- Early and continuous teamwork with the commander and across the staff. A collaborative environment is required to quickly solve complex intelligence warfighting function issues.
- Intelligence support to future plans with detailed transitions between operations.
- Developing a flexible scheme of intelligence (paragraph 3d of an OPLAN or OPORD). (See FM 5-0.)
- Ensuring intelligence operations are flexible enough to support rapid planning, responsive targeting, branches and sequels, and contingencies.
- Balancing the ability to leverage the intelligence enterprise and submitting RFIs and other requests with tactical information collection, PED, and intelligence analysis.
- Ensuring technical oversight and mission management effectively support information collection.
- Ensuring analysis supports focused and tailored intelligence products that facilitate situational understanding.

8-108. During planning, the G-2/S-2 determines how the intelligence warfighting function can best meet the commander's intent and achieve the desired end state. Intelligence analysis and support are built on successful information collection. An effective information collection effort is key to achieving and exploiting positions of relative advantage. Once organic, attached, assigned, and supporting information collection assets start information collection, the intelligence staff can better provide products, updates, and predictive assessments that support decision making, targeting, and the execution of branches and/or sequels. Intelligence synchronization, staff integration, operational planning, and information collection overlap significantly.

8-109. One example of this overlap occurs in collection management's execution management function, discussed in ATP 2-01. Personnel conducting execution management must—

- Understand the intricacies and details of the information collection plan (Annex L [Information Collection]).
- Constantly coordinate with mission management and ongoing PED and analysis.
- Track the progress of the ongoing operation, focusing on how the situation changes and emerging operational requirements.
- Assess the information collection plan and ensure it remains synchronized with various aspects of the operation, such as movements, objectives, schemes of maneuver, key logistical actions, TAIs, and engagement areas. When possible, this function is performed in conjunction with refining IPOE products and running estimates and providing feedback to collectors.
- Assist the COIC in making necessary adjustments to the information collection plan and retasking and in maintaining continuous control of collection execution.

EFFECTIVE INFORMATION COLLECTION

8-110. An effective information collection effort provides better opportunities for detecting enemy formations, fires capabilities, and critical specialized capabilities that pose the greatest threat to friendly forces. Effective information collection must occur across echelons through detailed synchronization and various means to achieve a layered, phased, and continuous approach. This approach supports the four tenets of operations: agility, convergence, endurance, and depth. The information collection plan must be simple enough to execute, should avoid being predictable to enemy forces, and should include adequate OPSEC measures to protect friendly operations.

8-111. When the commander and staff start planning information collection, many aspects of and limitations to that effort have been established based on operational constraints, the intelligence architecture, and the C2 network. While units can change some aspects of the intelligence architecture in a short timeframe, most components have been established or require a long lead time to change. Other staff activities and considerations that affect information collection include—

- Risk management.
- The air tasking order cycle.
- The targeting process, to include targeting boards and working groups, time permitting.
- Collection management boards and/or working groups or information collection working groups, when formed.
- Terrain management.
- Security operations missions.
- Counterreconnaissance.
- A reconnaissance-push or reconnaissance-pull approach. (See FM 3-98.)
- Communications, to include using retrains capabilities, when necessary.
- Fire support.
- Engineering support.
- Sustainment and IEW maintenance.
- Casualty evacuation.

Note. TC 2-19.01, developed for MI companies and platoons, includes appendixes applicable to other tactical units and information collection assets operating within a division or BCT AO. These appendixes include fire considerations, movement and maneuver, obstacle considerations, reaction drills, sustainment procedures, IEW maintenance, casualty response, CBRN considerations, cover and concealment, reporting, communications, and SOP considerations.

Layered Information Collection

8-112. In the offense or defense, units attack or defend in depth. Effective information collection planning depends on collaboration across the echelons vertically and horizontally to adjacent units. No echelon can operate on its own; there are interdependencies at each echelon. A layered information collection effort occurs based on this collaboration and dependency across echelons. However, each commander drives its own intelligence warfighting function.

8-113. Collaboration can occur in conjunction with orders and tasking or through informal collaboration. Collaboration can work both top-down—from theater army through each successive echelon—and bottom-up—from lower to higher echelons. This layering takes advantage of the various collection capabilities, the proximity of tactical echelons to the enemy, and other factors. Information collection layering is not easy, even between U.S. forces; this level of collaboration is very challenging with multinational elements, especially when operating on different networks such as CENTRIXS and US BICES. However, the challenge can be mitigated through close liaison.

8-114. Commanders, G-2/S-2s, and other staffs collaborate through several means, including video teleconference meetings, to create a common understanding of the enemy and to ensure the information collection plan addresses changes in the situation. The collection emphasis message is used between echelons to share important aspects of information collection and collection transitions before staffs can complete the entire information collection plan. Intelligence handover lines are also useful in collaborating between echelons and with adjacent units when the timely tracking of a specific enemy force is necessary.

8-115. In many situations, commanders and staffs can use intelligence handover lines to focus collection on HPTs. *Intelligence handover* refers to the transfer of information collection and intelligence analysis on an enemy force or capability between two echelons or units. The purpose is to maintain continuous contact with an enemy force or capability and gain an understanding of that force or capability in relation to the terrain and current situation. Intelligence handover occurs as a graphic control measure known as an intelligence handover line; however, a unit can use another type of control measure.

8-116. During intelligence handover, the initial unit (the unit first making contact) and the gaining unit share responsibility until the handover is complete or the mission is changed. When possible, the collection management team at the initial unit includes the intelligence handover line with specific details (such as handover guidance and operational and technical parameters as part of coordinating instructions) within Annex L (Information Collection) and shares the annex with the gaining and adjacent units. If the intelligence handover line is developed and coordinated during ongoing operations and Annex L (Information Collection) is not updated, the initial unit must share intelligence handover specific details in a collection emphasis message, or other means, especially when the intelligence handover involves ground reconnaissance.

8-117. When establishing intelligence handover lines, units can use existing graphic control measures. For example, the fire support coordination line (also called FSCL) can be used as an intelligence handover line between corps and divisions and the coordinated fire line between divisions and subordinate units. Using this practice simplifies intelligence handovers and is also effective in linking sensors to shooters. It also enables divisions to thoroughly nest their priorities with corps' priorities. Using an intelligence handover line also prevents redundancy of collection efforts while maintaining continuity of intelligence operations. However, there is utility for units to collect beyond the fire support coordination line as this can assist them in shaping future engagements. For example, information collection beyond the fire support coordination line may be necessary to plan for and employ capabilities to achieve favorable force ratios before the division engages enemy forces.

Information Collection Collaboration Examples

The corps G-2 anticipates that an enemy unit designated as an HPT will cross a key phase line in the next 24 to 48 hours. The predicted movement of the HPT causes the corps G-3 and G-2 to coordinate with the division G-3 and G-2 to ensure continuous tracking of the HPT with no loss of coverage. During the intelligence synchronization meeting, the corps G-2 and the division G-2 coordinate an intelligence handover line to ensure continuous coverage of the HPT. Another information collection technique is coordinating for complementary or supporting coverage. For example, the theater army conducts UAS collection for the corps while the HPT moves to an intelligence handover line where the corps then tracks the HPT to a deep engagement area and conducts BDA.

Phased and Continuous Information Collection

8-118. A phased and continuous information collection effort accounts for all phases of an operation as well as continued collection into a branch, sequel, or next operation. Different information collection tasks occur to support a specific phase or phases. The collection management and information collection plans are developed as part of the MDMP or RDSP. These planning processes drive the way a unit starts collection management and then phases into information collection.

8-119. As the MDMP or RDSP begins, there should already be ongoing information collection unless it is the unit's first operation in the AO. Additionally, joint forces should already be conducting ISR, and higher-level Army echelons should already be conducting information collection. When possible, every unit should plan collection to completion; by anticipating future conditions, the unit should plan collection into a transition that starts the next operation.

8-120. Based on the situation and the effectiveness or ineffectiveness of ongoing collection, the commander and staff have multiple opportunities to start information collection, including collection before completion of the MDMP. Starting information collection early in planning requires the commander's participation, hasty staff analysis, and early anticipation of requirements.

8-121. Current Army doctrine, including FM 3-55, identifies multiple places to revise ongoing collection, initiate the movement of collection assets, and/or start information collection before completion of the MDMP:

- At the conclusion of step 1 (receipt of mission), the staff provides a WARNORD, mostly designed to provide key guidance to subordinate and supporting units. The WARNORD includes initial information collection tasks, which can be challenging due to time constraints, especially those imposed during large-scale ground combat operations. This chapter builds on that discussion and introduces the optional use of the WARNORD to revise ongoing collection, initiate the movement of collection assets in preparation for future operations, and/or task assets to conduct limited preliminary information collection.
- At the conclusion of step 2 (mission analysis), the initial information collection plan is tasked to some collection assets through Annex L (Information Collection) in a WARNORD, FRAGORD, or OPORD. The initial information collection plan is different from the information collection plan at the end of the MDMP. Initial information collection is designed to answer the information gaps necessary to complete planning. ATP 2-01 reinforces this distinction and refers to the initial information collection plan in key places as the initial (planning-focused) information collection plan for emphasis.
- At the conclusion of step 6 (COA approval), the staff provides a WARNORD mostly designed to provide key information to subordinate units so they can refine their plans; it also confirms and elaborates guidance. The WARNORD includes principal tasks assigned to subordinate units. ATP 5-0.2-1 mentions adding any annexes already created before publishing the order. This chapter discusses the optional use of the WARNORD to revise ongoing collection or initiate the movement and/or tasking of collection assets to start information collection before publishing the OPORD.
- In step 7 (orders production, dissemination, and transition), the staff produces and disseminates the order, including the information collection plan as captured in Annex L (Information Collection). Information collection (which is separate and distinct from initial information collection) is designed to support the execution of operations to completion and into a transition period to collect information for the next operation. ATP 2-01 refers to the information collection plan in key places as the information collection plan (execution-focused) for emphasis.

Note. Planning early information collection is difficult. After completing steps 1 and 2 of the MDMP, the commander and staff have not created friendly COAs, compared those COAs, or chosen a COA. Throughout these steps, planning occurs that results in the development of many important operation details (such as decision points, concepts of operations, schemes of maneuver, TAIs and engagement areas, HPTs, and operational and fire control measures).

8-122. Realistically, the unit can attach Annex L (Information Collection) as part of a WARNORD, FRAGORD, or OPORD at any point, as needed, throughout the MDMP to start early information collection and/or revise ongoing information collection. Alternatively, if there are no critical planning gaps, the unit can decide to wait until publishing Annex L (Information Collection) as part of the order, in step 7, to begin most information collection. When deciding on whether and how much early information collection to conduct, the commander and staff should consider—

- Protecting the force.
- Supporting counterreconnaissance.
- Filling information gaps to successfully complete planning.
- The effectiveness or ineffectiveness of ongoing joint ISR and higher-echelon information collection.
- The effectiveness or ineffectiveness of ongoing (transitional) unit information collection.
- Risks to collection assets based on threat capabilities.
- The amount of time required to complete the MDMP.
- The amount of time necessary for collection assets to plan and prepare for executing collection.
- The risk of ineffectively tasking collection assets during preliminary or initial information collection, and then not being able to retask the assets in time to support executing operations.
- Using a reconnaissance-push or reconnaissance-pull approach.

Reconnaissance-Push and Reconnaissance-Pull

Reconnaissance-push is reconnaissance that refines the common operational picture, enabling the commander to finalize the plan and support main and supporting efforts (FM 3-90). The commander and staff use reconnaissance-push when they have a relatively thorough understanding of the OE. In these situations, commanders *push* reconnaissance assets into specific portions of their AOs to confirm, deny, and validate planning assumptions affecting operations. Reconnaissance-push emphasizes detailed, well-rehearsed planning.

Reconnaissance-pull is reconnaissance that determines which routes are suitable for maneuver, where the enemy is strong and weak, and where gaps exist, thus pulling the main body toward and along the path of least resistance (FM 3-90). Commanders use reconnaissance-pull when they are uncertain of enemy force compositions and dispositions in their AOs, information concerning terrain is vague, and time is limited. In these situations, reconnaissance assets initially work over broad areas to develop the enemy situation. As they gain an understanding of enemy vulnerabilities, these assets then *pull* the main body to positions of tactical advantage.

Aggressive Information Collection

8-123. Depending on the situation and threat capabilities, information collection at certain depths or against certain threat capabilities may not seem possible. Friendly forces may have to aggressively plan and execute information collection to overcome collection gaps. Overcoming these gaps is not only the collection manager and collection management team's responsibility; the commander, G-2/S-2, G-3/S-3, and other key staff members must take ownership of information collection. Commanders and staffs can attempt several approaches, such as the following, to overcome collection limitations and ensure or surge information collection during critical phases of an operation:

- Allocate maneuver, fires, and other capabilities to conduct combat operations to enable information collection. For example, the corps commander and staff can coordinate for the joint suppression of enemy air defenses during a critical phase of an operation to open a window of opportunity that allows aerial collection against the threat.
- Embed certain longer-range information collection capabilities in cavalry units or an advanced force operating further across the forward edge of the battle area.
- Employ certain special intelligence capabilities when a unit has deployed with those capabilities.
- Coordinate for specific special operations forces information collection, when possible.
- Leverage national technical means as a method to tip, cue, and/or validate IPOE and other intelligence products.
- Prearrange for specific joint ISR support tailored to Army tactical requirements, when possible.
- Coordinate for the use of multinational partner collection platforms in an integrated approach. Commanders and staffs should not overlook the valuable and sometimes unique collection capabilities of multinational partners.

PRODUCING FOCUSED AND TAILORED INTELLIGENCE

8-124. The commander drives intelligence, and the G-2/S-2 synchronizes intelligence closely through the transition to conducing tactical intelligence operations. This transition is complex and includes extending the tactical portion of the intelligence architecture, conducting thorough planning, and starting information collection. Consequently, the unit starts to produce focused and tailored intelligence. Depending on the tempo and the commander's guidance, planning may become abbreviated, and the unit may operate on overlay orders with emphasis on centralized planning and decentralized execution, allowing tactical flexibility. No matter how the unit operates, the commander decides how the unit plans, what staff products are required, and when the products are needed. The G-2/S-2 and intelligence staff must focus on what the commander requires. This may necessitate the intelligence staff to understand how to abbreviate various intelligence tasks while still ensuring task results effectively support operations and targeting.

8-125. Early during this tactical transition, units may have to depend on the theater army, joint force, and allied- or partner-nation forces for most of their intelligence. However, as tactical units make contact and start information collection, that dependence should become less significant although higher-level intelligence will always be important. During competition, crisis, deployment, and this early transition, allied and partner nations, DIA, the joint force, and regionally aligned Army forces must develop and populate an authoritative database of threat signatures and associated contextual information. Units establish localized intelligence databases following RSOI. This intelligence effort allows tactical units to access, maintain, populate, and continually update their databases throughout subsequent operations.

8-126. As during competition and crisis, all-source intelligence is central to supporting operations and targeting during large-scale combat operations. All-source intelligence analysis and production reduces the possibility of error, bias, misinformation, and disinformation by considering multiple sources of information and intelligence. As discussed earlier, an effective IPOE sets the conditions for effective staff planning. The commander narrows the focus to effectively account for the mission variables and then dictates how to complete staff planning. For example, the staff can use abbreviated planning to develop an overlay order.

8-127. Focused and tailored intelligence assists in providing a focused view of the OE and presents the commander with multiple options for employing capabilities and gaining positions of relative advantage. As the execution of the operation transpires, the G-2/S-2 collaborates with the commander and G-3/S-3 to develop and disseminate focused and tailored intelligence in the right format at the right time. However, intelligence must also support future operations. Intelligence products must predict future threat actions, capabilities, and dispositions; changes in the terrain and weather; and the ever-changing dynamics within civil considerations.

Note. Narrowing the focus to the mission variables does not mean focusing only on the land domain and physical dimension. Aspects of the other domains and the information and human dimensions can be the difference between mission success and failure. Threat capabilities from the other domains can be more lethal than threat capabilities in the land domain. Despite the natural tendency to focus on the land domain during large-scale ground combat, analysts must look across the OE to determine how the land, maritime, air, space, and cyberspace domains affect Army operations and seek possible windows of opportunity.

PROCESSING, EXPLOITATION, AND DISSEMINATION

8-128. Short and demanding timelines and requirements to support the commander's decisions at echelons corps and below may make intelligence PED more vulnerable to enemy denial and deception activities since there is less time available for initial analysis during exploitation activities. Frequent CP movements and short halts may preclude units from performing intelligence PED with the little time available to reestablish connections within the intelligence architecture. Further, because Soldiers are required to perform tasks to take-down and reestablish CPs, their time to resume intelligence PED activities is reduced when CPs make frequent moves.

8-129. More collection systems operate in theater during large-scale combat operations than during competition or crisis. More collection systems operating means more data is transported across the intelligence architecture; therefore, there is more data requiring intelligence PED. The introduction of new information collection systems, including multinational partner systems and sensors, onboard weapons systems, combat vehicles, and combat aerial platforms, requires adjustments to intelligence PED processes. Federated intelligence PED, including reach PED, will be challenged to adjust intelligence PED support when the situation in theater dictates those adjustments in 24 hours or less. These compressed timelines can occur when corps, division, or BCT CPs make frequent moves, sometimes unanticipated, or when unanticipated enemy actions change the situation in theater.

8-130. During large-scale combat operations, intelligence PED must be prioritized to answer PIRs and identify and track HPTs. The fluidity of the situation demands emphasis on constant feedback across the intelligence process as part of intelligence synchronization. The intelligence staff provides feedback to collection assets and PED activities on their performance. Feedback reinforces if collection, processing, and exploitation are effectively supporting the analysis and production effort. Feedback is essential to maintaining PED effectiveness and alerting MI leaders of deficiencies. Leaders and Soldiers exercising flexible, adaptive, and creative thinking and actions can mitigate many of the challenges and risks to intelligence PED during large-scale combat operations.

INTELLIGENCE ANALYSIS

8-131. Based on relevant aspects of the OE (determined during IPOE), the commander and staff continuously assess information, operations, and changes in the OE. Warning intelligence, situation development, intelligence support to targeting, and intelligence support to information advantage assist the unit in further shaping the OE to facilitate mission success. The continuous analysis of collected information also mitigates risk to friendly forces while identifying opportunities to leverage friendly capabilities to open a window of opportunity.

8-132. Intelligence analysts must understand at which points in an operation the commander needs a specific intelligence requirement answered (usually captured with the intelligence requirement as a latest time intelligence is of value) to support decisions and targeting. This understanding assists the intelligence analysis element, usually an ACE or BISE, in assigning analytical tasks to the various analysts and creating a timeline for conducting analysis.

8-133. Analysts must accept and embrace ambiguity when conducting analysis as they will never have all the information necessary to make certain analytical determinations. Intelligence analysts will be especially challenged during large-scale combat operations where peer threats will conduct elaborate deception operations and use effective counterreconnaissance, cover, concealment, and camouflage techniques. Even in the best of circumstances, maintaining a common interpretation of information and developing situational understanding are difficult.

8-134. Analysts may have to abbreviate certain analytical tasks by quickly screening collected information and using only basic structured analytic techniques to keep pace with the tempo of operations. (See ATP 2-33.4.) Intelligence analysts must predict and track rapidly evolving threat actions involving multiple capabilities across the domains and dimensions. When time is limited for adequate information collection, PED, and intelligence analysis, the all-source analytical element must inform the G-2/S-2 of the gaps, issues, and risks, so the G-2/S-2 can inform the commander. In these situations, the unit must collaborate with and depend on the higher-echelon all-source analytical element for additional support and overwatch or operate based on combat information.

8-135. A goal of intelligence analysis is assisting the unit to identify and open a window of opportunity to eventually achieve a position of relative advantage. Opening a window of opportunity often requires a significant amount of intelligence analysis to achieve a high degree of situational understanding; this is difficult. Tactical units must exercise tactical patience, accept a higher degree of risk, or allocate more capabilities to ensure effective information collection.

8-136. Once friendly forces have an open window of opportunity to execute information collection, intelligence analysts receive more information and may provide effective intelligence that can then assist friendly forces in opening subsequent windows of opportunity to reach a position of relative advantage.

EFFECTIVE INTELLIGENCE PRODUCTS

8-137. Through analysis, the G-2/S-2 identifies indicators of enemy activity, which can present opportunities or risks to friendly forces. Understanding these opportunities or risks is an important part of achieving situational understanding to leverage friendly capabilities against threat forces at the right time and place. Ultimately, effective intelligence products should be tailored to the commander's needs, continuously updated, and provided within the unit's battle rhythm in the commander's preferred format. Intelligence analysts should understand not only their units' operations but also their higher and subordinate forces' missions, key tasks, and end state. This ensures intelligence analysts have an operational context to provide more effective intelligence products.

8-138. In offensive and defensive operations, analysts must gear their efforts to the time available and provide the best possible intelligence products within condensed timelines. Operational planning and planning deadlines often impose challenging time constraints that analysts must meet. Analysts must often produce intelligence products without all the information to reach a more thorough or certain situational understanding. A quick analytical assessment in time to affect staff planning and friendly COAs is better than a perfect analytical assessment received too late to affect staff planning. Meeting analytical deadlines includes presenting intelligence products, assessments, conclusions, or projections about the AO and threat forces in a format that assists the commander and staff in achieving situational understanding.

THE COMMON INTELLIGENCE PICTURE

8-139. Maintaining the CIP during large-scale combat operations has its challenges. Dynamics on the battlefield can impact maintaining the CIP and the resulting situational understanding. G-2/S-2s must consider threat actions, friendly operations on the move, and other challenges like degraded communications that create intelligence latency and degrade populating and disseminating the CIP. Analog processes must be in place to maintain the CIP when conditions dictate, such as during a high tempo. Architecture connectivity concerns must be addressed in unit PACE plans.

8-140. Providing situational understanding of the OE is the main goal when developing and presenting the CIP. The CIP drives the staff's actions to counter the threat; therefore, the G-2/S-2 must consider the effectiveness of the intelligence. This enables the G-2/S-2 to effectively inform planning and decision making as well as provide a more holistic assessment of threat activities. Sharing and having access to the CIP allows multiple entities in different locations to gain and maintain situational understanding of enemy activities. This also enriches analysis, which can be conducted by multiple units, organizations, and agencies.

8-141. Information gained to develop and maintain the CIP derives from several sources, including but not limited to—

- Collection assets.
- All-source reporting.
- Tactical reports.
- Reporting from individual intelligence disciplines.
- SALUTE and/or spot reports.
- Staff running estimates.
- Allied- and partner-nation reporting.

8-142. The commander's requirements largely drive how data, information, and intelligence are depicted on a CIP. (See figure 8-8.)

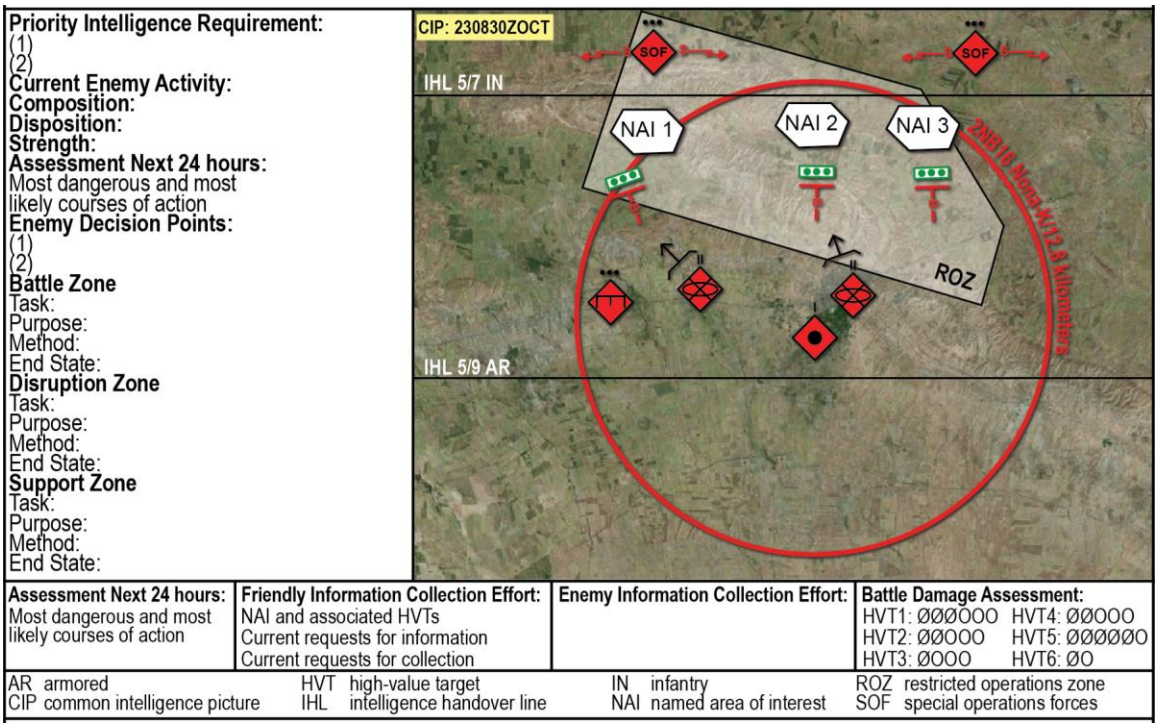


Figure 8-8. Common intelligence picture depiction (example)

8-143. The following are data, information, and intelligence considerations for inclusion on the CIP:

- Intelligence requirements.
- Enemy intent (disposition to the appropriate echelon and activity by the unit's battlefield framework according to unit SOPs):
  - Disruption zone with enemy units and tracks.
  - Battle zone with enemy units and tracks.
  - Support zone with enemy units and tracks.
- Enemy critical tasks, critical capabilities, and purpose.
- Enemy centers of gravity.
- Enemy surveillance and reconnaissance capabilities.
- Enemy scheme of maneuver by unit and unit entities.
- Enemy decision points.
- Routes or tracks of collection assets.
- Intelligence handover lines.
- Modified combined obstacle overlays.
- Combined information overlays.
- Range rings depicting areas where enemy capabilities can impact.
- Enemy composition, disposition, strengths, vulnerabilities, and intentions.
- Assessment of the most likely and most dangerous COAs.
- Assessment of future enemy actions.
- Intelligence and collection gaps.
- Current RFIs and requests for collection.

8-144. Developing and maintaining the CIP requires coordination across several intelligence staff elements. Each element provides critical information for developing and/or maintaining the CIP or uses the data, information, and intelligence within the CIP to conduct activities such as planning. For example, the G-2/S-2 COIC may provide useful information pertaining to—

- BDAs.
- Ongoing information collection activities.
- Answers to intelligence requirements.
- Impacts of friendly operations in the OE.
- Maneuver echelon reports of enemy activity.
- Current assessments on COAs the threat is adopting.
- Changes or effects in the OE that may impact operations.
- Updates from the decision support template and execution checklist to inform further information collection.

8-145. The CIP must be disseminated to the lowest level possible to ensure unity of effort across a unit's intelligence warfighting function capabilities and to nest intelligence with operations. The CIP informs the COP, and the COP influences intelligence activities; this is true at all levels of operations. Synchronizing operations and intelligence by using CIPs and COPs is important. These common tools assist in focusing efforts and ensuring a common understanding of often-chaotic and fast-paced OEs (see figure 5-10 on page 5-25).

8-146. Within unit SOPs, the G-2/S-2 annotates how to develop the CIP, for which there are various development methods. Some units may build the CIP by extracting information from different systems and databases and compiling the information narratively or graphically. Other units may use a process by which data, information, and intelligence are extracted from systems and databases and automatically populated into a narrative or graphic product or a combination of both. When using this method, systems, as part of the intelligence architecture, are typically established with knowledge management rules and processes to ensure data, information, and intelligence are populated to higher and lower echelons.

8-147. Before a mission, the G-2/S-2 must coordinate with higher and lower echelons and adjacent units to confirm how the CIP will be developed. A good practice is conducting rehearsals and confirmation briefs with intelligence staffs at each echelon to lessen the possibility of a particular echelon not receiving CIP updates when needed.

8-148. Typical questions for CIP development include but are not limited to—

- How does the commander—
  - Want to view the CIP (on a digital system, analog, narratively or graphically, relevant layers to display)?
  - Envision CIP development and content?
  - Envision the CIP supporting operations?
  - Envision subordinate units using the CIP?
  - Prioritize the CIP, the intelligence running estimate, and INTSUM?
  - Use the CIP when discussing operations with higher headquarters?
- How does the CIP answer intelligence requirements?
- Are intelligence analysts trained on systems and databases used to develop the CIP?
- How will data, information, and intelligence populate the CIP?
- How does the unit's CIP interface with higher- and lower-echelon CIPs?
- How are multinational and allied-partner data, information, and intelligence incorporated?
- What CIP data, information, and/or intelligence is used for the intelligence portion of the COP?
- Is the CIP rapidly tailorable to support new missions?

8-149. All-source analysts typically maintain the CIP. Whether information is automatically populated onto a unit CIP, or an analyst uses multiple systems and databases to attain information to build the CIP, updating the CIP should be addressed as a battle-rhythm event, much like INTSUM and running estimate activities. The higher headquarters typically annotates CIP requirements, including timelines for updates, within Annex B (Intelligence) of an OPORD.

Appendix A

Joint Task Force and Multinational Intelligence Considerations

JOINT TASK FORCE HEADQUARTERS

A-1. When a corps or division is designated to function as a JTF headquarters, it requires significant augmentation to fulfill the associated tasks. An Army unit designated as a JTF headquarters follows joint doctrine. (See JP 3-33.) The Army intelligence staff assumes the role of the J-2, whose primary function is providing information and analysis to facilitate accomplishing the mission. (See JP 2-0.)

A-2. The primary function of the Army intelligence staff when employed as a JTF intelligence staff does not change; however, this function becomes more complex. The amount of available information often exceeds the staff's ability to manage, fully understand, and leverage it. There is a high demand for information from national leaders, the media, and higher headquarters. This demand has the potential to overwhelm the staff unless additional resources are allocated. There are also complex multinational and interagency considerations for conducting intelligence operations, the intelligence architecture, liaison, and intelligence sharing.

A-3. The primary tasks of the joint intelligence staff include—

- Facilitating an understanding of the OE and supporting decision making.
- Tailoring and distributing intelligence operations, if necessary, implementing a federated structure across multiple echelons. When appropriate, the joint force intelligence staff must also place analysis assets in forward locations to better support lower-echelon requirements.
- Ensuring availability of intelligence.
- Prioritizing collection and allocating analysis resources.
- Integrating threat assessments developed by the combatant command intelligence organization to provide the JTF commander, staff, components, and subordinate units with the complete air, land, maritime, space, and cyberspace threat situation.

A-4. The joint force intelligence staff uses the joint IPOE process to analyze the relevant aspects of the environment, including the physical domains of air, land, maritime, and space; the information environment, which includes cyberspace and the electromagnetic OE; and the political, military, economic, social, information, and infrastructure system and subsystems. This analysis allows the joint staff to develop a COP and the joint force intelligence staff to provide other intelligence support products.

A-5. Joint ISR and Army information collection both share the purpose of integrating and synchronizing the planning and operation of sensors, assets, and PED systems in DS of current and future operations. In both joint and Army doctrine, this activity is an integrated operations and intelligence function.

A-6. Army information collection doctrine expanded the joint doctrinal concept of ISR by better accounting for the role of ground reconnaissance and surveillance operations. (See FM 3-55.) Information collection activities are a synergistic whole, with emphasis on integrating and synchronizing all components and systems. Commanders and staffs have vital responsibilities in information collection planning, preparation, execution, and assessment. Commanders' involvement is particularly important. The success of information collection is measured by its contributions to the commander's understanding, visualization, and decision making.

A-7. Table A 1 depicts the comparison of joint ISR and Army information collection.

Table A-1. Joint ISR and Army information collection responsibilities

Joint ISR		*Army*	
Task	***Responsibility***	***Task***	***Responsibility***
ISR concept of operations	J-2 (in coordination with the J-3)	Annex L (Information Collection) of the plan or order	G-2 and G-3 (S-2 and S-3)
Collection management: • Collection requirements management • Collection operations management	J-2 (in coordination with the J-3)	Collection management	G-2/S-2
		Direct information collection	G-3/S-3
Execute collection	Units and organizations	Execute collection	Units and organizations
Assessment and retasking		Assessment and retasking	

G-2 division or corps intelligence staff officer
G-3 division or corps operations staff officer
ISR intelligence, surveillance, and reconnaissance
J-2 intelligence directorate of a joint staff
J-3 operations directorate of a joint staff
S-2 battalion or brigade intelligence staff officer
S-3 battalion or brigade operations staff officer

A-8. The ISR concept of operations roughly corresponds to Annex L (Information Collection) of an Army OPLAN or OPORD. The ISR concept of operations—

- Documents the integration, synchronization, and operation of ISR resources to support current and future operations.
- Outlines the capability to task, collect, process, exploit, and disseminate timely and accurate information that provides the awareness necessary to successfully conduct operations.
- Addresses how all available ISR collection assets and associated PED infrastructure, including multinational and commercial assets, will be used to satisfy the joint force's anticipated collection tasks.

A-9. To facilitate the optimum use of all available ISR assets, the J-2, in coordination with the J-3, develops an ISR concept of operations in conjunction with the command's planning effort. The ISR concept of operations should be based on the collection strategy and ISR execution planning, and it should be developed jointly by the joint force intelligence and operations staffs. Planning for the ISR concept of operations must also identify and discuss any ISR and PED asset gaps relative to the joint force's validated PIRs. This assessment may be used to justify the commander's request for the allocation of additional ISR and PED resources. It should also require a periodic evaluation of the capabilities and contributions of all available ISR assets relative to the joint force mission. This maximizes their efficient use and ensures the timely release of allocated ISR resources when no longer needed by the joint force.

A-10. In the joint lexicon, collection management is a process composed of two subfunction, CRM and COM, and it requires collection orchestration:

- CRM defines what intelligence systems must collect, focuses on customers' requirements, and is all-source oriented and advocates for the information necessary for collection.
- COM specifies how to satisfy requirements, focuses on the selection of specific intelligence disciplines and systems within a discipline to collect information addressing customers' requirements, is conducted by organizations to determine which assets can best satisfy customers' product requests, and is informed by weather conditions, effects, and the timing of those effects on collection assets based on current and future forecasts in the OE.
- Collection orchestration is the integration, synchronization, and optimization of the intelligence process and operations, including national and theater collection integration; all-domain, multidiscipline collection strategy development; and end-to-end synchronization of CRM, COM, and overhead reconnaissance and DOD ISR mission management systems.

MULTINATIONAL INTELLIGENCE CONSIDERATIONS

A-11. Multinational operations are common, making multinational intelligence operations very important. (See FM 3-16.) National interests require the United States to act with other nations. In many situations, U.S. forces join allied and partner forces to defeat common threats.

Note. Both the ABCANZ Armies' Program and ABCANZ standards enable greater understanding of the Army's portion of multinational requirements and assist in identifying unique requirements that support the command. Access the All Partners Access Network (also known as APAN) website on NIPRNET for more information.

A-12. The multinational force synchronizes its intelligence efforts with unified action partners to achieve unity of effort and meet the commander's intent. Intelligence unity of effort is critical in accomplishing the mission. Unified action partners enable support and perspective to intelligence. Multinational and interagency partners provide expertise and unique perspectives that reinforce and complement Army intelligence capabilities. Unified action partners may have access to different capabilities, or they may have a capability with more capacity than the Army and joint forces' capacity. Some partners may have unique policies, authorities, or access that provide intelligence opportunities not otherwise available to Army forces. Using appropriate procedures and established policy, multinational force intelligence leaders provide information and intelligence support to multinational forces.

A-13. Intelligence leaders ensure the intelligence warfighting function operates effectively and efficiently. These leaders are the commander's primary advisors on employing ISR and information collection assets. Multinational forces need to approach ISR as a unified effort. To drive ISR and information collection properly, intelligence leaders consider and leverage all capabilities provided by the multinational force. Additionally, intelligence analysts support their commanders with analysis and production of timely, relevant, accurate, and predictive assessments and products tailored to their commanders' needs.

INTEROPERABILITY

A-14. *Interoperability* is the ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives (JP 3-0). Table A-2 lists the levels of interoperability according to AR 34-1. The foundation of interoperability spans the warfighting functions with human, procedural, and technical elements. Interoperability is often associated with technical issues; however, network and information technology systems are not the sole components. Human and procedural aspects are considerations in developing interoperability. The human element builds the basis of the mutual understanding and respect that is fundamental to unity of effort and operational success. The procedural element ensures that the Army achieves sufficient harmony in policies and doctrine enabling effective operations with other military unified action partners.

Table A-2. Levels of interoperability

Level 0 (not interoperable). Unified action partners (UAPs) have no demonstrated interoperability. Command and control (C2) interface with the Army is at the next higher echelon, and UAPs must operate independently from Army formations and operations.
Level 1 (deconflicted). Army and UAPs coexist but do not interact. Interoperability requires an alignment of capabilities and procedures to establish operational norms, so UAPs and the Army complement each other's operations. • **Communication and information systems.** The lead nation provides digital liaison support for network, services, and common operational picture (COP) interoperability to UAPs. (See note following this table.) • **Information management.** UAPs rely on manual information management and knowledge management processes. Information exchange processes and standardized products are undefined across the coalition. There exists a minimally acceptable information management policy and plan. • **Intelligence, surveillance, and reconnaissance and intelligence fusion.** Military UAPs conduct intelligence sharing on an ad hoc basis and rely solely on a lead nation's common intelligence picture (CIP). • **Fires.** Military UAPs use voice procedures for cross-nation boundaries and use only their national precision fires. • **Sustainment.** National support elements provide national logistics support only. ***Note.*** Nonmilitary UAPs coexist in the area of operations with the Army, and interoperability problems are largely solved by liaison officers to coordinate and exchange information at the UAP's location. No formal agreements exist regarding the sharing of information or pattens of behavior upon which to build a relationship.

Table A-2. Levels of interoperability (*continued*)

Level 2 (compatible). Army and UAPs can interact with each other in the same geographic area in pursuit of mutual goals. Army and UAPs have similar or complementary processes and procedures and operate effectively with each other. • **Communication and information systems.** UAPs achieve network connectivity through technical ad hoc procedures. Partners provide their own core services. The COP is achieved via ad hoc procedures. • **Information management.** UAPs exchange only information that is agreed upon (versus common information). UAPs must agree on information/knowledge management policies before deployment. UAPs conduct manual records management. • **Intelligence, surveillance, and reconnaissance and intelligence fusion.** National representatives and liaison officers facilitate partial access to intelligence across nations and domains for a partial CIP. UAP intelligence staffs use standard operating procedures to drive intelligence fusion, collection management, and intelligence, surveillance, and reconnaissance requirements. • **Fires.** National digital systems require Fire Direction Center translation, some ammunition interchangeable, and common voice call for fire procedures. • **Sustainment.** Liaison officers, manual processing, and limited digital automation are required for log replenishment.
Level 3 (integrated). Army and UAPs can integrate in theater. Interoperability is network-enabled to provide the full range of military operations capability. UAPs can routinely establish networks and operate effectively with or as part of Army formations. • **Communication and information systems.** UAPs share a common network, common services, and a COP. • **Information management.** Common defined information exchange products, common information management/knowledge management policies, common information management baseline, and automated records management. • **Intelligence, surveillance, and reconnaissance and intelligence fusion.** UAPs have sufficient access to intelligence across nations and access to Top Secret, Secret, and unclassified domains to facilitate high-tempo operations. UAPs can request and access intelligence, surveillance, and reconnaissance across domains and nations. UAPs contribute and share a CIP and intelligence staffs have common training, processes, and procedures. • **Fires.** UAPs use networked fires C2, including precision effects and interchangeable ammunition. • **Sustainment.** UAPs initiate and execute coalition logistic replenishment by digital automation.

Note. A digital liaison detachment provides a digital liaison capability to Army units—theater army, corps, and division headquarters—for connectivity with allied and multinational force units and other Services. (See ATP 3-94.1.)

A-15. The Army's capability and capacity to share information freely and securely are imperative to multinational partner interoperability. The speed of information sharing improves the commander's ability to create unity of effort and C2. Interoperability, and particularly a shared COP, builds trust during operations with multinational forces. It is critical for Army forces to be informed of pertinent information sharing authorities. Leaders must also emphasize the importance of information sharing.

A-16. Integrated and secure information sharing dramatically improves Army forces' ability to fight as one multinational team. The broader unified action partner team also includes other U.S. Government departments and agencies, state and local governments, allies, coalition members, host nations, other nations, multinational organizations, nongovernmental organizations, academia, and the private sector.

A-17. Units must be aware of and remain sensitive to cultural and religious differences among multinational partners. In some instances, these differences may result in periods of increased vulnerability for the joint force or may require scheduling changes for meetings and briefings. Major differences may include techniques for intelligence provided to the commander (jointly or individual Services or agencies), procedures for sharing information among intelligence agencies, and security afforded by different communications systems and procedures. Administrative differences may include classification levels, personnel security clearance standards, requirements for access to sensitive intelligence, and translation requirements.

A-18. Typically, there is a disparity in U.S. and multinational force capabilities. Multinational forces may have greater intelligence resources within a given region, including valuable and extensive HUMINT, critical foreign language skills, and access to the population and open sources. U.S. forces must generally provide technical assistance to share information and intelligence.

A-19. It is imperative for combined force commanders to establish a system that optimizes each nation's contributions and provides units reliable intelligence. U.S. units subordinate to non-U.S. headquarters may face unique problems in disseminating intelligence. If a direct channel is available to the next higher U.S. headquarters, the tactical U.S. unit may have better and more current intelligence than its controlling non-U.S. headquarters. In that instance, liaison personnel should disseminate intelligence while adhering to foreign disclosure regulations.

INTELLIGENCE OPERATIONS PLANNING AND COORDINATION IN MULTINATIONAL OPERATIONS

A-20. Like the United States, unified action partners have policy restraints and sovereignty concerns. Such restraints and concerns mean that nations will likely limit their available assets to a multinational force. Therefore, multinational forces accept that they will often have limited, decentralized control over some of their intelligence assets, and they will have no direct control over assets restricted by individual nations. These restricted assets are managed by nations' national intelligence cell. Multinational forces performing intelligence operations establish an intelligence fusion cell at the headquarters level through which intelligence tasks flow. This cell assists in integrating intelligence representatives and liaison personnel at each organizational level and improves access to intelligence capabilities. Staffs base information collection plans on matching a coalition organization's intelligence requirements with available and accessible intelligence assets.

A-21. The multinational force executes ISR with an emphasis on leveraging the larger intelligence enterprise. The commander provides the intelligence section with a clear mission statement and commander's intent. The intelligence section then develops PIRs and prioritizes intelligence collection requirements to meet the commander's needs. A multinational force's ability to gather and process intelligence varies widely. The command's collection manager accounts for this variance and tasks various intelligence assets and ISR platforms accordingly, matching collection assets with requirements to answer PIRs. Sharing information and mutual support are key to integrating all resources into a system to best meet the command's intelligence requirements.

INTELLIGENCE REQUIREMENTS MANAGEMENT AND COLLECTION MANAGEMENT

A-22. Conducted at all levels in NATO, intelligence requirements management and collection management are integrated management processes and services to satisfy intelligence requirements by making the best use of the available collection, PED, and intelligence processing capabilities. They ensure intelligence requirements are answered and the collection, PED, and processing capabilities available are focused and prioritized. A common understanding allows higher and lower headquarters within NATO and nations to share intelligence information and make the best use of collection and exploitation capabilities:

- **Intelligence requirements management** describes a set of integrated management processes and services that summarize, prioritize, and validate incoming intelligence requirements; initiate the collection of associated information; quality control processed outputs, and oversee the dissemination of intelligence products. The intelligence staff leads this management process. In any operation or planning situation, commanders determine the type of information required to allow them to plan and conduct their mission effectively.
- **Collection management**, defined in paragraph 5-17, also encompasses activities related to the execution and coordination of the joint ISR process. The theater collection manager implements collection management. The theater collection manager exercises collection management authority for a given mission and area of intelligence responsibility and directs CRM and COM to synchronize joint ISR and task, collect, process, exploit, and disseminate activities among participating nations and partners.

Note. Paragraph A-22 implements multinational doctrine contained in AJP-2 and AJP-2.1.

SHARING AND WRITE FOR RELEASE

A-23. The joint force should share relevant intelligence about the situation and adversary with its multinational partners consistent with respective national disclosure policy and JFC guidance. However, information about intelligence sources and methods should not be shared among allies and partner nations until approved by the appropriate national-level agency. In most multinational operations, commanders share intelligence with foreign forces and coordinate receiving intelligence from those forces.

A-24. One technique for facilitating intelligence sharing and collaboration is establishing an information exchange cell. Another technique for sharing critical intelligence with multinational partners is having U.S. intelligence information written for release at the lowest possible classification level (with the fewest dissemination restrictions) within foreign disclosure guidelines.

Writing for Release

JP 2-0 describes writing for release as the deliberate process of producing information for disclosure to mission partners all levels; any references to sources and methods should only be included below a tear line to maximize the ability to share relevant information with partners. Intelligence production agencies often use a tear line in classified reports to separate compartmented information from intelligence that can be widely disseminated. (The J-2 and component intelligence staff officers keep information above the tear line and disseminate the intelligence below.) Having intelligence production agencies use such tear lines facilitates intelligence sharing.

Note. *Tear line* is a visible line on an intelligence message separating categories of information that have been approved for foreign disclosure and release (JP 2-0).

A-25. When information relating to a particular source cannot be shared, the intelligence derived from that source should still be provided if the information itself does not potentially compromise the source. The Director of National Intelligence must establish procedures for separating intelligence from sources and methods. Analysts must balance the accuracy and amount of information written for release with the security of classified material. Then, they must properly vet that intelligence through the foreign disclosure officer before dissemination. Intelligence production agencies often publish highly classified reports in a format that separates compartmented information from intelligence that can be widely disseminated with a tear line. The U.S. joint and component intelligence staffs keep information above the tear line for U.S. forces while disseminating the intelligence below the tear line to multinational forces.

DISCLOSURE POLICY AND THE DISCLOSURE OF CLASSIFIED INFORMATION

A-26. The foreign disclosure office may approve the disclosure of classified and controlled unclassified military information to foreign representatives. This is based on the policies, directives, and laws that govern national disclosure policy and the release of classified information. The foreign disclosure office provides this service to the command and staff and to assigned, attached, and supporting agencies, allies, and other multinational partners. Each nation must determine what collected information its forces can share, in what format, and how information is passed; ideally, this will be discussed coalition-wide during the planning the phases of the operation. The U.S. force intelligence staff enforces national disclosure policy and the disclosure of classified information to multinational intelligence partners through the foreign disclosure office, which has staff proponency for this action.

A-27. Using the disclosure policy, pertinent laws, regulations and directives, the foreign disclosure office—

- Adjudicates disclosure requests by using delegated disclosure authorities and sanitization guidelines.
- Advises the commander and staff on potential problems when existing disclosure authorities do not support current or future requirements to disclose.
- Facilitates sharing relevant and pertinent intelligence about the situation and threat between the U.S. military and allies and other multinational partners consistent with disclosure policy and U.S. joint force guidance.
- Pays special attention to intelligence classification and levels of access of multinational personnel. However, the office avoids sharing information about intelligence sources and methods with allies and other multinational partners until approved by the appropriate national-level agency.

A-28. The U.S. joint force intelligence staff obtains the necessary foreign disclosure authorization for category 8 (MI) information from the DIA and disclosure authority from the combatant command foreign disclosure office as soon as possible. U.S. intelligence personnel should be knowledgeable of the specific foreign disclosure policy, procedures, and regulations for the operation. It is therefore imperative that the U.S. joint force intelligence staff considers adding extra foreign disclosure office billets to the joint manning document. Through local policy, the authorization for foreign disclosure representatives can be used by units to assist the foreign disclosure office after completing an authorized training program. Personnel knowledgeable of foreign disclosure enhance the efficient flow of intelligence.

A-29. Intelligence support to protection of the force is critical. Every effort should be made to share any intelligence that could affect accomplishing the multinational force mission or protecting the force. A key consideration is the apportionment of trained foreign disclosure personnel within a theater to facilitate sharing information and products with the multinational force. (See AR 380-10 for foreign disclosure information.)

A-30. The following are other general principles that assist in guiding multinational intelligence sharing:

- **Maintain unity of effort.** Each nation's intelligence personnel must view the threat from multinational and national perspectives. A threat to one element of the multinational force by the common adversary is a threat to all multinational force elements.
- **Make adjustments.** Coalition members should agree on processes and procedures when planning because of differences in intelligence doctrine and procedures among the multinational partners. Differences may include how intelligence is provided to the commander or procedures for sharing information among intelligence agencies. Intelligence leaders often use information sharing processes and procedures discussed in ABCANZ standards and NATO standardization agreements.
- **Plan early and plan concurrently.** This permits solutions to any differences to be developed and tried before operations begin. This also ensures there are sufficient resources for liaison requirements to support multinational operations.
- **Conduct complementary operations.** Partner intelligence operations must be complementary, and all intelligence resources must be available for application to the entire intelligence problem. The intelligence staff must be prepared to navigate different approval processes and political sensitivities when executing multinational intelligence operations.

A-31. The following are considerations for intelligence networks and architectures while operating with multinational forces:

- Establish a shared local area network using systems such as CENTRIXS or the US BICES.
- Establish and enforce a standardized process for the intelligence sharing architecture such as using the cross-domain enterprise all-source user repository for cross-domain operations.
- Many nations provide their own national suite of analytical tools, digital mapping capabilities, collaboration software, and internal capabilities.
- Multinational intelligence analysis occurs on the multinational network of shared database servers with its metadata catalog and releasable databases. These tools access and pull data from multinational force shared databases and other nationally owned data repositories.
- Standardize compatible formats in which information is converted or stored to make the information accessible and useable by multinational partners. However, ensure the information that does not require conversion is left in its original format. This facilitates a faster flow of information.
- Use the multinational intelligence center to coordinate multinational ISR and collection plans for each nation.
- Designate a single officer as the director of intelligence for the multinational force.
- Ensure each nation has a representative present at the multinational intelligence center.

A-32. The effective use of intelligence liaison personnel can establish strong relationships with multinational partners. Effective liaisons can be instrumental in resolving the normal problems that result from language barriers and cultural and operational differences during multinational intelligence operations. Intelligence leaders must plan for and carefully manage U.S. intelligence liaisons and interpreters to an allied nation, partner nation, or multinational headquarters and their supporting intelligence cells. This ensures effective collaboration and unity of effort.

This page intentionally left blank.

Appendix B

Intelligence Warfighting Function Tasks

THE ARMY INTELLIGENCE WARFIGHTING FUNCTION TASK LIST

B-1. The Army Intelligence Warfighting Function Task (IWFT) List is a comprehensive, but not all-inclusive, listing of Army IWFTs, missions, and operations intended to inform commanders, staffs, and Soldiers of intelligence warfighting function contributions. Units and staffs perform these tasks, missions, and operations or capabilities at the corps level and below. As a reference, the Army IWFT List captures doctrinal tasks associated with the intelligence warfighting function. (See figure B-1.)

Notes. This appendix is a proponent-developed listing of Army IWFTs. The numbering system is based on the Functional Category 2 (Intelligence) for doctrine, assigned in accordance with DA PAM 25-40.

Appendix B can be treated as a stand-alone appendix; therefore, acronyms and definitions have been reintroduced.

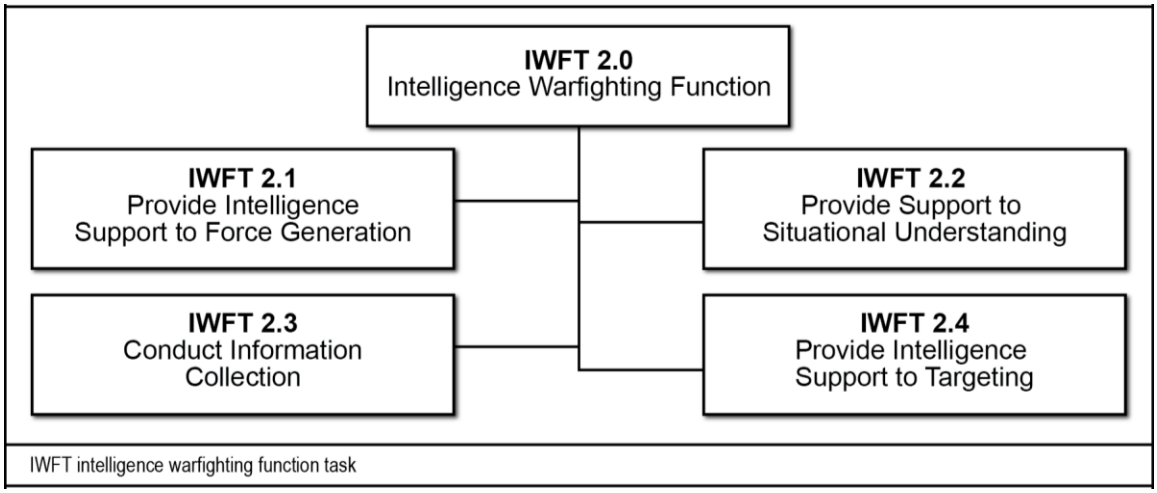


Figure B-1. Intelligence warfighting function tasks

PROVIDE INTELLIGENCE SUPPORT TO FORCE GENERATION (IWFT 2.1)

B-2. *Force generation* is an element of military force. It is the operation that creates and provides units for projection and employment to enable military effects and influence across multiple operational environments. It is the primary responsibility of the Services to develop, provide, and preserve forces in support of the national military strategy to enable the combatant commanders to execute their missions (AR 525-29). Provide intelligence support to force generation is the intelligence warfighting function's flexible and responsive support to the Army sustainable readiness model that involves providing intelligence readiness; planning, establishing, and revising an intelligence architecture; providing intelligence overwatch; and tailoring the intelligence force. These activities facilitate the design and augmentation of military forces

deployed to respond to a crisis or contingency operation. Provide intelligence support to force generation includes establishing intelligence communications and knowledge management architectures, which enable collaboration among strategic, operational, and tactical intelligence organizations through intelligence reach, collaborative analysis, data storage, processing and analysis, and intelligence support to force generation. Provide intelligence support to force generation includes four tasks, as shown in figure B-2.

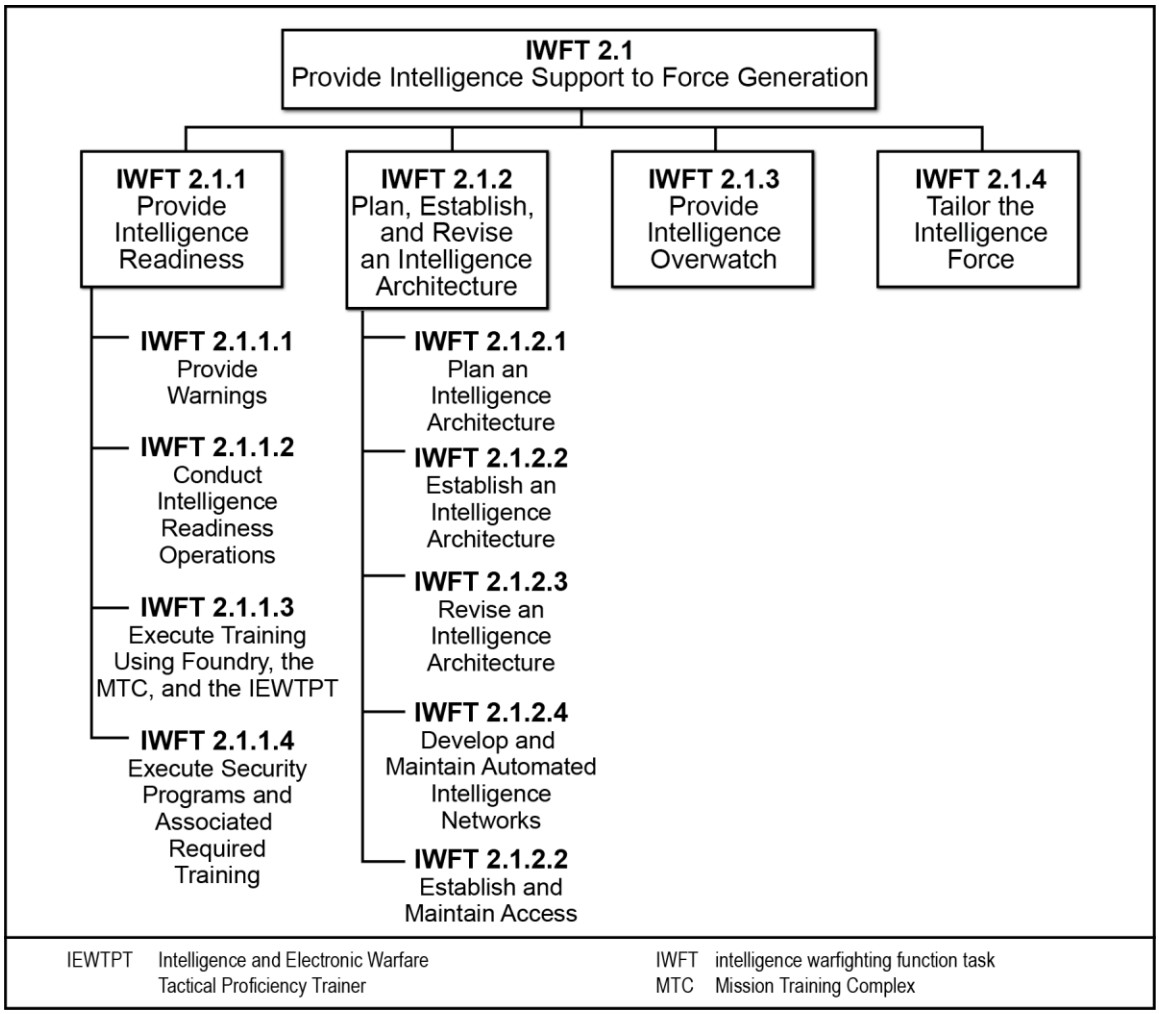


Figure B-2. Providing intelligence support to force generation

PROVIDE INTELLIGENCE READINESS (2.1.1)

B-3. Intelligence readiness operations develop baseline knowledge of multiple potential threats across domains and the operational environment (OE). These operations support ongoing operations, contingency planning, and operational preparation. These operations and related intelligence training activities enable the intelligence warfighting function to support the commander's intelligence requirements. Provide intelligence readiness includes four tasks:

- Provide warnings.
- Conduct intelligence readiness operations.
- Execute training using Foundry, the Mission Training Complex, and the Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT).
- Execute security programs and associated required training.

Provide Warnings (2.1.1.1)

B-4. The provide warnings task provides the commander with advanced warning of threat actions or intentions. The intelligence staff develops warnings to rapidly alert the commander of events or activities that would change the basic nature of the operation. The conduct of CI activities can detect and identify threat intelligence targeting U.S. forces, allowing the commander to understand and counter threat intentions. Warnings enable the commander and staff to quickly reorient the force to unexpected contingencies and to shape the OE.

Conduct Intelligence Readiness Operations (2.1.1.2)

B-5. Conducting intelligence readiness operations supports contingency planning and preparation by developing a baseline knowledge of multiple potential threats and OEs. This information and training enable a collaborative effort and environment to provide the best possible initial threat understanding.

Execute Training Using Foundry, the Mission Training Complex, and the Intelligence and Electronic Warfare Tactical Proficiency Trainer (2.1.1.3)

B-6. The Foundry Intelligence Training Program is a critical enabler to Army global readiness; it provides commanders select resources to train military intelligence (MI) Soldiers and civilians supporting multidomain operations at the strategic, operational, and tactical levels. Foundry—

- Enables available and ready MI individuals and units to conduct multidomain intelligence operations and activities to support commanders executing their missions.
- Provides venues for commanders to collectively certify MI individuals and units (team and higher) to support regional alignment and global contingency operations.
- Enables intelligence oversight and compliance of laws, policies, and directives for intelligence missions that are highly technical.
- Provides access to the intelligence enterprise and sensitive networks, required accreditation, and technical certification.
- Enhances command and control (C2) proficiency.
- Compliments unit-led training and the Training Support System.

B-7. The Mission Training Complex supports commanders' collective and individual training by providing various C2 training capabilities to enhance unit readiness. It unifies exiting capabilities that provide simulation/stimulations to integrate live, virtual, and constructive training environments and execute training and exercises for all echelons. Mission Training Complex locations include all military installations with a corps or division headquarters.

B-8. IEWTPT is the Army's program of record for training the intelligence warfighting function in realistic simulated mission environments. This provides the digital range for the Military Intelligence Training Standards (also called MITS) certification. IEWTPT enables intelligence warfighting function systems and software with realistic data and information to train collectors and analysts in supporting institutional and operational training objectives. IEWTPT enhances the constructive or virtual training environment with complex simulated data and information that exhibit the characteristics of real-world, relatively raw data. Additionally, this data can also be tailored to address the commander's specific training objectives. IEWTPT supports MI Soldier and system training for individual and collective events. (See AR 350-32.)

Execute Security Programs and Associated Required Training (2.1.1.4)

B-9. The staff executes security programs appointed as additional duties or orders from the commander, including training requirements directed by the security program. This task is designed to support programs such as physical security, operations security, communications security, personnel security, and other programs as directed by Army regulations.

PLAN, ESTABLISH, AND REVISE AN INTELLIGENCE ARCHITECTURE (2.1.2)

B-10. The plan, establish, and revise an intelligence architecture task supports the intelligence enterprise. It has five tasks:

- Plan an intelligence architecture.
- Establish an intelligence architecture.
- Revise an intelligence architecture.
- Develop and maintain automated intelligence networks.
- Establish and maintain access.

Note. The Ground Intelligence Support Activity serves as the Army service provider for sensitive compartmented information systems, the single Army JWICS Internet Protocol registration authority, and the responsible organization for implementing Army JWICS Internet Protocol policy.

Successfully Planning, Establishing, and Revising an Intelligence Architecture

A successful technique for dealing with the complexities of planning, establishing, and revising an intelligence architecture is using Digital Intelligence Systems Master Gunner (also known as DISMG) course graduates. The course informs leaders of integration factors with joint and mission partner networks to enable OE visualization as well as informs and advises unit leaders on current digital MI capabilities. The Foundry Intelligence Training Program offers the Digital Intelligence Systems Master Gunner course under the direction of the U.S. Army Forces Command G-2.

Plan an Intelligence Architecture (2.1.2.1)

B-11. Developing an intelligence architecture plan requires planners to understand the mission and OE where the military operation will occur in order to determine intelligence architecture requirements. To do this, planners must evaluate the OE by using the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]) and mission variables (mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations [METT-TC (I)]). Planners must consider the intelligence disciplines, joint and multinational partners/equipment, complementary capabilities, systems interoperability, intelligence and other communications, foreseeable/unforeseeable physical locations of intelligence elements/assets, and system capabilities to support intelligence reach, processing, exploitation, analysis, federated analysis, data storage, and intelligence production. As much as is feasible, the intelligence architecture should be resilient and effective even in degraded, intermittent, and limited communications environments.

Establish an Intelligence Architecture (2.1.2.2)

B-12. Establishing an intelligence architecture encompasses complex and technical issues such as sensors, data flow, hardware, software, communications, communications security materials, network classifications, technicians, database access, liaison officers, training, and funding. A well-defined and well-designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible understanding of all relevant aspects of the OE.

Revise an Intelligence Architecture (2.1.2.3)

B-13. 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 C2 nodes.

Develop and Maintain Automated Intelligence Networks (2.1.2.4)

B-14. Developing and maintaining automated intelligence networks entail providing information systems that connect unique assets, units, echelons, agencies, and multinational partners for intelligence, collaborative analysis and production, dissemination, and intelligence reach. They use existing automated information systems and, when necessary, create operationally specific networks. In either case, these networks allow access to unclassified and classified means and interoperability across the *area of operations*—an operational area defined by the commander for the land or maritime force commander to accomplish their missions and protect their forces (JP 3-0). This task includes identifying deficiencies in the systems or networks, Service procedures, system administration procedures, security procedures, alternate power plans, redundancy, system backups, and update procedures.

Establish and Maintain Access (2.1.2.5)

B-15. The establish and maintain access task entails establishing and providing access to classified and unclassified programs, databases, networks, systems, and other web-based collaborative environments for Army and multinational organizations to facilitate intelligence reporting, production, dissemination, sustainment, and intelligence reach. This task also includes establishing access with joint forces and national agencies to facilitate a multilevel collaborative information dimension.

PROVIDE INTELLIGENCE OVERWATCH (2.1.3)

B-16. Intelligence overwatch is creating standing fixed analytical intelligence capabilities that provide dedicated intelligence support to committed maneuver units. The overwatch element is connected through a shared intelligence network that can extract information from multiple sources and provide succinct answers (vice megabytes of information) directly to supported units when time is critical.

TAILOR THE INTELLIGENCE FORCE (2.1.4)

B-17. The generating force uses mission analysis to focus the allocation of intelligence resources for use by a joint task force or combatant commander as well as to support strategic objectives, the Army's mission, and operations at each echelon. Based on its own mission analysis, the staff at each echelon allocates intelligence resources obtained through the generating force according to the commander's guidance, intent, and mission objectives.

PROVIDE SUPPORT TO SITUATIONAL UNDERSTANDING (2.2)

B-18. *Situational understanding* is the product of applying analysis and judgment to relevant information to determine the relationship among the operational and mission variables (ADP 6-0). This task provides information and intelligence to commanders so they can clearly understand the force's current state in relation to the threat and other aspects of the OE. It supports the commander's ability to make sound decisions. Provide support to situational understanding consists of six tasks, as shown in figure B-3 on page B-6.

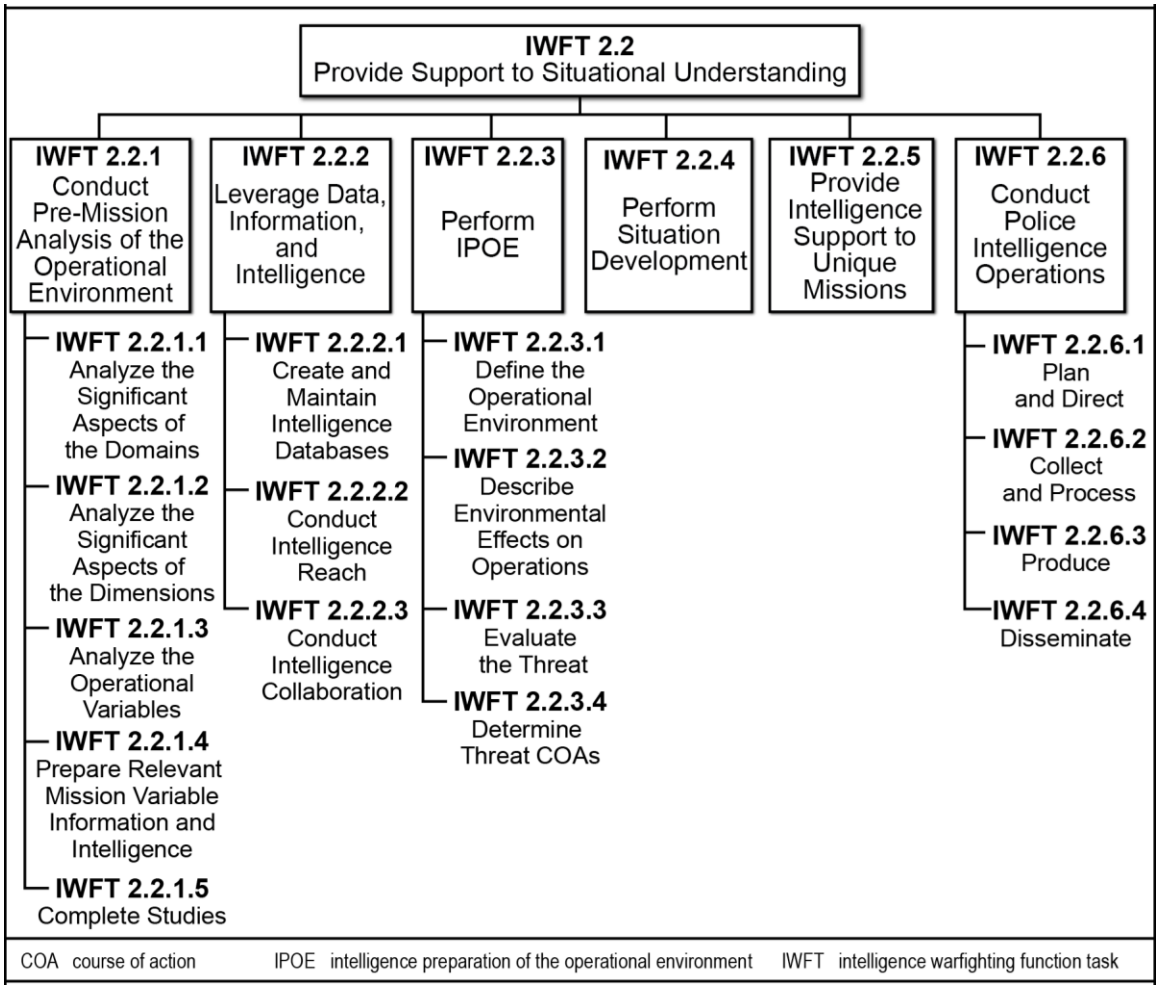


Figure B-3. Providing support to situational understanding

CONDUCT PRE-MISSION ANALYSIS OF THE OPERATIONAL ENVIRONMENT (2.2.1)

B-19. Conduct pre-mission analysis is a continuous task driven by the commander. To perform intelligence preparation of the operational environment (IPOE) and the other important intelligence tasks that support operations, the intelligence staff must conduct a significant amount of analysis before the receipt of a mission. As soon as the intelligence officer and other staff sections begin to collect data on the OE, they should organize the data into databases that meet the commander's visualization requirements. The execution of this task must follow all applicable policies and regulations on information collection and operations security.

B-20. The information and intelligence obtained are refined into knowledge for use in mission analysis through functional analysis. Information is obtained through intelligence reach; publicly available information (PAI) research; data mining; database access; academic studies, products, or materials; intelligence archives; and other information sources. Pre-mission analysis is the foundation for performing IPOE and mission analysis. Initial data files are a primary product of the conduct pre-mission analysis of the OE task.

B-21. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). For Army forces, an OE includes portions of the land, maritime, air, space, and cyberspace domains understood through three dimensions (human, information, and physical). The land, maritime, air, and space domains are defined by their physical characteristics. Cyberspace, a man-made network of networks, transits and connects the other domains. Conduct pre-mission analysis of the OE consists of five tasks:

- Analyze the significant aspects of the domains.
- Analyze the significant aspects of the dimensions.
- Analyze the operational variables.
- Prepare relevant mission variable information and intelligence.
- Complete studies.

Analyze the Significant Aspects of the Domains (2.2.1.1)

B-22. A *domain* is a physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills (FM 3-0). The interrelationship of the land, maritime, air, space, and cyberspace domains requires cross-domain understanding. Analyzing the significant aspects of the domains during pre-mission analysis requires understanding the strengths and dependencies of Army and joint capabilities in each domain that are fundamental to a multidomain, combined arms approach to operations.

Analyze the Significant Aspects of the Dimensions (2.2.1.2)

B-23. Army leaders seek to understand an OE through the human, information, and physical dimensions inherent to each domain. While used to understand all aspects of an OE, analyzing the human, information, and physical dimensions also assists leaders in identifying and understanding *informational considerations*—those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information (FM 3-0). Understanding the human, information, and physical dimensions of each domain assists commanders and staffs in assessing and anticipating their future operations effects.

Analyze the Operational Variables (2.2.1.3)

B-24. Analyzing the operational variables begins well before the deployment of forces. Given the limited time available to collect and evaluate information and intelligence on the operational variables during pre-mission analysis, the information obtained from these data files may not be specific enough to support the IPOE process and the military decision-making process (MDMP). However, the commander and staff can use the information to assist in framing the OE during the Army design methodology. Upon receipt of a warning order (WARNORD) or mission, the commander and staff draw relevant information categorized by the operational variables and filter it into the mission variables used during mission analysis.

Prepare Relevant Mission Variable Information and Intelligence (2.2.1.4)

B-25. During pre-mission analysis, the staff obtains information and intelligence focused on the relevant aspects of the OE as they pertain to the staff's warfighting function. The intelligence staff focuses primarily on the mission variables of enemy, terrain and weather, and civil considerations. However, depending on the staff's echelon, the type of OE, the type of operation, and changes in the OE, the staff may need to update its analysis to ensure the mission focus is both relevant and accurate. This task comprises four subtasks.

Develop the Foundation to Define Threat Characteristics (2.2.1.4.1)

B-26. Developing the foundation to define threat characteristics entails obtaining detailed information and intelligence about threat characteristics affecting the conduct of operations. The intelligence section obtains this information from sources that include intelligence reach; PAI research; data mining; database access; academic studies, products, or materials; intelligence archives; and other information sources. This task develops specific, detailed information for each threat characteristic. The information, intelligence, products, and materials obtained are refined for use in mission analysis, IPOE, and other planning tasks. This refinement occurs through functional analysis and other analytic techniques.

Obtain Detailed Terrain Information and Intelligence (2.2.1.4.2)

B-27. This task entails obtaining detailed information and intelligence about the terrain in the expected area of interest (AOI) from sources that include intelligence reach; PAI research; data mining; database access; academic studies, products, or materials; intelligence archives; and other information sources. The information, intelligence, products, and materials are refined for use in mission analysis, IPOE, and other planning tasks through functional analysis. This task encompasses the types of environments (for example, the desert and jungle) and the military aspects of terrain.

Obtain Detailed Weather and Weather Effects Information and Intelligence (2.2.1.4.3)

B-28. This entails obtaining detailed information and intelligence of the present and future physical environment. Detailed information and weather analysis includes incorporating climatology effects on the AO and assessments of current and future weather effects on Army operational capabilities, including forecast weather effects on both friendly and enemy forces. The intelligence staff relies on the Air Force staff weather officer at each echelon to assist in developing mission analysis and IPOE weather support products, information, and the knowledge required to incorporate forecast weather effects into all Army operational planning and mission execution.

Obtain Detailed Civil Considerations Information and Intelligence (2.2.1.4.4)

B-29. This task entails obtaining specific and detailed information and intelligence concerning the civil considerations (areas, structures, capabilities, organizations, people, and events [also called ASCOPE]) within or affecting the AOI. The intelligence section obtains this information and intelligence within or affecting an expected OE through staff collaboration with the G-9/S-9; intelligence reach; PAI research; data mining; database access; academic studies, products, or materials; and intelligence archives. The data, information, intelligence, products, and materials obtained are refined for use in mission analysis, IPOE, and other planning and operational tasks through functional analysis.

Complete Studies (2.2.1.5)

B-30. To assist in achieving goals and objectives, the complete studies task entails providing the requesting command or organization with detailed information, assessments, and conclusions about the AO and AOI. A study can be a systems or functional analysis product and should be as detailed as time allows. Studies provide knowledge that supports understanding local populations; cultures and caste systems; societal systems or organizations; political systems and structures; religions practiced and their impacts; moral beliefs and their impacts; civil authority considerations; military organizations, structure, and equipment; and attitudes toward U.S., multinational, or host-nation forces. Studies can also include the views and attitudes of multinational and host-nation forces toward these factors. The complete studies task consists of two subtasks.

Produce an Area, Region, or Country Study of a Foreign Country (2.2.1.5.1)

B-31. Units study and provide mission-focused knowledge of the terrain and weather, civil considerations, and threat characteristics for a specified area or region of a foreign country—including the attitudes of the populace and leaders toward joint, multinational, or host-nation forces—to assist in achieving goals and objectives. Studies can also include the views and attitudes of multinational and host-nation forces. Studies provide detailed information, assessments, and conclusions concerning the AOIs of the requesting command or organization.

Produce a Specified Study (2.1.4.5.2)

B-32. Units study and provide focused knowledge of the terrain and weather, civil considerations, and threat characteristics for a specified topic or requirement. Studies provide the requesting command or organization with detailed information, assessments, and conclusions on the AOI. Studies should be as detailed and in-depth as time allows.

LEVERAGE DATA, INFORMATION, AND INTELLIGENCE (2.2.2)

B-33. To leverage data, information, and intelligence to support operations, intelligence professionals must understand the relationship between data, information, and intelligence for situational awareness, situational understanding, and knowledge. Commanders require intelligence about the threat and other aspects of the OE before and during operations—to effectively accomplish their missions—and after operations—to continuously assess the OE and determine if subsequent operations may be imminent.

B-34. *Data* is, in the context of decision making, unprocessed observations detected by a collector of any kind (human, mechanical, or electronic) (ADP 6-0). After data is collected and assigned meaning, it becomes *information*—in the context of decision making, data that has been organized and processed in order to provide context for further analysis (ADP 6-0). Information is obtained through information collection and by using already available information, which units can access through intelligence reach, research, data mining, databases, academic studies, intelligence archives, and PAI. The information and intelligence obtained can be refined into specific knowledge for the conduct of operations.

B-35. Leverage data, information, and intelligence consists of three tasks:

- Create and maintain intelligence databases.
- Conduct intelligence reach.
- Conduct intelligence collaboration.

Note. When leveraging formal national-level intelligence, it is important to understand that these products adhere to analytic intelligence standards and tradecraft principles outlined in the Intelligence Community Directive 203.

Create and Maintain Intelligence Databases (2.2.2.1)

B-36. This task entails creating and maintaining unclassified and classified databases to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task also facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach. It also includes the requirements for formatting and standardization, indexing and correlation, normalization, storage, security protocols, and associated applications. (As technology improves the integration of artificial intelligence, machine learning, and potential autonomous data processing, MI analysts will have greater access to the volume of data/data sets at speeds and durations to improve assessments, enabling decision making.) The following must be addressed in database development, management, and maintenance:

- Data sources.
- Information redundancy.
- Import and export standards.
- Data management and standards (maintaining data literacy).
- Update and backup procedures.
- Data mining, query, and search protocols (executing data sets).

Conduct Intelligence Reach (2.2.2.2)

B-37. Intelligence obtained through *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 (ADP 2-0)—assists the staff in planning and preparing for operations and answering intelligence requirements without the need for the information to pass through a formal hierarchy. The staff can perform the following steps to ensure the optimal use, operability, and effectiveness of intelligence reach:

- Establish data exchange methods and procedures.
- Establish electronic message transfer procedures.

- Establish unit-specific links for identified forces.
- Establish points of contact for the following:
  - Production centers.
  - Combatant command joint intelligence and operations centers.
  - The Defense Intelligence Agency and the U.S. Army Intelligence and Security Command, and its major subordinate commands, such as the National Ground Intelligence Center.
  - Higher MI organizations.
- Ensure the intelligence staff has the necessary personnel, training, automated systems, bandwidth, and resources to conduct intelligence reach.
- Determine information requirements through staff planning.
- Develop production requirements for identified intelligence gaps.
- Obtain geospatial products for the projected AOI.
- Establish and maintain a comprehensive directory of intelligence reach resources before deployment and throughout operations. The value of intelligence reach greatly increases as the staff develops and maintains ready access to rich information resources. These resources are numerous and may include Army, joint, DOD, non-DOD, national, commercial, foreign, and university research programs.
- Know the types of information that intelligence reach resources can provide. Continuously expand the resource directory by identifying new resources.
- Use intelligence reach first to fill intelligence gaps and requirements and to answer requests for information (RFIs). This technique can preclude unnecessary tasking or risk to limited collection assets.
- Strive to maintain continuous situational understanding and anticipate intelligence requirements. Use intelligence reach to answer these requirements and provide the results to the commander and staff for the conduct of operations.
- Exchange intelligence reach strategies with other units, allies, and partners.
- Present the information retrieved through intelligence reach in a usable form; share the information derived from intelligence reach with subordinate, lateral, and higher echelons; and ensure follow-on forces have the information as well.

Conduct Intelligence Collaboration (2.2.2.3)

B-38. Collaboration is the central principle of conducting analysis across intelligence organizations. Army tactical units provide accurate and detailed intelligence about the threat and other relevant aspects of the OE (especially those related to Army activities) through the intelligence enterprise, while other intelligence organizations provide expertise and access not readily available to the Army at the tactical level. Additionally, national-level intelligence organizations provide governance over certain intelligence methods and activities. Cooperation can benefit every echelon.

Perform Intelligence Preparation of the Operational Environment (2.2.3)

B-39. *Intelligence preparation of the operational environment* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an AOI to determine their effect on operations. The G-2/S-2 leads the staff effort and prepares for the IPOE process during pre-mission analysis of the OE associated with force generation and incorporated into the Army design methodology. During this task, the intelligence staff creates data files on specific OEs based on an evaluation of the information and intelligence related to the operational variables identified. IPOE is a continuous staff planning activity undertaken by the entire staff. The staff aims to understand the OE and the options it presents to friendly and threat forces. (See ATP 2-01.3.) Perform IPOE consists of four tasks:

- Define the OE.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat courses of action (COAs).

Define the Operational Environment (2.2.3.1)

B-40. Defining the OE results in identifying significant characteristics of an OE that can affect friendly and enemy operations. Using the operational variables assists the commander in defining relevant aspects of an OE in time and space. The intelligence staff must identify those significant characteristics related to the mission variables of enemy, terrain and weather, and civil considerations that are relevant to the mission and justify that analysis to the commander. Understanding friendly and enemy forces is not enough; other factors, such as culture, languages, tribal affiliations, and operational and mission variables are equally important. Defining the significant characteristics of each operational variable is essential in identifying the additional information needed to complete IPOE.

Describe Environmental Effects on Operations (2.2.3.2)

B-41. The intelligence staff uses operational and mission variables to describe how terrain, weather, and civil considerations affect enemy forces and friendly operations. The entire staff determines the effects to the population of friendly and enemy force actions.

Evaluate the Threat (2.2.2.3)

B-42. This activity analyzes current intelligence to determine how the threat normally organizes for combat and conducts operations. The evaluation includes each threat function as well as potential foreign intelligence elements, criminal organizations, factions, guerrillas, and insurgents. This step focuses on creating threat models and templates that depict how the threat operates across multiple domains when unconstrained by effects of the environment.

Determine Threat Courses of Action (2.2.2.4)

B-43. This activity determines possible threat COAs, describes threat COAs, ranks COAs in probable order of adoption, and, at a minimum, identifies the most probable and the most dangerous threat COAs.

Perform Situation Development (2.2.4)

B-44. Situation development is a process for analyzing information and producing current intelligence concerning the relevant aspects of the OE within the AO before and during operations. The process assists the intelligence officer in recognizing and interpreting indicators of threat intentions and objectives. Situation development confirms or denies threat COAs, provides threat locations, explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness. The locations and actions of noncombatant elements and nongovernmental and other civilian organizations in the AO that may impact operations should also be considered. Through situation development, the intelligence officer quickly identifies information gaps, explains threat activities in relation to the unit's operations, and assists the commander in gaining and maintaining situational understanding. Situation development assists the commander in making decisions, including when to execute branches and sequels.

Provide Intelligence Support to Unique Missions (2.2.5)

B-45. Intelligence supports the staff sections and warfighting function capabilities by applying the intelligence process, IPOE, and information collection. The intelligence process leverages all sources of information and expertise, including the U.S. intelligence community and nonintelligence entities, to provide situational awareness to the commander and staff. Information collected provides insight into hazards within the AO, enemy activities, capabilities, motivations, and objectives, and it enables the conduct of operations. Providing intelligence support to unique missions is designed to support the different unique missions, branches, and activities, such as those listed in table B-1 on page B-12, necessary to successfully execute operations.

Table B-1. Unique mission examples supported by intelligence

Air and missile defense. Intelligence support to air and missile defense provides information and intelligence on the capabilities and limitations of threat aerial and tactical ballistic missile platforms, their locations, and how the threat will organize for combat and conduct operations with these platforms under normal conditions. (See ATP 3-01.16.)
Antiterrorism. Intelligence support to antiterrorism provides timely, accurate, relevant, and predictive intelligence about the terrorist threat to support combating terrorism. The commander uses this intelligence to make better risk decisions when protecting the force during force projection and deployment. This information also provides the necessary targeting information to conduct counterterrorism. (See ATP 3-37.2.)
Aviation. Intelligence support to aviation provides assessments of relevant OE characteristics impacting the employment of Army aviation capabilities and assets. This includes but is not limited to assessing aviation-specific threat considerations, including threat employment of EW capabilities and aviation ground elements, and providing terrain analysis for pick-up zones and helicopter landing zones, air avenues of approach, forward arming and refueling points, engagement areas, and attack by fire/support by fire/battle positions. Additionally, this task provides input to the development of security and deception plans for aviation assets, understanding and tracking aviation weather impacts; input to inform the commander's airframe survivability considerations; and input on the advantages and limitations of aerial reconnaissance and aviation platforms. (See FM 3-04.)
CBRN operations. Intelligence support provides detailed information and intelligence about— • Environmental hazards within the area of responsibility. • Facilities, which, if damaged, could cause secondary hazards. • The adversary's possession of, access to, and capability to employ CBRN weapons or material and under what conditions that adversary is most likely to do so. This information includes— ▪ Capabilities and limitations of adversary CBRN weapons. ▪ Command, control, and release procedures. ▪ Delivery systems. ▪ Medical disease threats. ▪ Technological advancements. ▪ Indicators of intent to employ CBRN weapons. Additionally, CBRN staffs require information about industrial facilities and products stored and produced onsite to make accurate threat and vulnerability assessments from the CBRN perspective.
CA. Intelligence support provides information and intelligence products about civil considerations to support CA operations. Additionally, MI personnel conduct a functional analysis of civil information collected by CA personnel through civil reconnaissance, civil engagement, and civil network development. The analysis and evaluation of civil information that leads to identifying civil strengths and vulnerabilities is a multifaceted problem that requires interbranch coordination, integration, and synchronization. CA personnel— • Collect, collate, and process civil information as part of the civil knowledge integration. • In conjunction with trained intelligence analysts in CA formations, conduct in-depth analysis of civil knowledge to deduce, distinguish, and categorize relationships and networks. • Evaluate and interpret the analysis to assess, predict, validate, and determine the impact of ongoing CA operations and civil-military operations on the commander's overall mission. CA staff officers use this evaluation to create adaptive plans and innovative solutions to the commander's mission challenges and consolidate gains. (See FM 3-57.)
Cybersecurity. The intelligence warfighting function provides information to identify threat capabilities, activities, and TTP. Intelligence assists in identifying threat systems, activities, and procedures that may be vulnerable. (See FM 3-12.)
CEMA. MI organizations provide information to identify threat decision making and command and control nodes, processes, and means in order of criticality. Intelligence also assists in identifying threat systems, activities, procedures that may be vulnerable, and conducting intelligence gain or loss analysis for cyberspace targets with intelligence value. Intelligence support to CEMA increases its capability and leverage to seize, retain, and exploit an advantage over adversaries and enemies in the electromagnetic spectrum. (See FM 3-12.)
EOD. Intelligence support to EOD includes but is not limited to providing information about explosives trends and threats in OEs. Intelligence also supports the exploitation of first seen, modified, and improvised explosive ordnance and systems collected by EOD for technical intelligence purposes. (See ATP 4-32.)
EW. Intelligence support to EW includes providing threat characteristics to support programming unit EW systems, maintaining appropriate threat EW data, ensuring electromagnetic order of battle requirements are part of the information collection plan, determining enemy EW vulnerabilities and high-value targets, and conducting intelligence gain or loss analysis of EW targets of intelligence value. (See ATP 3-12.3.)
Engineers. Intelligence support to engineers includes but is not limited to providing information and intelligence about terrain analysis and threat analysis, including known threat hardened and buried facilities, enemy obstacles and positions, threats to friendly mobility, and threat equipment, capabilities, maneuverability, and TTP. (See ATP 3-34.10.)
Force protection. Intelligence support to force protection includes but is not limited to providing information and intelligence on early warning of a possible attack on friendly forces, foreign intelligence entities, civil disturbances, and continuous threat assessments. (See ADP 3-37.)

Table B-1. Unique mission examples supported by intelligence (*continued*)

Medical. Medical elements require intelligence support to avoid losing medical personnel's protected status under Article 24 of the1949 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field by performing tasks, such as intelligence collection, inconsistent with their noncombatant role. The support required includes determining— • If an enemy plans to use CBRN weaponry or toxic industrial material releases. • Health threats (such as local diseases in humans, animals, insects, and plants; diseases that can be transmitted by food or water; and adverse environmental and occupational conditions). • Health threats in multinational forces. • The health status of enemy forces (including new or exotic diseases). • If there are many enemy prisoners of war or detainees requiring medical care.
Military deception. Intelligence support to military deception provides information and intelligence to support actions executed to deliberately mislead the threat, thereby causing the threat to take specific actions or inactions that support accomplishing the friendly mission. The information and intelligence to support military deception includes but is not limited to information on the enemy's intelligence collection capabilities, intelligence network, intelligence process, biases and perceptions, and reporting channels. (See FM 3-13.4.)
Military information support operations. This requires information and intelligence to support the analysis of foreign target audiences and their environment, including the operational variables. Continuous and timely intelligence are required to assess target audience behavioral trends. Information and intelligence focus on the target audience's motivation and behavior, indicators of progress (or lack of progress) toward achieving measures of effectiveness and measures of performance, and the target audience's reaction to friendly, hostile, and neutral force actions. (See FM 3-53.)
OPSEC. Intelligence support to OPSEC identifies capabilities and limitations of the threat's intelligence system, including adversary intelligence objectives and means, procedures, and facilities that collect, process, and analyze information. This task supports the identification of indicators that adversary intelligence capabilities and systems might detect that could be interpreted or pieced together to obtain friendly information in time to use against friendly forces. (See AR 530-1 and ATP 3-13.3.)
PA. Intelligence support to public affairs entails MI organizations ensuring PA activities do not include controlled unclassified information or classified information or do not expose sources and methods. Additionally, as required for movement, the intelligence staff provides information and intelligence products concerning civil considerations in the area of operations to support PA activities. Commander's communication synchronization process may require some unique intelligence support, such as the current state of the information environment, local communication means and methods, trusted sources, key influencers, established cognitive patterns, cultural norms, perspectives, historical narrative, system of opposition, adversary, and host nation communication capabilities. Intelligence resources contribute to assessing local populations through human factors analysis, influence net modeling, foreign media analysis, media mapping, polling and focus group analysis, and analysis of key communicators and sources of influence. (See JP 3-61.)
Space. Intelligence support to space enhances situational understanding to support intelligence preparation of the OE for multidomain operations in competition below armed conflict, crisis, and armed conflict. Space-focused intelligence analysis assists commanders and staffs in understanding space-environment effects on friendly operations, the adversary's vulnerability to offensive space control operations, and how adversaries may seek to degrade friendly use of space-based capabilities—mainly positioning, navigation, and timing; intelligence, surveillance, and reconnaissance; satellite communications; and meteorology. (See FM 3-14.)
Sustainment. Intelligence support to sustainment includes but is not limited to providing information and intelligence threat analysis on threat dispositions, ports, supply routes, and obstacles affecting freedom of movement. (See ADP 4-0.)

ADP	Army doctrine publication	FM	field manual
AR	Army regulation	JP	joint publication
ATP	Army techniques publication	MI	military intelligence
CA	civil affairs	OE	operational environment
CBRN	chemical, biological, radiological, and nuclear	OPSEC	operations security
CEMA	cyberspace electromagnetic activities	PA	public affairs
EOD	explosive ordnance disposal	TTP	tactics, techniques, and procedures
EW	electromagnetic warfare		

CONDUCT POLICE INTELLIGENCE OPERATIONS (2.2.6)

B-46. *Police intelligence operations* is the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order (FM 3-39). Conducting police intelligence operations is a continuous military police (MP) task, integrated within all MP operations, that supports the operations process and protection activities. Police intelligence operations collect information using police activities for analysis, production, and dissemination to enhance situational understanding, protection, civil control, and law enforcement. Upon analysis, this information may contribute to commander's critical information requirements, intelligence-led

operations, time-sensitive operations, or policing strategies necessary to forecast, anticipate, and preempt crime or related disruptive activities to maintain order.

B-47. *Police intelligence* is the product resulting from the collection, processing, analysis, and integration of criminal intelligence and crime analysis about crime, disorder, criminal activity, and criminal threats (FM 3-39). Police intelligence provides commanders and MPs with a complete picture of the criminal environment. (See FM 3-39.)

B-48. The following provide a framework for and understanding of police intelligence operations:

- *Police information* is information collected during military police operations concerning crime, disorder, criminal activity, and criminal threats (FM 3-39).
- *Crime analysis* is the systematic examination and interpretation of police information to determine when, where, and why crime, disorder, fear of crime, and other destabilizing events occur in specific places (FM 3-39).
- *Criminal intelligence* is police information compiled, analyzed, and disseminated in an effort to anticipate, prevent, or monitor criminal activity (FM 3-39).

Note. Police intelligence operations is not an MI task. However, it is within the *provide support to situational understanding* IWFT that police intelligence operations best supports the operations process and informs the intelligence process. Police intelligence operations is essential to this task, particularly where irregular threats (criminal, terrorist, and insurgent) threaten the security of U.S. forces and military operations. Police intelligence operations supports and enhances the commander's situational awareness and common operational picture through planning and directing, collecting and processing, producing (crime and criminal analysis), and disseminating relevant police intelligence products. Police intelligence operations consists of vital law enforcement and criminal investigation tools that distribute and focus MP and criminal investigation assets. U.S. Codes, executive orders, DOD directives, and Army regulations contain specific guidance regarding the prohibition of intelligence personnel from collecting intelligence on U.S. persons, U.S. corporations, and resident aliens. Any access by the U.S. intelligence community to information or products due to police intelligence operations directed against U.S. persons should undergo competent legal review.

Plan and Direct (2.2.6.1)

B-49. Planning information collection leverages unique DA Criminal Investigation Division and MP capabilities (such as special agents, detention specialists, military working dogs), skills, and knowledge to understand crime environments and organized criminal activity relevant to current and future operations. MPs direct collection assets through the operations process and the Army planning methodologies (Army problem solving, Army design methodology, the MDMP, the rapid decision-making and synchronization process, and troop leading procedures) based on the information collection plan. MPs direct collection assets through the tasking process based on the information collection plan. Collection assets typically consist of organic or attached MP patrols, but they may include other specialty MP personnel such as DA Criminal Investigation Division special agents, detention specialists, or military working dog teams.

Collect and Process (2.2.6.2)

B-50. Collection of police information is a continuous activity. MPs identify gaps in existing police information and develop intelligence requirements. This collection can be completed through several means: MP patrols, police engagement, criminal investigations, collected evidence, database queries, and the use of intelligence reach centers. Collection efforts also assist in enhancing protection operations and antiterrorism by identifying potential criminal threat and other threat activities. (See ATP 3-39.20.)

Produce (2.2.6.3)

B-51. Production involves analyzing collected police information. The police intelligence operations model integrates criminal analysis and crime analysis processes to provide commanders, staffs, and MPs with a complete picture of the criminal environment. Criminal analysis and crime analysis are interdependent and complementary; they are overlapping analysis processes that allow MPs to holistically identify and defeat criminal threats and environmental factors that promote crime, disorder, and the fear of crime. Police information analysis varies based on intelligence requirements and the purpose of the analysis (such as identifying and apprehending a criminal offender, informing the public, enabling protection efforts, or shaping crime prevention strategies to prevent and deter criminal activity).

B-52. Police intelligence products resulting from police intelligence (along with police information) may be produced, grouped, and packaged to fulfill information and intelligence requirements. These products are fed into policing, corrections, and investigative missions through policing strategies and investigative processes as well as into the operations process through the integrating processes (IPOE, information collection, targeting, risk management, and knowledge management). This dissemination allows MP personnel, commanders, and staffs to make decisions ranging from policy, budgeting, and resource allocation to direct tactical action to reduce crime, eliminate crime-conducive conditions, target criminal offenders and networks, and establish safe and secure environments for U.S. forces, allies, and host nations.

Disseminate (2.2.6.4)

B-53. Police intelligence and police information are disseminated for use by law enforcement to focus policing activities. Police intelligence products are disseminated and integrated within the operations process, enhancing situational understanding, mission planning, and execution at every echelon. Dissemination entails delivering timely, accurate, relevant, predictive, and tailored police intelligence products to the appropriate and authorized stakeholders. Dissemination must comply with legal restrictions, mission requirements, and protection considerations. Police intelligence or police information may be provided verbally, in writing, or graphically. These products may be disseminated to support host-nation law enforcement in combating crime and neutralizing criminal threats to military operations based on trend and pattern analysis and shared with other law enforcement agencies. When permitted legally allowable, these products are provided to the MI community for fusion and incorporation into the all-source intelligence effort, contributing to a more complete intelligence picture. (See FM 3-39.)

CONDUCT INFORMATION COLLECTION (2.3)

B-54. *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 that focuses on answering intelligence requirements. Through information collection, commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information, combat information, and intelligence to satisfy intelligence requirements. When necessary, collection assets focus on special requirements, such as personnel recovery. For joint operations, information collection is referred to as intelligence, surveillance, and reconnaissance (also called ISR). Conduct information collection consists of four tasks, as shown in figure B-4 on page B-16. (See FM 3-55.)

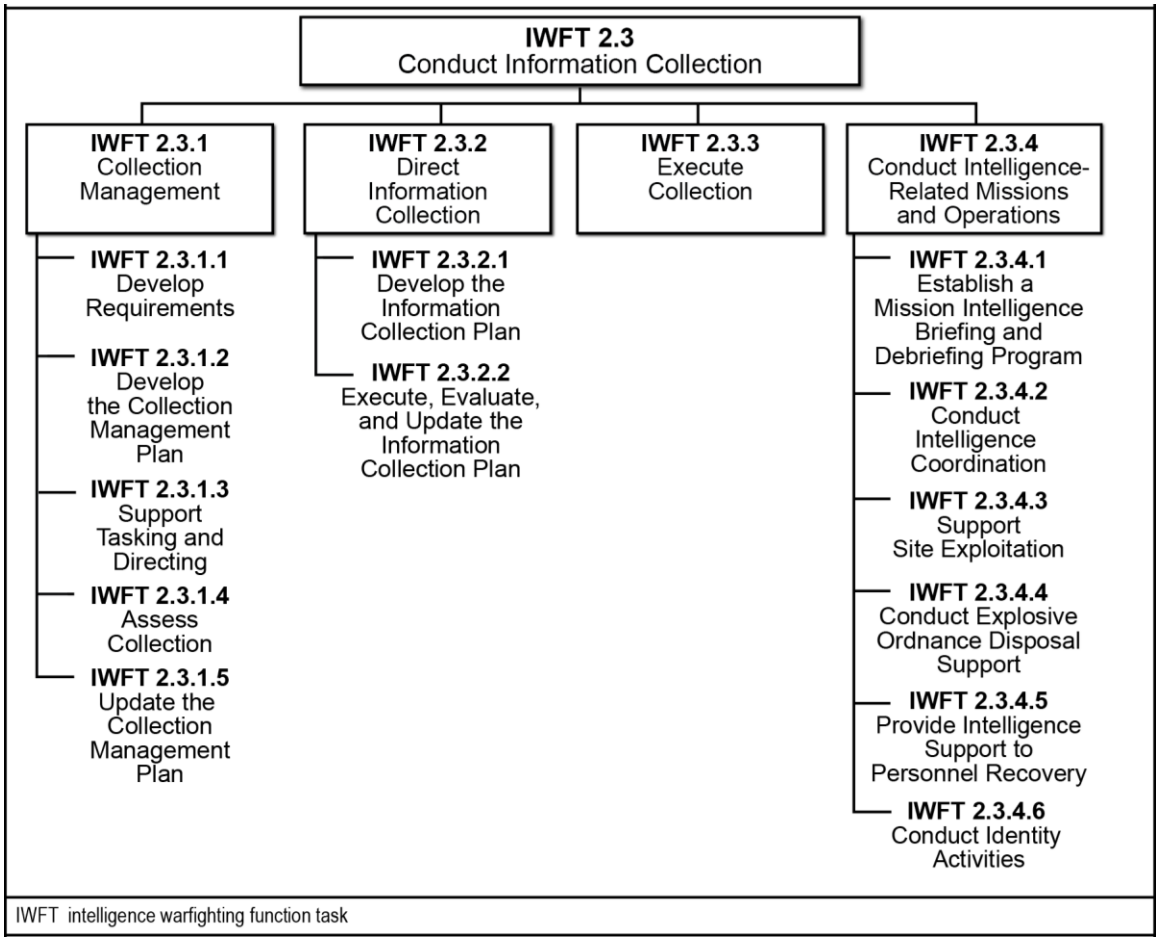


Figure B-4. Conducting information collection

COLLECTION MANAGEMENT (2.3.1)

B-55. *Collection management* is, in intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required (JP 2-0). Collection management is driven by the commander, coordinated by staff effort, and led by the G-2/S-2. The continuous functions of managing collection and identifying intelligence gaps identify the best way to satisfy the supported commander and staff's requirements. These functions are not necessarily sequential. (See ATP 2-01.)

B-56. The intelligence staff (in collaboration with the operations officer and the entire staff) receives and validates requirements for collection, prepares the collection management plan, recommends collection assets and capabilities to the operations staff, and maintains synchronization as operations progress.

B-57. Collection management ensures information collection, intelligence reach, and RFIs successfully report, produce, and disseminate information, combat information, and intelligence to support decision making. Collection management includes the following tasks:

- Develop requirements.
- Develop the collection management plan.
- Support tasking and directing.
- Assess collection.
- Update the collection management plan.

Develop Requirements (2.3.1.1)

B-58. The intelligence staff develops a prioritized list of requirements that focuses on what information it needs to collect to produce intelligence. Additionally, the intelligence staff dynamically updates and adjusts the requirements in response to mission adjustments and changes. Each requirement is assigned a latest time information is of value (also called LTIOV) to meet operational requirements.

Develop the Collection Management Plan (2.3.1.2)

B-59. Developing the collection management plan involves integrating and synchronizing collection assets and addressing intelligence requirements through proposed information collection tasks such as the concept of operations and scheme of maneuver. The entire staff must cooperate and collaborate. The collection management plan is the primary input in the development of the information collection plan, as captured in Annex L (Information Collection). The collection management plan is updated as planning changes or the operation evolves. Developing the collection management plan includes evaluating collection assets; developing a collection strategy; developing collection management tools, which graphically represent the collection strategy; and drafting partial Annex L (Information Collection) for staffing.

Support Tasking and Directing (2.3.1.3)

B-60. To support the G-3/S-3 in tasking and directing collection assets, the collection management team provides the collection management plan to the operations staff. The collection management plan is the basis (compiling all requirements and planning collection against those requirements) for the information collection plan. The collection management plan consists of the three collection management tools, at a minimum, and any other useful products, such as a collection emphasis message at higher echelons. The operations staff adds some details to the collection management plan and publishes the information collection plan within the order as Annex L (Information Collection). The collection management plan addresses all available assets and requests for collection from higher or adjacent units, as well as the coordinating mechanisms required to ensure collection coverage.

Assess Collection (2.3.1.4)

B-61. The commander and staff continuously evaluate the information collection plan based on the assessment of results from reconnaissance missions, surveillance tasks, intelligence operations, and security operations. Assessing collection is particularly important during execution because situations change rapidly; it identifies updates for information collection activities. Together, commanders and staffs determine if requirements have been satisfied or are still relevant:

- If requirements have been satisfied or are no longer relevant, they are eliminated from the information collection plan.
- If requirements have not been satisfied but are still relevant, the intelligence staff coordinates with the operations staff during the information collection working group for additional assets and/or recommends adjustments to the current coverage.

Update the Collection Management Plan (2.3.1.5)

B-62. Collection management is continuous, collaborative, and interactive. As such, updating the collection management plan as the situation changes keeps information collection synchronized with current operations, thus ensuring an effective information collection effort. Keeping the plan current requires constant coordination among all staff members. When the commander designates a requirement as satisfied, the collection management team deletes that requirement so that collectors remain focused on unanswered and new requirements. Success results in the collection and reporting of timely and relevant information to support the commander’s decisions.

DIRECT INFORMATION COLLECTION (2.3.2)

B-63. The operations staff integrates collection assets through a deliberate and coordinated effort across all warfighting functions. Tasking and directing information collection are vital in controlling limited collection assets. During tasking and directing information collection, the staff recommends cueing, redundancy, and mix as appropriate. Staffs task information collection by issuing WARNORDs, fragmentary orders, and operation orders. They direct collection assets by continuously monitoring the operation. Staffs conduct retasking to refine, update, or create new requirements. Tasking and directing information collection include two tasks:

- Develop the information collection plan.
- Execute, evaluate, and update the information collection plan.

Develop the Information Collection Plan (2.3.2.1)

B-64. The operations officer develops the information collection plan. The entire staff analyzes each requirement to determine how best to satisfy each requirement. The staff receives information collection tasks and RFIs from subordinate and adjacent units and higher headquarters. The information collection plan includes all assets that the operations officer can task or request and coordinating mechanisms to ensure adequate coverage of the AOI.

Execute, Evaluate, and Update the Information Collection Plan (2.3.2.2)

B-65. The evaluation of reporting, production, and dissemination identifies updates for the information collection plan. As the current tactical situation changes, staffs adjust the overall information collection plan to synchronize collection tasks. This optimizes collection and exploitation capabilities. The staff constantly updates requirements to ensure the information collection effort synchronizes with current operations and supports future operations planning. As collected information answers requirements, the staff updates the information collection plan.

EXECUTE COLLECTION (2.3.3)

B-66. Executing collection focuses on requirements connected to the execution of tactical missions (reconnaissance, surveillance, security operations, and intelligence operations) based on the intelligence requirements. Collection activities acquire information about the adversary and the AO, and they provide that information to intelligence processing and exploitation elements. Typically, collection activities begin soon after the receipt of mission and continue throughout the preparation and execution of the operation. They do not cease at the conclusion of the mission but continue as required. This allows the commander to simultaneously focus combat power, execute current operations, and prepare for future operations.

CONDUCT INTELLIGENCE-RELATED MISSIONS AND OPERATIONS (2.3.4)

B-67. The associated intelligence tasks (such as *intelligence support to personnel recovery*) facilitate conducting reconnaissance and surveillance. These tasks also include specialized missions (such as the exploitation of a sensitive site) that provide information and intelligence outside the traditional information collection construct. Conduct intelligence-related missions and operations includes six tasks:

- Establish a mission intelligence briefing and debriefing program.
- Conduct intelligence coordination.
- Support site exploitation.
- Conduct explosive ordnance disposal support.
- Provide intelligence support to personnel recovery.
- Conduct identity activities.

Establish a Mission Intelligence Briefing and Debriefing Program (2.3.4.1)

B-68. Commanders establish, support, and allocate appropriate resources for a mission intelligence briefing and debriefing program. Conducting battle updates and after action reviews are separate tasks from the mission briefing and debriefing program. This task has two subtasks.

Establish a Mission Intelligence Briefing Plan (2.3.4.1.1)

B-69. The intelligence section develops a mission intelligence briefing plan. It identifies information that Soldiers conducting patrols should seek. The plan ensures all Soldiers conducting engagements, patrols, tactical movements, and nontactical movements are sensitized to specific information and reporting requirements, information gaps, and unique mission requirements. The mission intelligence briefing and debriefing generally follow the format of a mission briefing: review the route traveled, patrol collection objectives, and methods employed.

Establish a Debriefing Plan (2.3.4.1.2)

B-70. The intelligence section develops a complementary debriefing plan and coordinates for human intelligence support, when appropriate. The debriefing plan captures information related to the specific information requirements the patrol collected on and any additional information and observations the patrol made concerning the OE. It also includes collected information, such as fliers, pamphlets, media, or pictures, the patrol found or obtained. The plan should involve all returning patrols and leaders who traveled to meetings, returning human intelligence collection teams, aircrews, and others who may have obtained information of intelligence value. The intelligence section debriefs personnel; debriefers then write and submit reports or verbally report information, as appropriate. The requirement for an intelligence section debriefing following each mission should be included in the mission intelligence briefing. Leaders should not consider a mission complete and release personnel until the reporting and debriefing are complete.

Conduct Intelligence Coordination (2.3.4.2)

B-71. The intelligence section conducts intelligence coordination to facilitate active collaboration laterally and vertically. This includes establishing and maintaining technical channels to refine and focus the intelligence disciplines on the information collection tasks. It also properly coordinates intelligence discipline collection assets when operating in another unit's AO. Conduct intelligence coordination includes two subtasks.

Ensure Proper Authorities and Deconflict Authorities, When Necessary (2.3.4.2.1)

B-72. When necessary, intelligence operations should be coordinated with and supported by the proper authorities. For example, during cyberspace operations, a resource can be contested between Title 10, USC, and Title 50, USC, operations; therefore, deconfliction of the resource is crucial.

Establish and Maintain Technical Authority and Channels (2.3.4.2.2)

B-73. Intelligence commanders and intelligence staffs maintain control of each intelligence discipline during operations through technical channels to 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. laws, the law of war, international laws, DOD directives, DOD instructions, and orders. Although commanders direct operations, they often rely on the intelligence section's technical expertise to conduct portions of 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 guiding the use of specific collection assets.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Coordinating operations.
- Directing specialized training for specific MI personnel or units.

Conduct Deconfliction and Coordination (2.3.4.2.3)

B-74. Conducting deconfliction and coordination consists of a series of related activities that facilitate operations in another unit's AO. These activities facilitate successful information collection, support the operation, and support fratricide avoidance. MI organizations may be used in general support for coverage of an AO or in direct support to a specific unit. MI organizations operating in general support should coordinate with unit commanders when operating in that unit's AO. At a minimum, the MI organizations should announce

their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission; organizations should conduct a thorough face-to-face coordination. An MI organization operating in direct support of a specific unit coordinates with the unit for augmentation to conduct operations in accordance with force protection requirements. The MI organization's leader also coordinates with the supported unit's intelligence section to debrief returning members, convoy leaders, and others.

Support Site Exploitation (2.3.4.3)

B-75. *Site exploitation* is the synchronized and integrated application of scientific and technological capabilities and enablers to answer information requirements, facilitate subsequent operations, and support host-nation rule of law (ATP 3-90.15). Generally, a site is a location that potentially contains valuable information. While the physical process of exploiting the site begins at the site itself, full exploitation may involve teams of experts located worldwide. (See ATP 3-90.15.)

Conduct Explosive Ordnance Disposal Support (2.3.4.4)

B-76. *Explosive ordnance disposal* is the detection, identification, on-site evaluation, rendering safe, exploitation, recovery, and final disposal of explosive ordnance (FM 4-30). Explosive ordnance disposal or the combined explosive ordnance disposal joint task force provides support to the intelligence warfighting function. This task enables synchronizing the information collection tasks conducted during explosive ordnance missions, site exploitation, developing technical intelligence and other intelligence based on collected information from explosive ordnance disposal incident scene collection, and distributing intelligence to support targeting and tactics, techniques, and procedures adjustments. (See ATP 4-32.)

Provide Intelligence Support to Personnel Recovery (2.3.4.5)

B-77. *Army personnel recovery* is the military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel (FM 3-50). Intelligence support to personnel recovery consists of intelligence activities and capabilities focused on gathering information to recover and reintegrate U.S. personnel—whether Soldier, Army Civilian, selected DOD contractor, or other personnel as determined by the Secretary of Defense—who are isolated in a specific AO. This support also includes developing thorough analysis, detailed products, and estimates to support isolated Soldier guidance and Army personnel recovery coordination measures. (See FM 3-50.)

Conduct Identity Activities (2.3.4.6)

B-78. Identity activities refer to a collection of functions and actions that appropriately recognize and differentiate one person or persona from another person or persona to support decision making as well as security, force protection, and law enforcement. They include the collection, processing, and exploitation of identity attributes and physical materials to inform policy and strategy development, planning, and assessment and to enable prosecution and the appropriate action at the point of encounter. Some of this data and information can inform all-source analytic efforts, leading to the production of I2.

B-79. *Identity intelligence* is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0). I2 is used to disrupt competitors, support joint operations, counter threats, deny anonymity to the Nation's adversaries, and protect the Nation's assets, facilities, and forces. Units and organizations use I2 products informed by capabilities such as biometrics, forensics, and document and media exploitation as well as information from the intelligence disciplines.

B-80. I2 is currently produced at echelons corps and above from the fusion of all-source and multidisciplined reporting. It results in intelligence from the human dimension, which encompasses the interaction among individuals and groups, how they understand information and events, make decisions, generate will and act within an OE. Intelligence analysts use I2 products to identify relevant actors and provide intelligence that allows a commander to anticipate those actors' behaviors and the potential consequences of their behaviors. *Relevant actors* refer to actors who could substantially impact campaigns, operations, or tactical actions. Understanding this human element across the strategic contexts is essential to commanders' efforts to defeat, destroy, deny, or disintegrate the enemy.

PROVIDE INTELLIGENCE SUPPORT TO TARGETING (2.4)

B-81. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Intelligence support to targeting provides the commander and staff the information and intelligence needed to support targeting actions. The intelligence cell (supported by the entire staff) provides the fire support coordinator, public affairs officer, cyberspace electromagnetic warfare officer, space support element, and other staff officers with information and intelligence for targeting threat forces and systems with direct and indirect fires to create effects (through lethal and nonlethal means). The information and intelligence include identifying threat capabilities and limitations. The Army's targeting process uses the decide, detect, deliver, and assess (also called D3A) methodology. The intelligence officer provides accurate, current intelligence and information to the staff and ensures the information collection plan supports the finalized targeting plan. intelligence support to targeting consists of three tasks, as shown in figure B-5. (See FM 3-60.)

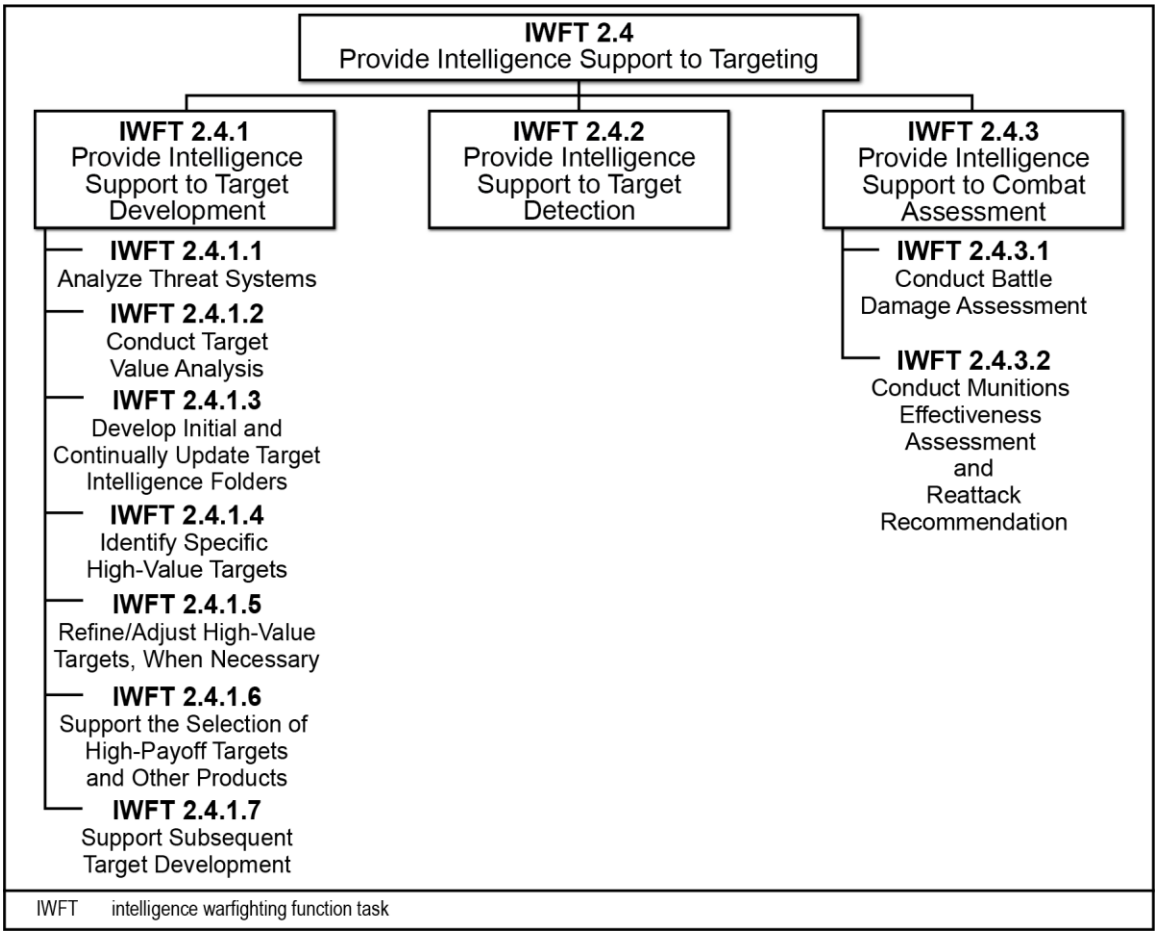


Figure B-5. Providing intelligence support to targeting

PROVIDE INTELLIGENCE SUPPORT TO TARGET DEVELOPMENT (2.4.1)

B-82. *Target development* is the systematic examination of potential target systems—and their components, individual targets, and even elements of targets—to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objectives (JP 3-60). Target development involves the systematic analysis of threat forces and operations to determine high-value targets (HVTs) (people, organizations, or military units the threat commander requires for successful completion of the mission), high-payoff targets (HPTs) (people, organizations, or military units whose loss to the enemy contributes significantly to the success of the friendly COA), and systems and system

components for potential engagement through maneuver, fires, electronic means. The following are the tasks of intelligence support to target development:

- Analyze threat systems.
- Conduct target value analysis.
- Develop initial and continually update target intelligence folders.
- Identify specific HVTs.
- Refine/Adjust HVTs, when necessary.
- Support the selection of HPTs and other products.
- Support subsequent target development.

Analyze Threat Systems (2.4.1.1)

B-83. Friendly forces cannot target threat forces and capabilities without understanding threat systems—from the most general level to very detailed target elements (a macro to micro approach). This effort results in intelligence that is pushed from the joint force and theater army down to the battalion level. The analysis of threat systems focuses on breaking down target systems into successive elements at a greater level of detail to eventually identify HVTs and HVT elements. The resulting products and the development of threat models support subsequent and more detailed target development.

Conduct Target Value Analysis (2.4.1.2)

B-84. *Target value analysis* refers to a methodology that assists in prioritizing HVTs and identifies potential HVT sets with a given tactical situation. It is led by the fire support element/fires cell as part of targeting that quantifies the relative value of HVTs with each other in relation to a threat operation. This analysis is based in part on the conclusions reached by the intelligence staff after evaluating threat characteristics. Target value analysis continues the detailed analysis of relevant threat factors, including doctrine, tactics, equipment, capabilities, and expected actions for a specific threat COA.

Develop Initial and Continually Update Target Intelligence Folders (2.4.1.3)

B-85. Army intelligence targeting elements develop and refine target intelligence folders to account for HVTs, HPTs, or systems and system components based on the continuous targeting process. Target intelligence folders consist of two components: target intelligence packages and work folders. When not covered by joint target folders, theater army G-2 requirements, standards, and unit standard operating procedures (also called SOPs) set the standard for Army target intelligence packages. As required, target development elements develop target intelligence packages using specific intelligence products and analysis from the corps or division analysis and control element, tailored to the user. Target intelligence folders are both offensive and defensive in nature and subsequently updated throughout operations to further detail information and intelligence over time. This results in updates to target intelligence packages.

B-86. If a unit or organization anticipates requesting support from a higher-level organization for nonlethal means or intelligence collection, the unit or organization should develop detailed target intelligence folders in the higher-level organization's required format. This effort requires additional time. For example, requesting support from the U.S. Space Command or the U.S. Cyber Command requires a greater level of detail within products to meet their requirements.

Identify Specific High-Value Targets (2.4.1.4)

B-87. HVTs are developed during step 3 (evaluate the threat) and initially refined during step 4 (determine threat COAs) of the IPOE process—an integrated process of step 2 (mission analysis) of the MDMP. (See paragraphs B-39 through B-43.) Outputs from step 3 include the threat template, HVT list, and threat capability statement. Step 4 requires an understanding of the threat characteristics, as well as the effects of terrain, weather, and civil considerations on operations. (See ATP 2-01.3.) The most important element in determining threat COAs is understanding threat operational art and tactics.

Refine/Adjust High-Value Targets, When Necessary (2.4.1.5)

B-88. During step 3 of the MDMP, the intelligence targeting element, as part of the targeting working group, refines the HVT list one last time based on the most current intelligence and analysis. The entire staff conducts further analysis, including another iteration of target value analysis. Conducting target value analysis assists the staff in prioritizing HVTs and identifying potential HVT sets for each threat COA. HVTs are placed in order of their relative worth to the threat's operation and recorded as part of the threat model. The value of HVTs varies over the course of an operation. The entire staff analyzes and identifies those HVTs that must be attacked to ensure friendly mission success. Additionally, the staff analyzes all implications of attacking those HVTs and possible threat counteractions. The HVT list is the result of this analysis. Those critical HVTs that the staff confirms as acquired and attacked are nominated as potential HPTs for each COA.

Support the Selection of High-Payoff Targets and Other Products (2.4.1.6)

B-89. HPTs are critical to both the adversary's needs and the friendly concept of operations. They support achieving the commander's intent and executing the concept of operations. HPTs are determined based on the commander's targeting guidance. Upon receipt of HPT nominations, the staff groups the HPTs into a prioritized HPT list, associating the HPTs to a specific point in the battle. HPTs are incorporated into the scheme of fires and used to develop target selection standards, attack guidance matrices (AGMs), and target synchronization matrices for each friendly COA. The HPT list, target selection standards, AGMs, and target synchronization matrices are later refined during step 4 (COA analysis) and finalized during step 6 (COA approval) of the MDMP.

Support Subsequent Target Development (2.4.1.7)

B-90. After the MDMP, more detailed target development occurs. Some aspects of subsequent target development—such as target validation and dynamic target development—overlap with intelligence support to target detection. The intelligence target element is not the lead element for developing most of the subsequent target development products.

Provide Intelligence Support to Target Detection (2.4.2)

B-91. The targeting working group establishes target detection and tracking priorities based on targeting priorities. The information collection plan aligns collection assets to named areas of interest and target areas of interest that support the execution of the AGM. Target tracking is inherent in target detection. The fire support element/fires cell provides the intelligence cell with the degree of accuracy required and dwell time for a target to be eligible for engagement. The collection manager can then match those requirements to the *target location error*—the difference between the coordinates generated for a target and the actual location of the target (JP 3-09.3)—of the collection asset. Executing the information collection plan begins as early as possible during planning and continues through the assess function of the Army's targeting process and even assists in transitioning unit operations into the next mission. Executing the information collection plan to answer targeting intelligence requirements is central to detection. Targets are detected by using the appropriate collection assets.

B-92. The current operations integration cell is the primary cell responsible for directing the execution of the information collection effort to detect HPTs. The unit intelligence cell (with the current operations integration cell) must focus intelligence analysis efforts to support both situation development and the targeting effort.

Provide Intelligence Support to Combat Assessment (2.4.3)

B-93. *Combat assessment* is the determination of the overall effectiveness of force employment during military operations (JP 3-60). The commander uses combat assessment to determine if targeting actions have met the attack guidance and, if reattack is necessary, to perform essential fires tasks and achieve the commander's intent for fires. Intelligence supports the assessment activity of the operations and targeting processes. Combat assessment is composed of three related elements: battle damage assessment (BDA), munitions effectiveness assessment (MEA), and reattack recommendations.

Conduct Battle Damage Assessment (2.4.3.1)

B-94. *Battle damage assessment* is the estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of fires (JP 3-0). BDA includes known or estimated enemy unit strengths; degraded, neutralized, or destroyed enemy weapons systems; and all known captured, wounded, or killed enemy personnel during the reporting period. BDA in targeting pertains to the results of lethal and nonlethal engagements on targets designated by the commander.

B-95. The intelligence staff, in coordination with the rest of the staff, determines how combat assessment relates to specific targets by completing BDA, which includes physical damage and functional damage assessments. Producing BDA is primarily an intelligence cell responsibility but requires coordination across the staff, similarly to IPOE and most steps of intelligence support to targeting. BDA requirements should be captured as PIRs or as similar high-priority information collection requirements. Together, BDA and MEA provide the commander and staff with an assessment of the effects achieved against targets and whether the targeting guidance was met. Based on this information, the staff can recommend reattacks when necessary.

Conduct Physical Damage Assessment (2.4.3.1.1)

B-96. *Physical damage assessment* is the estimate of the quantitative extent of physical damage to a target resulting from the application of military force (JP 3-60). The staff conducts a physical damage assessment to estimate the extent of physical damage to a target based on observed or interpreted damage. Physical damage assessment is a post-attack target analysis coordinated among all units and the entire staff.

Conduct Functional Damage Assessment (2.4.3.1.2)

B-97. *Functional damage assessment* is the estimate of the effect of military force to degrade or destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target (JP 3-60). The staff conducts a functional damage assessment for the threat's remaining functional or operational capabilities. The assessment focuses on measurable effects. It estimates the threat's ability to reorganize or find alternative means to continue operations. The targeting working group and staff integrate analysis with external sources to determine if the commander's intent for fires has been met.

Conduct Munitions Effectiveness Assessment and Reattack Recommendation (2.4.3.2)

B-98. *Munitions effectiveness assessment* is the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness (JP 2-0). The G-3/S-3, in coordination with the fires cell and the targeting working group, conducts MEA concurrently with BDA and uses MEA to recommend an increase in the effectiveness of—

- The methodology.
- Tactics.
- Weapons systems.
- Munitions.
- Weapons delivery parameters.

B-99. The G-2/S-2, G-3/S-3, and fire support coordinator/fire support officer use BDA and MEA results to determine if operational objectives were achieved and make recommendations to the commander. *Reattack recommendation*—an assessment, derived from the results of battle damage assessment and munitions effectiveness assessment, providing the commander systematic advice on reattack of a target (JP 3-60)—and other recommendations must address objectives relative to targets, target critical elements, target systems, enemy combat force strengths, and friendly maneuver.

B-100. Future target nominations and reattack recommendations merge the picture of what was done (BDA) with how it was done (MEA) and compare results with predetermined measures of effectiveness developed at the start of the targeting process. This determines the degree of success in achieving objectives and formulating any required follow-up actions or indicates readiness toward new tasks to achieve overall objectives.

Appendix C

Force Projection Operations Considerations

FORCE PROJECTION THREATS

C-1. *Force projection* is the ability to project the military instrument of national power from the United States or another theater in response to requirements for military operations (JP 3-0). It is the military component of power projection and a central element of the national military strategy. Army organizations and installations linked with joint forces and industry form a strategic platform to maintain, project, and sustain Army forces wherever they deploy. Force projection operations are inherently joint and require situational understanding and detailed planning and synchronization.

C-2. During force projection, peer threats can apply strategic and operational reach to contest Army deployments; in terms of the most dangerous COAs, they can employ devastating lethal and nonlethal capabilities across multiple domains. Gaining situational understanding of threat intentions and activities across force projection processes can present challenges for deploying units since their assigned intelligence collection assets are transitioning from home station to forward theaters, and intelligence analysis may be focused on understanding threats in the forward theater operational areas.

C-3. Peer threats possess the capability and capacity to observe, disrupt, delay, and attack U.S. forces at any stage of force projection, including while still positioned at home stations in the United States and while overseas. (See FM 3-0.) The Army relies on various interdependent infrastructures, most of which it does not own or operate. This makes the Army's domestic operations rely heavily on external resources susceptible to a multitude of lethal and nonlethal threat methods and capabilities leveraged across one or more domains. Leveraged threat methods and capabilities include but are not limited to—

- Conducting lethal and nonlethal attacks against units posturing for deployment.
- Conducting persistent, multidomain information collection on Army forces, training, and installations.
- Conducting information warfare operations against local communities, Service members, DOD civilians, contractors, and Soldiers' Family members:
  - Targeted threats through social media, email, or other means designed to frighten and distract deploying Soldiers and their Families.
  - Cyberspace attacks against Soldier and Family member bank and credit agencies, impeding or disrupting access to personal funds.
  - Cyberspace attacks against civilian infrastructure (including transportation, supply, fuel, and navigation) used to support military operations.
  - Targeted strikes against defense communications infrastructure to disrupt communications between units, installations, and other unified action partners that assist deployment.
- Disinformation dissemination and misinformation support designed to—
  - Undermine the legitimacy of or reduce support for U.S. Government action.
  - Incite civil unrest in local communities and along road and rail lines of communications that deploying forces need or plan to use to reach ports of embarkation.
  - Reduce trust in future official communications from government, law enforcement, or military officials by releasing disinformation that appears genuine but contains incorrect or confusing information.
- Conducing infrastructure sabotage using pre-positioned agents in the U.S. homeland or theater.

C-4. Peer threat objectives and advantages may not be immediately recognized since the effects of peer threat activities may appear over prolonged time windows. By using a range of military and nonmilitary activities, a peer threat can use various instruments of national power to further its interests and contest Army force projection processes. The adversary's use of diplomatic, information, economic, and military activities shape the OE well before armed conflict by gaining situational awareness of, detecting, and even deterring Army force projection processes. In crisis, peer threats may seek to delay or disrupt friendly forces moving from the U.S. homeland to overseas theaters long enough to achieve their goals in forward theaters. During armed conflict, peer threats may seek to inflict significant damage to or deny or defeat Army forces in the deployment phase or at home station before Army forces reach their assigned operational area or debarkation location. Army forces must evaluate the peer threat's ability to contest U.S. force deployment and home station activities in all domains and across the Army strategic contexts.

C-5. Nonpeer or opportunistic threats may attempt to detect, deter, delay, or defeat Army forces conducting CONUS and OCONUS force projection processes. These threats may be inspired or influenced by peer threats and attempt to take advantage of peer threat associated contested deployment activities to advance their own goals. Peer threat, nonpeer threat, or other opportunistic threat actions may use the same methods, making attribution difficult.

C-6. Because threat forces may attempt to disrupt one or more force projection processes, G-2/S-2s must continuously leverage the intelligence enterprise to maintain visibility of potential threats to force projection processes in CONUS and OCONUS territories. Close collaboration between the deploying unit; the installation; appropriate federal, state, and local agencies (both government and law enforcement); and USAR and ARNG elements is critical in mitigating threat activities leveraged to disrupt force projection. G-2/S-2s and other staff members must consider incorporating strategies into planning and training to mitigate the potential for threat activities during force projection. Key planning and training considerations include but are not limited to—

- Local, state, and federal authorities able to mitigate deployment disruptions.
- Coordination and relationship building with local, state, and federal civilian law enforcement agencies to ensure effective movement control from fort to port.
- Understanding about critical infrastructure vulnerable to sabotage and unsuited for the movement of heavy equipment along surface (road and rail) lines of communications.
- Using alternate railheads and marshalling yards as well as multiple lines of communication to reach ports of embarkation.
- Developing alternate surface transportation options to deliver unit equipment to a seaport of embarkation when rail service is degraded or disrupted.
- Establishing fuel, maintenance, and rest locations along lines of communications.
- Implementing a communications plan that informs the public while maintaining OPSEC.
- Establishing specific cyberspace defenses for systems and associated data used to support movement.

C-7. G-2/S-2s, in conjunction with the intelligence enterprise, perform IPOE for threat activities associated with force projection processes. Additionally, G-2/S-2s conduct intelligence reach to AISE and theater intelligence units and organizations to inform deployment-related IPOE and address information gaps concerning threats to movement into a specific theater. Conversely, AISE and theater intelligence units and organizations conduct activities to support their intelligence operations, analysis, activities, and anticipated intelligence requirements for Army forces conducting force projection processes. AISE and theater intelligence units and organizations can support force projection processes by—

- Providing situational understanding of the threat's attempt to gain and/or maintain positions of relative advantage associated with force projection activities.
- Detecting indicators of imminent threat activities.
- Providing an understanding of enemy intentions.
- Tracking enemy activities and capabilities across domains and dimensions.

INTELLIGENCE SUPPORT TO FORCE PROJECTION

C-8. Unstable conditions worldwide often reduce or limit the amount of time required to produce intelligence to meet contingency operation requirements. Therefore, MI units and staffs prepare for potential contingencies by building intelligence readiness daily, including their skills and systems expertise. When a unit receives a WARNORD for deployment or is assigned a contingency mission, the unit conducts pre-mission analysis of the projected AOI.

C-9. Built on a foundation of intelligence readiness, the intelligence warfighting function provides the commander with the intelligence needed to conduct force projection operations. Successful intelligence during force projection operations relies on continuous collection and intelligence production before and during the operation. During force projection operations, higher echelons provide intelligence to lower echelons until the early-entry force secures the lodgment area. The J-2 begins to set the theater, exercising. judgment when providing information to subordinate intelligence staffs to avoid overwhelming them.

C-10. Key planning considerations for intelligence in force projection include—

- Staying out front in intelligence planning:
  - Begin pre-mission analysis of the OE as soon as possible.
  - Develop a steady effort.
  - Prioritize information requirements to develop the initial intelligence requirements.
  - Identify intelligence training requirements (including augmentees).
- Understanding how to get intelligence support:
  - Understand the combatant command and deployed force intelligence architecture.
  - Identify asset, sensor, and intelligence PED requirements.
  - Identify personnel augmentation requirements.

C-11. Intelligence leaders anticipate, identify, consider, and evaluate all threats to the unit throughout force projection operations. This is critical during the deployment and entry operations stages of force projection. During these stages, the unit is particularly vulnerable to threat actions because of its limited combat power and knowledge of the AO. Therefore, intelligence professionals emphasize providing combat information and intelligence products that indicate changes to the threat or relevant aspects of the OE. Intelligence leaders should—

- Review available databases on assigned contingency areas, begin collaboration and pre-mission analysis of the OE, and develop initial IPOE products concerning the AOIs.
- Comply with regulatory guidelines for conducting specific intelligence operations.
- Coordinate for and rehearse using the same communications protocols that the joint force, higher headquarters, and subordinate and lateral units use when deployed.
- Plan, train, and practice surging intelligence analysis on regionally aligned, likely, or developing contingencies.
- Prepare and practice coordination with other elements and organizations such as—
  - Intelligence units and analytical elements.
  - Information operations officers.
  - The USAF SWO. (See JP 3-59 and AR 115-10.)
  - CA elements and units. (See FM 3-57.)
  - Military information support operations elements and units. (See FM 3-53.)
  - Space support elements. (See FM 3-14.)
  - Special forces elements and units. (See FM 3-05 and FM 3-18.)
- Include the following as a part of daily (sustainment) operations:
  - A linguist plan with proficiency requirements.
  - Training (individual and collective), including augmentees.
  - Appointed and trained foreign disclosure personnel.
- Establish formal or informal intelligence links, relationships, and networks to meet developing contingencies.

- Conduct analysis of threats, terrain and weather, and civil considerations or submit RFIs in accordance with unit SOPs.
- Determine the need for additional civil considerations and sociocultural research and pre-mission analysis of the OE.
- Establish statements of intelligence interests and develop production and warning requirements.

C-12. Intelligence leaders support peacetime contingency planning with intelligence knowledge and IPOE products and databases on likely contingency areas. Intelligence leaders, with the G-2/S-2 and G-3/S-3, establish an information collection plan implemented upon alert notification. For a smooth transition from predeployment to entry, intelligence leaders must coordinate an intelligence architecture. To support information collection, the intelligence staff identifies requirements, including—

- Collection assets providing support throughout the AOI.
- The intelligence PED required to support collection assets, including the use of expeditionary or reach intelligence PED to best support the requirements of the operation.
- Command and support relationships.
- Report and request procedures not covered in unit SOPs.
- Deployment sequence of information collection personnel and equipment. Early deployment of key information collection personnel and equipment is essential for force protection and operations. The composition of initial and follow-on deploying assets is influenced by the mission variables (METT-TC [I]), availability of communications, and availability of lift.
- Communications architectures supporting both intelligence staffs and collection assets.
- Friendly vulnerabilities to hostile intelligence threats and plans for conducting force protection. The staff must begin this planning as early as possible to ensure adequate support to force protection of deploying and initial-entry forces.
- TPFDD requirements. When necessary, the staff should recommend changes to priority of movement, unit, or capability to enable information collection.

C-13. Intelligence leaders continually monitor and update applicable plans and orders to reflect the evolving situation, especially during crisis. National intelligence activities monitor regional threats worldwide and can answer some intelligence requirements supporting the development of plans and orders.

FORCE PROJECTION SUBPROCESSES

C-14. Force projection is the enabler of the Army's expeditionary capability. It is a process that ultimately involves unified action. This requires organizing combat power through force tailoring, task organization, and mutual support. The five subprocesses of force projection are—

- Mobilization.
- Deployment.
- Employment.
- Sustainment.
- Redeployment.

MOBILIZATION

C-15. *Mobilization* is the process by which the Armed Forces of the United States, or part of them, are brought to a state of readiness for war or other national emergency (JP 4-05). This is also the point where the intelligence staff begins conducting the tasks required to set the theater. It assembles and organizes resources to support national objectives. (See ADP 4-0.)

C-16. The intelligence staff updates estimates, databases, IPOE products, and other intelligence products required to support command decisions on force composition and deployment priorities and sequence. Units reassess their collection requirements immediately after alert notification. The intelligence staff begins verifying planning assumptions within the OPLAN. The intelligence staff, with CI personnel support, provides force protection support and recommends antiterrorism measures.

C-17. During mobilization, intelligence leaders—

- Monitor intelligence reporting on threat activity, civil considerations, and warning data.
- Manage information requirements and RFIs from the unit and subordinate units, to include updating information collection planning.
- Establish habitual training relationships with augmentation units and personnel as well as higher echelon intelligence organizations identified in the existing OPLAN.
- Support augmentation units and personnel by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify information collection and intelligence PED force requirements for the different types of operations and contingency plans.
- Identify individual military, civilian, and contractor augmentation requirements.

C-18. During mobilization, intelligence leaders, in conjunction with the rest of the staff, ensure the adequate equipping and training of MI organizations and individual augmentees that conduct intelligence operations. Predictive intelligence supports the decisions the commander and staff make regarding the size, composition, structure, and deployment sequence of the force.

C-19. In a force projection operation, higher echelons provide intelligence for situation and target development to lower echelons until the tactical ground force completes entry and secures the lodgment area. The higher headquarters intelligence section may be reluctant to push everything down through tactical-level intelligence channels due to the volume of the intelligence information available. Intelligence analysis systems provide the BCT S-2 access to theater and national databases with the ability to collaborate with knowledge centers. Intelligence readiness training assists in ensuring intelligence professionals and assets can meet the unit's needs during operations. The G-2/S-2 must anticipate, identify, consider, and evaluate all potential threats to the entire unit throughout force projection operations.

C-20. Throughout mobilization, unit intelligence activities provide deploying forces with the most recent intelligence on the contingency area. The intelligence staff also updates databases and situation graphics. Intelligence leaders—

- Fully understand the unit, higher headquarters, and joint force intelligence organizations.
- Revise intelligence and intelligence-related communications architectures and integrate any new systems and software into current architectures.
- Support 24-hour operations and provide continuous intelligence (to include terrain and weather) support.
- Plan all required intelligence reach procedures.
- Determine transportation availability for deployment as well as during deployment.
- Determine all sustainability requirements.
- Determine intelligence release requirements and restrictions and releasability to multinational and host-nation sources.
- Review status-of-forces agreements, rules of engagement, international law, intelligence sharing agreements, and other agreements, emphasizing the effect they have on intelligence collection. (Coordinate with the staff judge advocate on these issues.)
- Ensure deployment priorities for the collection assets and sensors along with the required intelligence PED personnel are reflected in the TPFDD to support information collection activities.
- Ensure intelligence links provide the early-entry commander access to joint and Army all-source intelligence and collection assets, processing systems, and databases.
- Review the supported unit commander's specified tasks, implied tasks, task organization, intelligence scheme of support, and coordination requirements. Address issues or shortfalls and direct or coordinate changes.
- Establish access to national databases and repositories for each intelligence discipline and complementary capability, as well as links to joint, Service, multinational, and host-nation databases and repositories.

DEPLOYMENT

C-21. *Deployment* is the movement of forces into and out of an operational area (JP 3-35). The joint deployment process is divided into four phases: deployment planning, predeployment activities, movement, and joint RSOI. The joint process includes a planning phase at the outset whereas the Army considers planning to be woven through all phases. Moreover, the movement phase in the Army process occurs in two segments: fort-to-port and port-to-port. The Army and other Services rely on the U.S. Transportation Command to provide the strategic lift to, through, and from strategic ports, both in CONUS and OCONUS. (For doctrine on deployments, see ATP 3-35.)

C-22. A smooth and effective deployment is a challenge for intelligence staffs and MI units because of the many complex and technical aspects of intelligence support and intelligence operations. During deployment, intelligence organizations at the home station or deployed with the early-entry force use the communications architecture and higher and lower intelligence organizations to provide graphic and textual intelligence updates to the forces en route. En route updates assist in reducing information gaps and allow commanders to adjust plans in response to changes in the situation before arriving at the operational area. During stability operations and other circumstances, intelligence transitions are conducted between arriving units and those that are redeploying. The three primary areas of intelligence transition are—

- Operations.
- Targeting.
- Technical oversight.

C-23. Intelligence units extend established networks to connect intelligence staffs and collection assets at various stages of the deployment. Where necessary, units establish new communications paths to meet mission requirements. If deployed, the joint force, theater army, and corps ACEs have a critical role in providing access to and building out the intelligence architecture and in sharing intelligence databases to deploying forces.

C-24. The Army relies on space-based capabilities and systems, such as global positioning satellites, communications satellites, weather satellites, cruise missile launches, and intelligence collection platforms. These systems are critical enablers for Army personnel to plan, communicate, navigate and maneuver, provide missile warning, and protect and sustain Army forces. Planning and coordination of space support with national, joint, Service, and theater resources occur through liaison with space and weather professionals. Space-enabled capabilities are key to supporting intelligence during deployment and employment by—

- Monitoring terrestrial AOIs to assist in revealing the threat's location and disposition.
- Providing communications links between deploying forces, the United States, and its territories.
- Permitting collection assets to determine their position accurately through the Global Positioning System.
- Providing meteorological, oceanographic, and space environmental information and data that are processed, analyzed, and exploited to produce timely and accurate weather effects on operations.
- Providing warnings of ballistic missile launches.

C-25. Situation development dominates intelligence activities during early-entry operations. The intelligence staff attempts to identify all threats to arriving forces and assists the commander in developing force protection measures. Peer threat capabilities (such as long-range strike and A2 and AD capabilities) create additional challenges to entry operations and freedom of movement. During entry operations, echelons above corps organizations provide intelligence support, which includes providing access to the national intelligence and early deployment intelligence elements. The entire effort focuses on providing tailored support to deploying and deployed echelons in response to their intelligence requirements.

C-26. Collection and processing capabilities are enhanced as assets arrive and buildup in the AO, with emphasis on the buildup of the deployed capability required to conduct sustained information collection activities. Intelligence PED personnel are employed either through the deployment of PED with the force (expeditionary PED) or through reach PED conducted in theater, at sanctuary sites, or from the locations within the United States.

C-27. Liaison personnel, basic communications, and an initial intelligence architecture should be in place before the scheduled arrival of parent commands. When the senior Army headquarters arrives in the operational area, the joint force intelligence staff implements and, where necessary, modifies the theater intelligence architecture. Deploying intelligence assets establish liaison with staffs and deployed units. As more units deploy and complete RSOI, the amount of information collection units increases.

C-28. Installations in the United States and its territories and other bases outside the operational area continue to support deployed units. Systems capable of rapid receipt and processing of intelligence from national systems and high-capacity, long-haul communications systems are critical to the success of intelligence reach and overwatch to a deployed force. These systems provide a continuous flow of intelligence to satisfy many operational needs.

C-29. During entry operations the intelligence staff—

- Monitors protection indicators.
- Assesses the information collection effort.
- Monitors intelligence reporting on threats and civil considerations.
- Assesses—
  - Push versus pull requirements of intelligence reach and overwatch.
  - The effectiveness of the intelligence communications architecture.
  - Reporting procedures and timelines.

EMPLOYMENT

C-30. *Employment* is the strategic, operational, and tactical use of forces (JP 5-0). Intelligence and information collection support operations by understanding and answering the commander's requirements. They focus primarily on supporting the commander's situational understanding, targeting, and protection requirements. Good planning and preparation can ensure a smooth transition from deployment to employment and from employment through sustainment to redeployment.

SUSTAINMENT

C-31. *Sustainment* is the provision of logistics, financial management, personnel services, and health services support necessary to maintain operations until successful mission completion (ADP 4-0). The intelligence warfighting function must both support friendly force sustainment, which is often vulnerable to threat attack, and sustain intelligence support and intelligence operations. Supporting sustainment is similar to supporting other force projection subprocesses and is discussed in other portions of this publication. Sustaining intelligence support and intelligence operations is broad and can be complex. Aspects of sustaining intelligence can include—

- IEW collection systems maintenance.
- Intelligence architecture and PED maintenance and logistics.
- Providing and maintaining the appropriate numbers and skill levels of intelligence professionals, in many situations, low-density specialties.
- Contract support (including linguists).
- Port, railhead, airhead, or transshipment operations.
- Convoy operations and resupply of the different classes of supply.
- Medical support and casualty evacuation.
- Mortuary affairs.

REDEPLOYMENT

C-32. *Redeployment* is the transfer of forces and materiel to home and/or demobilization stations for reintegration or out-processing (ATP 3-35). This definition differs from the joint definition. As with deployment, there is a requirement to conduct an intelligence transition from the redeploying unit to the deploying unit. A well-prepared intelligence transition ensures a smooth and seamless transition between units.

C-33. As combat power and resources decrease in the operational area, protection and warning become the focus of the commander's intelligence requirements. This drives the selection of those assets that must remain deployed until the end of the operation and those that may redeploy earlier. The G-2/S-2—

- Monitors intelligence reporting on threat activity and warning data.
- Continues to conduct intelligence support to protection.
- Requests information collection support (combatant command and national systems) and intelligence to support redeployment.

C-34. After redeployment, MI personnel and units recover and return to predeployment activities. Information collection units resume contingency-oriented peacetime intelligence operations. The intelligence staff—

- Prepares after-action reports and lessons learned.
- Monitors intelligence reporting on threat activity and civil considerations for contingencies.
- Updates or consolidates databases.
- Maintains intelligence readiness.
- Provides input to the force-design update process to refine modified tables of organization and equipment and to evaluate the need for individual mobilization augmentee personnel.
- Submits organizational needs requests.

HOMELAND DEFENSE AND DEFENSE SUPPORT OF CIVIL AUTHORITIES CONSIDERATIONS

C-35. While Army forces are preparing to deploy during crisis or armed conflict against a peer threat, other units may be tasked to support homeland defense or DSCA. The circumstances that lead to national authorities directing the deployment of Army forces may also necessitate operations to simultaneously defend the U.S. homeland or support civil authorities. (See FM 3-0.)

C-36. *Homeland defense* is the protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President (JP 3-27). *Defense support of civil authorities* is support provided by U.S. Federal military forces, DOD civilians, DOD contract personnel, DOD 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, USC 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). Homeland defense and DSCA are critical to successful force projection operations. A peer threat's ability to impact the U.S. homeland through lethal and nonlethal means across the strategic contexts has increased due to reliance on technology that is susceptible to threat capabilities. The G-2/S-2s must be aware of threats against the U.S. homeland with the potential to impact their units' operations.

C-37. Homeland defense and DSCA operations are conducted in a complex OE that contains layers of different jurisdictions (federal, state, territorial, tribal, and local), many agencies and organizations, the private sector, and several allies and multinational partners. (See FM 3-0.) Within the same city, Army forces may be simultaneously conducting different missions, each with distinct authorities and requirements. This could include adjacent units conducting—

- Deployment preparation activities.
- Homeland defense missions, as directed by the U.S. Northern Command or U.S. Indo-Pacific Command.
- DSCA to support the Department of Homeland Security or other organizations.

C-38. During crisis and armed conflict, Army forces allocated to the CCDR will likely conduct homeland defense and DSCA missions simultaneous to enable Army force projection processes. For Army intelligence forces conducting homeland defense and DSCA, intelligence staffs and units must reference specific intelligence mission and authorities detailed in homeland defense related OPORDs and their associated Annex B (Intelligence). These intelligence homeland defense related intelligence missions are informed by guidelines for theater army, corps, division, and BCT intelligence staffs and units (see chapter 6).

C-39. Forward theater intelligence activities greatly contribute to homeland defense. In addition to assessing threats in forward theaters, Army intelligence staffs, units, and organizations worldwide have a significant role in detecting, deterring, and preventing attacks against the United States. Forward theater intelligence staffs, in coordination with intelligence staffs supporting homeland defense, must establish intelligence handover lines and other approved control measures and procedures to lessen the possibility of gaps in coverage to detect threats against the U.S. homeland.

C-40. Interorganizational cooperation is critical to homeland defense. The success of interorganizational cooperation hinges on timely and accurate information and intelligence for decision making. Information sharing environments should include as many essential participants as possible, with the understanding that not all can participate in a collaborative environment. When possible, a collaborative intelligence sharing environment should be capable of generating and disseminating intelligence, operational information, and orders, where needed, in the shortest time possible.

C-41. Army intelligence units conducting homeland defense should anticipate sharing intelligence with Army units during force projection processes. Theater army ACEs and JTF/JFLCC-level joint force intelligence operations centers have a critical role in making intelligence assessments available to deploying forces. (See ATP 2-91.7 and ADP 3-28.)

C-42. Intelligence units may conduct analysis of and intelligence collection against peer threats or foreign-intelligence-related opportunist threats impacting DOD DSCA missions, and in certain instances, provide situational awareness, damage assessments, or incident awareness and assessments according to Secretary of Defense authorization and combatant command DSCA-related mission orders. (See ATP 2-91.7.)

Note. For Army intelligence forces conducting homeland defense and DSCA, intelligence staffs, units, and organizations must reference specific intelligence mission and authorities in homeland defense related OPORDs and associated Annex B (Intelligence) in order to ensure compliance with DOD intelligence activity guidance.

This page intentionally left blank.

Appendix D

General Intelligence Provisions, Authorities, and Oversight Principles

OVERVIEW

D-1. Intelligence personnel conducting intelligence operations must comply with laws, regulations, and policies. The implications of and considerations associated with these provisions and authorities include the oversight, management, and resourcing of intelligence operations and the authority for or prohibitions on certain specific intelligence activities. This appendix provides a description of laws, regulations, and policies that govern intelligence operations and a general overview of intelligence oversight.

UNITED STATES CODE TITLES

D-2. G-2/S-2s, intelligence planners, and MI unit commanders must comply with the intelligence provisions and authorities in the following titles of the USC:

- Title 10, USC, *Armed Forces of the United States*, addresses—
  - The authority of the Secretary of Defense over all DOD intelligence organizations and activities.
  - The position of Under Secretary of Defense for Intelligence and Security.
  - The role of national intelligence through tactical intelligence and the integration of DOD ISR capabilities.
  - Meeting the needs of CCDRs through tactical commanders.
  - Funds for foreign cryptologic support.
  - The appropriation, use, and auditing of DOD intelligence funds.
  - Congressional oversight.
- Title 18, USC, *Crimes and Criminal Procedure*, addresses Posse Comitatus prohibition.
- Title 32, USC, *National Guard*, addresses—
  - Homeland defense activities.
  - DSCA.
- Title 50, USC, *War and National Defense*, addresses—
  - The role of the Secretary of Defense in conducting intelligence activities.
  - The purpose of all-source intelligence and the role of integrated and synchronized DOD intelligence collection, analysis, and dissemination as part of the larger U.S. IC.
  - The role of national intelligence through tactical intelligence.
  - The needs of CCDRs through tactical commanders.
  - Specialized intelligence functions of the National Security Agency, the National Geospatial-Intelligence Agency, National Reconnaissance Office, and DIA.
  - CI activities.
  - Intelligence budget and oversight.

D-3. Title 10, USC, and Title 50, USC, are inextricably linked and mutually supportive statutory provisions for DOD intelligence activities at every level of warfare (strategic, theater-strategic, operational, and tactical) during peacetime or war.

INTELLIGENCE OVERSIGHT

D-4. Intelligence oversight derives from Executive Order (EO) 12333 as amended, with DOD implementing guidance in DODM 5240.01 and the Army implementing guidance in AR 381-10:

- EO 12333, *United States Intelligence Activities* (as amended)—
  - Is the principal legal authority for intelligence activities (provides intelligence goals and directions).
  - Defines the structure and mission of the U.S. IC.
  - Delineates jurisdictional boundaries among intelligence agencies and establishes duties and responsibilities for each department and agency within the U.S. IC.
  - Declares rules to guide and limit the conduct of intelligence activities.
  - Defines agency responsibilities, including the DOD's role, for national intelligence efforts.
  - Declares rules of conduct for intelligence activities involving U.S. persons.
  - Contains general provisions pertaining to oversight, implementation, and definitions.
- DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*—
  - Establishes procedures to enable DOD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons.
  - Authorizes defense intelligence components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, EOs, policies, and regulations.
- AR 381-10, *The Conduct and Oversight of U.S. Army Intelligence Activities*—
  - Establishes policies and procedures for the conduct of authorized intelligence functions to protect the rights and privacy of U.S. persons.
  - Applies to any Army component performing authorized Army intelligence and intelligence-related activities.
  - Does not, in and of itself, authorize intelligence activities—it simply sets forth the policies and procedures for conducting such activities, provided the personnel conducting collection have the appropriate mission and authority.

D-5. Intelligence activities authorized by EO 12333 as amended are further extended to CCDRs through OPORDs and OPLANs. Additionally, certain intelligence activities may be directed by other legislative authority and are not exclusive to Title 10 or Title 50 statutes.

D-6. Each organization or unit must have a specific assigned mission to conduct a particular type of intelligence activity. These specific authorities are often found in a wide range of documents, such as DOD directives, intelligence agency specific authorities, Army regulations, OPORDs, and OPLANs.

D-7. If the intelligence staff has any questions on authorities or funding sources—due to the dynamic nature, complexity, and large volume of intelligence laws and policies—the staff should coordinate closely with the unit staff judge advocate for clarification.

U.S. Person Information

Intelligence personnel will conduct intelligence collection activities in accordance with the requirements of EO 12333 as amended, DODM 5240.01, and AR 381-10 in a manner that ensures legality and propriety and preserves and respects the privacy and civil liberties of U.S. persons. Army intelligence personnel conducting intelligence collection activities will complete intelligence oversight training as required in DOD 5240.1-R and AR 381-10 before conducting intelligence collection activities.

Soldiers with an authorized intelligence mission or function can collect, retain, and disseminate intelligence on U.S. persons in compliance with specific criteria and restrictions. An Army component may collect information that identifies U.S. persons only if—

- It is necessary to the conduct of a function assigned to the collecting component.
- It falls within 1 of 13 categories in DODM 5240.01, procedure 2.
- Collection techniques are limited to those necessary to perform assigned functions using the least intrusive means.

If, during authorized collection activities, U.S. person information is incidentally collected (it was not the target of the collection), all such information may be temporarily retained, evaluated for permanent retention, and disseminated only in accordance with DODM 5240.01, procedures 3 and 4, and AR 381-10.

INTELLIGENCE AUTHORITY SOURCES

D-8. Table D-1 lists some of the most important intelligence authority sources.

Table D-1. Law, policy, and other sources applicable to intelligence operations

Executive Order 12333, *United States Intelligence Activities* (as amended)
AR 381-10, *The Conduct and Oversight of U.S. Army Intelligence Activities*
AR 381-20, *The Army Counterintelligence Program*
AR 381-26, *Army Foreign Materiel Program*
AR 381-47, *Offensive Counterintelligence Operations*
AR 381-100, *Army Human Intelligence Collection Programs*
AR 381-102, *Army Cover Program*
AR 381-141, *Intelligence Contingency Funds*
AR 381-143, *Intelligence Property Book*
AR 525-95, *Army Geospatial Intelligence and Geospatial Information Services*
DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons* (Procedures 11 through 13 remain)
DOD Law of War Manual
DODD 2310.01E, *DOD Detainee Program*
DODD 3115.09, *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*
DODD 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*
DODD 5148.13, *Intelligence Oversight* (Replaced Intelligence Oversight Procedures 14 and 15 of DOD 5240.1-R)
DODD 5240.01, *DOD Intelligence Activities*
DODM 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*
FM 2-22.3, *Human Intelligence Collector Operations*
FM 6-27, *The Commander's Handbook on the Law of Land Warfare*
ICD 104, *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation*
ICD 113, *Functional Managers*
ICD 116, *Intelligence Planning, Programming, Budgeting, and Evaluation System*
ICD 203, *Analytic Standards*
ICD 204, *National Intelligence Priorities Framework*
ICD 302, *Document and Media Exploitation*
ICD 304, *Human Intelligence*
ICD 310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence and Counterintelligence Activities Outside the United States*

Table D-1. Law, policy, and other sources applicable to intelligence operations (*continued*)

ICD 311, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence and Counterintelligence Activities Inside the United States*
ICPG 107.1, *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*
Title 10, USC, *Armed Forces*
Title 32, USC, *National Guard*
Title 50, USC, *War and National Defense*
Relevant DOD instructions
U.S. Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities*
Privacy Act of 1974 (Section 552a, Title 5, USC [also called 5 USC § 552a])
Manual for Courts-Martial United States (2019 Edition)
International treaties, such as the Hague Convention (1899 and 1907), the Geneva Conventions (1949), and Protocol I to the Geneva Conventions (1977)

AR	Army regulation	ICD	intelligence community directive
DOD	Department of Defense	ICPG	intelligence community police guidance
DODD	Department of Defense directive	U.S.	United States
DODM	Department of Defense manual	USC	United States Code
FM	field manual		

Appendix E
Language Support Considerations

LANGUAGE REQUIREMENTS

E-1. Military operations highly depend on military- and contractor-provided foreign language support. The requirement to communicate with and serve on multinational staffs, communicate with local populations, and collect information necessitates the use of linguists. The growing focus on multinational operations increases the competition for limited linguist resources that are vital for mission success.

LANGUAGE SUPPORT CATEGORIES

E-2. Language support requirements typically fall into one of seven broad categories:

- Intelligence operations.
- Multinational liaison.
- Special operations.
- CMO.
- CA operations.
- Sustainment.
- Information.

Intelligence Operations

E-3. Intelligence operations includes linguist requirements inherent in CI, HUMINT, OSINT, and SIGINT.

Multinational Liaison

E-4. Multinational liaison includes the coordination of military operations and liaison with multinational partners, previously unaffiliated nations, host-nation personnel and offices, and, at times. adversary or former adversary nations. (See FM 6-0.)

Special Operations

E-5. Operations conducted by special operations forces typically require foreign language capabilities. Because of the broad range of languages, Army special operations forces may not have the required number of personnel trained in a specific language or dialect. In many situations, Army special operations forces require sophisticated language skills requiring a nuanced language capability that can only a native speaker can provide or vet. For example, psychological operations specialists develop product series in target languages to obtain specific responses, and special forces team members convey the intent of the operation to an indigenous force; CA personnel work in specialized teams found in government, law, medical support, law enforcement, infrastructure projects, public safety, and population control. (See FM 3-53, FM 3-18, and FM 3-57.)

Civil-Military Operations

E-6. *Civil-military operations* are activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation (JP 3-57). CMO may include military forces performing activities and functions normally performed by the local, regional, or national government. These activities may occur before, during, or after other military actions. They are fundamental to executing stability

operations conducted during offensive and defensive operations. Commanders are inherently responsible for CMO, and Army forces conduct CMO to coordinate civil and military activities, minimize civil-military friction and threats from the civil component, maximize support for operations, and meet commanders' legal obligations and moral responsibilities to civilian populations within the operational area.

E-7. CA personnel, other Army forces, other government agencies, or a combination of all three perform these activities, and the G-9 is the lead staff officer for these activities. Foreign language support is critical to CMO and may include language requirements in addition to those native in the nation where the operation is occurring, as there may be other foreign governments and nongovernmental agencies involved in stability operations. (See FM 3-57.)

Civil Affairs Operations

E-8. CA operations enhance the relationship between civil authorities and military forces. They involve applying CA functional specialty skills to areas normally under the civil government's responsibility. These operations involve establishing, maintaining, influencing, or exploiting relations between military forces and all levels of host-nation government agencies. CA personnel work with specialized vernacular in such areas as government liaison, legal agreements, medical support and operations, law enforcement, infrastructure projects, engineering projects, public safety, security, and population control. (See FM 3-57.)

Sustainment

E-9. This category consists of foreign language support to sustainment functions, which include logistic contracting; port, railhead, airhead, or transshipment operations; and convoy operations. (See ADP 4-0.)

Information

E-10. DOD makes every effort to synchronize, align, and coordinate communications activities to facilitate an understanding of how the planning and execution of DOD strategies, plans, operations, and activities will be received or understood by key audiences. To support these efforts, commanders and staffs should identify and understand key audience perceptions and possible reactions when planning and executing operations. This understanding of key audience perceptions and reactions is a vital element of every theater campaign and contingency plan, and it is essential to the Army's ability to achieve unity of effort through unified action with the joint force, interagency partners, and the broader interorganizational community. Key audience beliefs, perceptions, and behaviors are crucial to the success of any strategy, plan, and operation.

E-11. Using accurate language, in the right tone and with the right connation, is crucial to these efforts and requires foreign language support. Through the commander's communications synchronization, public affairs, information advantage activities, and defense support to public diplomacy are realized as communications supporting capabilities. The commander's communications synchronization assists leaders, planners, and operators at all levels in understanding the desired effects and anticipating potential undesired effects of the Army's actions and words, identifying key audiences, and actively addressing their perspectives when appropriate.

COMMAND LANGUAGE PROGRAM MANAGER

E-12. Commanders with many assigned linguists (150 or more) must appoint a full-time command language program manager with a specified job description to manage the command language program. All personnel performing command language program manager duties (either full-time or as an additional duty) must attend the Defense Language Institute Foreign Language Center Command Language Program Manager course.

COMMAND LANGUAGE COUNCIL

E-13. A command language council is required for a unit with more than 50 language-coded positions authorized on Army manning documents. This council promotes linguistic excellence through the sharing of ideas and information and to prioritize training. The command language council should include the commander, command sergeant major, S-1, S-2, S-3, S-4, and the resource manager. However, the

commander may direct other staff participation. For units with less than 50 linguists, it is at the commander's discretion to authorize the establishment of a command language council. (See AR 11-6.)

LANGUAGE SUPPORT FOR INTELLIGENCE OPERATIONS

E-14. The SIGINT and HUMINT disciplines require specific language skills to accomplish their collection tasks successfully. SIGINT collectors often analyze and report information obtained through the intercept of foreign language communications. Communications intelligence, together with intelligence research and analysis missions, demands highly skilled listening and reading language capabilities. HUMINT collection operations that require foreign language capabilities include the following:

- **Interrogation.** Foreign language requirements for interrogation include listening and speaking abilities for conducting the interrogation itself.
- **Debriefing.** Debriefers require foreign language reading, listening, and speaking capabilities to prepare for and carry out debriefings of foreign subjects.
- **Liaison.** HUMINT collectors rely heavily on language ability to conduct effective liaison with host-nation and other officials.
- **HUMINT source operations.** All foreign language capabilities are required to conduct military source operations effectively.

E-15. The HUMINT specialty identifies language proficiency with a skill qualification identifier. However, when language-qualified debriefers are unavailable, debriefers may use interpreters. During the train/ready phase, CI and HUMINT Soldiers must have the opportunity to participate in language and cultural immersion programs that provide commanders with the socioeconomic expertise for specific target areas.

LANGUAGE SUPPORT SOURCES

E-16. Commanders can use various sources to obtain the linguists needed to support operations. It is vital to know the advantages and disadvantages of each type of linguist and to match the available linguists to the various requirements of the operation carefully.

ARMY LANGUAGE MILITARY OCCUPATIONAL SPECIALTIES

E-17. The language-dependent MI enlisted military occupational specialty (MOS) is 35P with a skill qualification identifier of L (cryptologic linguist). HUMINT collector specialties (MOS 35M and warrant officer MOS 351M) are designated as language dependent. Leaders should be aware of the language proficiency level of their assigned HUMINT collectors, which may range from no language to full native proficiency. (See table E-1 on page E-4.)

E-18. Not all 35M Soldiers are language dependent. Active Component and ARNG 35M Soldiers who did not attend language training before 30 September 2020 are grandfathered and do not have to attend language training to maintain MOS qualification for the duration of their career. Active Component and ARNG Soldiers who entered service as MOS 35W or 35M and graduated from the Defense Language Institute Foreign Language Center, or were recruited for their language, are subject to the provisions of AR 11-6. USAR 35M Soldiers who signed a contract before 15 July 2020 are grandfathered. These 35M Soldiers are considered language capable for the duration of their career. USAR 35M Soldiers who enter service after 15 July 2020 are considered language dependent and are subject to the provisions of AR 11-6.

E-19. The following non-MI career management fields, branches, and functional areas include language-qualified enlisted MOSs and officer areas of concentration:

- Career management field 18 (special forces [enlisted, warrant officers, and officers]).
- Career management field 37 (psychological operations [enlisted and officers]).
- Career management field 38 (CA).
- Functional area 48 (foreign area officer).

Table E-1. Foreign language skill rating and language modalities

Foreign language skill rating	*Rated language modalities*
0 No proficiency	(L) No practical understanding of the spoken language. Understanding is limited to occasional isolated words with essentially no ability to comprehend communication. (R) No practical ability to read the language. Consistently misunderstands or cannot comprehend at all. (S) Unable to function in the spoken language. Oral production is limited to occasional isolated words.
0+ Memorized proficiency	(L) Understands with reasonable accuracy only when this involves short, memorized utterances or formulae. (R) Can recognize all the letters in the printed version of an alphabetic system and high-frequency elements of a syllabary or a character system. (S) Vocabulary is usually limited to areas of immediate survival needs.
1 Elementary proficiency	(L) Can understand simple questions and answers, simple statements, and very simple face-to-face conversations in a standard dialect. (R) Can read very simple connected written material in a form equivalent to usual printing or typescript. (S) Able to satisfy minimum courtesy requirements and maintain very simple face-to-face conversations on familiar topics.
1+ Elementary proficiency plus	(L) Sufficient comprehension to understand short conversations about all survival needs and limited social demands. (R) Sufficient comprehension to understand simple discourse in printed form for informative social purposes, as well as understand some main ideas from more complex texts. (S) Can initiate and maintain predictable face-to-face conversations and satisfy limited social demands; range and control of the language are limited.
2 Limited working proficiency	(L) Sufficient comprehension to understand conversations on routine social demands and limited job requirements. (R) Sufficient comprehension to read simple, authentic written material in a form equivalent to usual printing or typescript on subjects within a familiar context. (S) Able to satisfy routine social demands and limited work requirements.
2+ Limited working proficiency plus	(L) Sufficient comprehension to understand most routine social demands and most conversations on work requirements as well as some discussions on concrete topics related to interests and special fields of competence. (R) Sufficient comprehension to understand most factual material in nontechnical prose as well as some discussions on concrete topics related to special professional interests. (S) Able to satisfy most work requirements with language usage that is often, but not always, acceptable, and effective.
3 General professional proficiency	(L) Able to understand the essentials of all speech in a standard dialect including technical discussions within a special field. (R) Able to read within a normal range of speed and with almost complete comprehension a variety of authentic prose material on unfamiliar subjects. (S) Able to speak the language with sufficient structural accuracy and vocabulary to participate effectively in most formal and informal conversations in practical, social, and professional topics.
3+ General professional proficiency plus	(L) Comprehends most of the content and intent of a variety of forms and styles of speech pertinent to professional needs, as well as general topics and social conversation. (R) Can comprehend a variety of styles and forms pertinent to professional needs and rarely misinterprets such texts or difficulty relating ideas or making inferences. (S) Is often able to use the language to satisfy professional needs in a wide range of sophisticated and demanding tasks.
4 Advanced professional proficiency	(L) Able to understand all forms and styles of speech pertinent to professional needs as well as understand fully all speech with extensive and precise vocabulary. (R) Able to read fluently and accurately all styles and forms of the language pertinent to professional needs as well as understand full ramifications of texts in wider sociopolitical environment. (S) Able to use the language fluently and accurately on all levels normally pertinent both personal and professional needs.
4+ Advanced professional proficiency plus	(L) Increased ability to understand extremely difficult and abstract speech as well as ability to understand all forms and styles of speech pertinent to professional needs, including social conversations. (R) Nearly native ability to read and understand extremely difficult or abstract prose, a very wide variety of vocabulary, idioms, colloquialisms, and slang. (S) Speaking proficiency is regularly superior in all respects, usually equivalent to that of a well-educated, highly articulate native speaker.
5 Functionally native proficiency	(L) Comprehension equivalent to that of the well-educated native listener. (R) Reading proficiency is functionally equivalent to that of the well-educated native reader. (S) Speaking proficiency is functionally equivalent to that of a highly articulate well-educated native speaker and reflects the cultural standards of the country where the language is natively spoken.
L listening modality	R reading modality S speaking modality

CONTRACT LINGUISTS

E-20. U.S. civilians can be contracted to provide linguist support. They have an advantage over local-national hires because their loyalty to the United States is more readily evaluated and it is easier for them to be granted the necessary security clearance. However, there are usually severe limitations on the deployment and use of civilians. A careful assessment of their language ability is important because they may use outdated terms or interject U.S. idioms. If the linguists are recent immigrants, the use of the language in their country of origin could be dangerous to them; similarly, their loyalty may reside with their country of origin, religious group, tribal affiliation, or other close connections when the interests of these groups are at odds with U.S. interests.

E-21. Local-national hires often provide the bulk of linguist support. They are usually less expensive to hire than U.S. civilians and know the local dialect, idioms, and culture. The expertise of these linguists in particular areas or subject matters can be an asset.

E-22. All commands must comply with the CI screening policy for contract linguist support. CI screenings may be performed by the hiring agency within the joint operations area or by CI personnel, who also screen contract linguists periodically throughout their employment.

E-23. When requesting civilian contract linguists, the commander and staff must identify requirements by category:

- **Category I** linguists are locally hired personnel with an understanding of the English language. They undergo a limited screening, are hired in-theater, do not possess a security clearance, and are used for unclassified work. During most operations, category I linguists must be rescreened on a scheduled basis. Category I linguists cannot be used for intelligence operations:
  - **Advantages:** Category I linguists—
    - Have the best knowledge of the local area such as terrain and familiarity of the local populace.
    - Are native speakers of the target language and can normally communicate more fluently with the local populace.
    - Usually have a more thorough understanding of the interactions of the various local population groups.
  - **Disadvantages:** Category I linguists—
    - Can be a risk to OPSEC.
    - Have loyalties that may align more with the local populace or the threat than with the United States.
    - Do not possess a security clearance and cannot be involved in sensitive missions requiring one.
    - May also be under direct physical threat by the local populace or threat for appearing to collaborate with U.S. forces.
    - May not be as fluent in the English language as category II or III linguists.
    - Who are typically local hires, may more closely associate with one or more indigenous groups, which may or may not be friendly toward the United States.
- **Category II** linguists are U.S. citizens who have native command of the target language and near-native command of the English language. They undergo a screening process that includes a national agency check. Upon favorable findings, category II linguists are granted a Secret Collateral clearance.
  - **Advantages:** Category II linguists—
    - Are normally U.S. citizens or military members who have been granted a Secret security clearance, which is the minimum acceptable clearance for CI and HUMINT collection.
    - Are normally fluent in both English and the target language, may hold a Secret security clearance, and can be used on missions requiring one. Their loyalties align with the United States more than with the local populace.

  - **Disadvantages:** Category II linguists—
    - Can be a liability if they are civilians and may encounter imminent danger depending on the type of element they support.
    - Are probably not as good in their command for local dialects as category I linguists.
    - May have limited, if any, experience or knowledge of the local terrain or knowledge of the local populace.
    - Knowledge of how the various local population groups interact may not be as detailed or as comprehensive as that of category I linguists.
- **Category III** linguists are U.S. citizens who have native command of the target language and native command of the English language. They undergo a screening process that includes a special background investigation and a polygraph. Upon favorable findings, category III linguists are granted an interim or final Top Secret/sensitive compartmented information clearance by the designated U.S. Government personnel security authority:
  - **Advantages:** Category III linguists—
    - Have an extensive security background investigation.
    - Hold a Top Secret and/or interim Top Secret security clearance and can be used on missions requiring one.
    - Align their loyalties wholly or most closely with the United States than with other entities, groups, or organizations.
  - **Disadvantages:** Category III linguists—
    - Language capability may be limited due to minimal family language immersion, limited language training, and/or limited in-country experience.
    - Normally have language proficiency that is adequate for missions, but it may not be as good as category I or II linguists.
    - Are probably not as good in their command for local dialects as category I or II linguists.
    - May have the least understanding or knowledge of the local terrain and populace. Their knowledge of how the various local population groups interact may be the least detailed or comprehensive.

NON-DEPARTMENT OF DEFENSE TRAINED ARMY LINGUISTS

E-24. The Army has numerous Soldiers of all grades who are proficient in a foreign language but whose primary duties do not require foreign language proficiency. They may have attended a civilian school to learn a foreign language, or they may have acquired proficiency through their heritage. They have the advantage of being trained Soldiers and are therefore readily deployable throughout the AO. They may qualify for a foreign language proficiency bonus by passing the Defense Language Proficiency Test. Nonlinguists have difficulties assessing the capabilities of Soldiers who have not taken the Defense Language Proficiency Test. Without a test score on record, the manpower and personnel staff also have difficulties identifying them as linguists.

DETERMINING LANGUAGE SUPPORT REQUIREMENTS

E-25. Determining linguist requirements for any operation can be difficult because each operation is unique. The staff determines linguist requirements as part of IPOE during mission analysis. It starts by identifying specified or implied tasks requiring foreign language support. Other critical factors are the organization or echelon of command and the location of the AO. The staff uses these criteria to determine the allocation of linguists, such as one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed. The staff then determines the number of linguists needed for an operation based on the tasks to be performed and the allocation of linguists. Within this process, the staff considers the different dialects within the AO when determining language support requirements. (For policy on the Army foreign language program, see AR 11-6.)

E-26. The intelligence cell at each echelon is responsible for the following:

- Identifying category II and category III linguist requirements needed to support intelligence functions in all contingency areas. Intelligence staff requirements for linguist support include but are not limited to—
  - Evaluating and/or using local maps and terrain products in operations.
  - Assessing local open-source information for intelligence value.
- Determining linguist requirements based on the mission and the foreign languages and dialects spoken in the AO.
- Providing intelligence training for MI linguists employed in the AO.
- Coordinating for security investigations, as necessary, for local-hire linguists.
- Providing support to CI screenings of contracted linguists and hired local-national labor force.

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 FM 2-0 is the proponent with an asterisk (*) before the term. For other terms, the proponent publication is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

A2	antiaccess
AA	avenue of approach
ABCANZ	American, British, Canadian, Australian, and New Zealand
ACE	analysis and control element
AD	area denial
ADCON	administrative control
ADP	Army doctrine publication
AGM	attack guidance matrix
AISE	Army Intelligence and Security Enterprise
AJP	Allied joint publication
AO	area of operations
AOI	area of interest
AOR	area of responsibility
AR	Army regulation
ARNG	Army National Guard
ASCC	Army Service component command
ATP	Army techniques publication
BCT	brigade combat team
BDA	battle damage assessment
BISE	brigade intelligence support element
C2	command and control
CA	civil affairs
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCIR	commander's critical information requirement
CEMA	cyberspace electromagnetic activities
CENTRIXS	Combined Enterprise Regional Information Exchange System
CI	counterintelligence
CIP	common intelligence picture
CMO	civil-military operations

COA	course of action
COIC	current operations integration cell
COM	collection operations management
CONUS	continental United States
COP	common operational picture
CP	command post
CRM	collection requirements management
D3A	decide, detect, deliver, and assess
DA	Department of the Army
DA G-2	Army Deputy Chief of Staff for Intelligence
DDIL	denied, disrupted, intermittent, and limited
DIA	Defense Intelligence Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODM	Department of Defense manual
DOMEX	document and media exploitation
DS	direct support
DSCA	defense support of civil authorities
EA	electromagnetic attack
E-MIB	expeditionary-military intelligence brigade
EMS	electromagnetic spectrum
EO	executive order
EP	electromagnetic protection
ES	electromagnetic support
EW	electromagnetic warfare
FAIO	field artillery intelligence officer
FM	field manual
FRAGORD	fragmentary order
FSE	fire support element
G-2	assistant chief of staff, intelligence
G-2X	counterintelligence and human intelligence staff element
G-3	assistant chief of staff, operations
G-5	assistant chief of staff, plans
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
GEOINT	geospatial intelligence
GS	general support
HPT	high-payoff target
HPTL	high-payoff target list
HVT	high-value target
HUMINT	human intelligence

I2	identity intelligence
IADS	integrated air defense system
IC	intelligence community
ICD	intelligence community directive
IEW	intelligence and electronic warfare
IEWTPT	Intelligence and Electronic Warfare Tactical Proficiency Trainer
INSCOM	United States Army Intelligence and Security Command
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
IPOE	intelligence preparation of the operational environment
ISR	intelligence, surveillance, and reconnaissance
IWFT	intelligence warfighting function task
J-2	intelligence directorate of a joint staff
J-2X	joint force counterintelligence and human intelligence staff element
J-3	operations directorate of a joint staff
JFC	joint force commander
JFLCC	joint force land component commander
JP	joint publication
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications System
MASINT	measurement and signature intelligence
MDEB	multidomain effects battalion
MDMP	military decision-making process
MDTF	multidomain task force
MEA	munitions effectiveness assessment
METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations (mission variables)
MI	military intelligence
MIB-T	military intelligence brigade-theater
MIRC	United States Army Military Intelligence Readiness Command
MOS	military occupational specialty
MP	military police
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NIPRNET	Nonclassified Internet Protocol Router Network
OCONUS	outside the continental United States
OE	operational environment
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security

OSINT	open-source intelligence
PACE	primary, alternate, contingency, and emergency
PAI	publicly available information
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
RDSP	rapid decision-making and synchronization process
RFI	request for information
RSOI	reception, staging, onward movement, and integration
S-1	battalion or brigade personnel staff officer
S-2	battalion or brigade intelligence staff officer
S-2X	battalion or brigade counterintelligence and human intelligence staff officer
S-3	battalion or brigade operations staff officer
S-4	battalion or brigade logistics staff officer
S-6	battalion or brigade signal staff officer
S-9	battalion or brigade civil affairs operations staff officer
S&TI	scientific and technical intelligence
SALUTE	size, activity, location, unit, time, and equipment
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SIR	specific information requirement
SOP	standard operating procedure
SWO	staff weather officer
TACON	tactical control
TAI	target area of interest
TECHINT	technical intelligence
TLP	troop leading procedures
TPFDD	time-phased force and deployment data
TPFDL	time-phased force and deployment list
TSA	target system analysis
TSS	target selection standards
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
U.S.	United States
USAF	United States Air Force
USAR	United State Army Reserve
US BICES	United States Battlefield Information Collection and Exploitation System
WARNORD	warning order

SECTION II – TERMS

adversary

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

agility

The ability to move forces and adjust their dispositions and activities more rapidly than the enemy. (FM 3-0)

air domain

The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. (JP 3-30)

all-source intelligence

(Army) The integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations. (ADP 2-0)

all-source intelligence

(DOD) 1. Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that, in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 2-0)

antiaccess

Action, activity, or capability, usually long-range, designed to prevent an advancing enemy force from entering an operational area. (JP 3-0)

area defense

A type of defensive operation that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright. (ADP 3-90)

area denial

Action, activity, or capability, usually short-range, designed to limit an enemy force's freedom of action within an operational area. (JP 3-0)

area of operations

An operational area defined by a commander for the land or maritime force commander to accomplish their missions and protect their forces. (JP 3-0)

area reconnaissance

A form of reconnaissance operation that focuses on obtaining detailed information about the terrain or enemy activity within a prescribed area. (FM 3-90)

area security

A type of security operation conducted to protect friendly forces, lines of communications, installation routes and actions within a specific area. (FM 3-90)

ARFOR

The Army component and senior Army headquarters of all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command. (FM 3-94)

Army personnel recovery

The military efforts taken to prepare for and execute the recovery and reintegration of isolated personnel. (FM 3-50)

Army Service component command

Command responsible for recommendations to the combatant commander on the allocation and employment of Army forces. (JP 3-31)

assessment

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

attack

A type of offensive operation that defeats enemy forces, seizes terrain, or secures terrain. (FM 3-90)

battle damage assessment

The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of fires. (JP 3-0)

battle rhythm

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

biometrics

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

civil-military operations

Activities of a commander performed by designated military forces that establish, maintain, influence, or exploit relations between military forces and indigenous populations and institutions by directly supporting the achievement of objectives relating to the reestablishment or maintenance of stability within a region or host nation. (JP 3-57)

civil reconnaissance

A targeted, planned, and coordinated observation and evaluation of specific civil aspects of the environment such as areas, structures, capabilities, organizations, people, or events. (JP 3-57)

close area

The portion of the commander's area of operations where the majority of subordinate maneuver forces conduct close combat. (ADP 3-0)

close operations

Tactical actions of subordinate maneuver forces and the forces providing immediate support to them, whose purpose is to employ maneuver and fires to close with and destroy enemy forces. (FM 3-0)

collection asset

A collection system, platform, or capability that is supporting, assigned to, or attached to a particular commander. (JP 2-0)

collection management

In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 2-0)

combat assessment

The determination of the overall effectiveness of force employment during military operations. (JP 3-60)

***combat information**

A report that is gathered by or provided to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence before being used to support decision making.

combat power

(DOD) The total means of destructive and disruptive force that a military unit/formation can apply against an enemy at a given time. (JP 3-0)

combined arms

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

command and control

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

commander's critical information requirement

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

command post

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

command post cell

A grouping of personnel and equipment organized by warfighting function or by planning horizon to facilitate the exercise of command and control. (FM 6-0)

common intelligence picture

A single, identical display of relevant, instructive, and contextual intelligence information regarding enemy, adversary, and neutral force disposition, and supporting infrastructures derived from all sources at any level of classification, shared by more than one command, that facilitates collaborative planning and assists all echelons to enhance situational awareness and decision making. (JP 2-0)

common operational picture

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

communications intelligence

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

concept of operations

(Army) A statement that directs the manner in which subordinate units cooperate to accomplish the mission and establishes the sequence of actions the force will use to achieve the end state. (ADP 5-0)

consolidate gains

Activities to make enduring any temporary operational success and to set the conditions for a sustainable environment, allowing for a transition of control to other legitimate authorities. (ADP 3-0)

conventional warfare

A violent struggle for domination between nation-states or coalitions of nation-states. (FM 3-0)

convergence

An outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area. (FM 3-0)

counterintelligence

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (JP 2-0)

cover

(Army) A type of security operation done independent of the main body to protect them by fighting to gain time while preventing enemy ground observation of and direct fire against the main body. (ADP 3-90)

crime analysis

The systematic examination and interpretation of police information to determine when, where, and why crime, disorder, fear of crime, and other destabilizing events occur in specific places. (FM 3-39)

criminal intelligence

Police information compiled, analyzed, and disseminated in an effort to anticipate, prevent, or monitor criminal activity. (FM 3-39)

crisis

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

cyberspace capability

A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (JP 3-12)

cyberspace domain

The interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum. (FM 3-0)

data

In the context of decision making, unprocessed observations detected by a collector of any kind (human, mechanical, or electronic). (ADP 6-0)

deep operations

Tactical actions against enemy forces, typically out of direct contact with friendly forces, intended to shape future close operations and protect rear operations. (FM 3-0)

***deep sensing**

The employment of capabilities beyond the division coordinated fire line to collect data and information that supports targeting, situational understanding, or decision making.

defeat

To render a force incapable of achieving its objectives. (ADP 3-0)

defeat in detail

Concentrating overwhelming combat power against separate parts of a force rather than defeating the entire force at once. (ADP 3-90)

defeat mechanism

A method through which friendly forces accomplish their mission against enemy opposition. (ADP 3-0)

defense support of civil authorities

Support provided by U.S. Federal military forces, DOD civilians, DOD contract personnel, DOD 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, USC 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)

delay

When a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on enemy forces without becoming decisively engaged. (ADP 3-90)

deployment

The movement of forces into and out of an operational area. (JP 3-35)

depth

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

destroy

A tactical mission task that physically renders an enemy force combat-ineffective until reconstituted. (FM 3-90)

direct support

(Arny) A support relationship requiring a force to support another specific force and authorizing it to answer directly to the supported force's request for assistance. (FM 3-0)

disintegrate

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

dislocate

To employ forces to obtain significant positional advantage in one or more domains, rendering the enemy's dispositions less valuable, perhaps even irrelevant. (FM 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.

domain

A physically defined portion of an operational environment requiring a unique set of warfighting capabilities and skills. (FM 3-0)

electromagnetic attack

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

electromagnetic protection

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

electromagnetic reconnaissance

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

electromagnetic support

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

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-85)

electronic intelligence

Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 3-85)

employment

The strategic, operational, and tactical use of forces. (JP 5-0)

enabling operation

An operation that sets the friendly conditions required for mission accomplishment. (FM 3-90)

endurance

The ability to persevere over time throughout the depth of an operational environment. (FM 3-0)

enemy

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

estimative intelligence

Intelligence that identifies and describes adversary capabilities and intentions, and forecasts the full range of alternative future situations in relative order of probability that may have implications for the development of national and military strategy, and planning and executing military operations. (JP 2-0)

execution

The act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation. (ADP 5-0)

exploitation

(Army) A type of offensive operation following a successful attack to disorganize the enemy in depth. (FM 3-90)

explosive ordnance disposal

(Army) The detection, identification, on-site evaluation, rendering safe, exploitation, recovery, and final disposal of explosive ordnance. (FM 4-30)

field army

(Army) An echelon of command that employs multiple corps, divisions, multi-functional brigades, and functional brigades to achieve objectives on land. (ADP 3-90)

fixing force

A force designated to supplement the striking force by preventing the enemy from moving from a specific area for a specific time. (ADP 3-90)

force generation

An element of military force. It is the operation that creates and provides units for projection and employment to enable military effects and influence across multiple operational environments. It is the primary responsibility of the Services to develop, provide, and preserve forces in support of the national military strategy to enable the combatant commanders to execute their missions. (AR 525-29)

force projection

The ability to project the military instrument of national power from the United States or another theater in response to requirements for military operations. (JP 3-0)

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 aerospace, surface, and subsurface systems. (JP 2-0)

foreign intelligence entity

Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupts U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists. (DODD 5240.02)

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)

forensic science

The application of multidisciplinary scientific processes to establish facts. (DODD 5205.15E)

functional damage assessment

The estimate of the effect of military force to degrade or destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target. (JP 3-60)

fusion

Consolidating, combining, and correlating information together. (ADP 2-0)

general military intelligence

Intelligence concerning the military capabilities of foreign countries or organizations, or topics affecting potential United States or multinational military operations. (JP 2-0)

general support

Support given to the supported force as a whole and not to any particular subdivision thereof. (JP 3-09.3)

geospatial information

Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on or about the Earth, including: data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geomatics data, and related products and services. (JP 2-0)

geospatial intelligence

The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on or about the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (JP 2-0)

guard

A type of security operation done to protect the main body by fighting to gain time while preventing enemy ground observation of and direct fire against the main body. (ADP 3-90)

homeland defense

The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. (JP 3-27)

human dimension

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

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. (ADP 2-0)

identity intelligence

The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. (JP 2-0)

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 likeness and presentations produced by satellites, airborne platforms, unmanned aerial vehicles, 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 2-0)

imagery intelligence

The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. (JP 2-0)

indicator

In intelligence usage, an item of information that reflects the intention or capability of an enemy and/or adversary to adopt or reject a course of action. (JP 2-0)

information

In the context of decision making, data that has been organized and processed in order to provide context for further analysis. (ADP 6-0)

informational considerations

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

information collection

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

information dimension

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

instruments of national power

All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational, and military. (JP 1, Volume 1)

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 conducting such activities. (JP 2-0)

intelligence analysis

The process by which collected information is evaluated and integrated with existing information to facilitate intelligence production. (ADP 2-0)

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 discipline

A well-defined area of intelligence planning, collection, exploitation, analysis, and reporting using a specific category of technical or human resources. (JP 2-0)

***intelligence handover line**

A control measure between two friendly units used to pass responsibility for the conduct of information collection against a specific enemy force.

intelligence operations

(Army) The tasks undertaken by military intelligence units through the intelligence disciplines to obtain information to satisfy validated requirements. (ADP 2-0)

***intelligence preparation of the operational environment**

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

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. (ADP 2-0)

intelligence requirement

1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0)

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. (ADP 2-0)

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)

interoperability

The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (JP 3-0)

irregular warfare

(Army) The overt, clandestine, and covert employment of military and nonmilitary capabilities across multiple domains by state and non-state actors through methods other than military domination of an adversary, either as the primary approach or in concert with conventional warfare. (FM 3-0)

isolate

To separate a force from its sources of support in order to reduce its effectiveness and increase its vulnerability to defeat. (ADP 3-0)

knowledge management

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

land domain

The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. (JP 3-31)

landpower

The ability—by threat, force, or occupation—to gain, sustain, and exploit control over land, resources, and people. (ADP 3-0)

large-scale combat operations

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

lethality

The capability and capacity to destroy. (FM 3-0)

main command post

A portion of a unit headquarters containing the majority of the staff designed to command and control current operations, conduct detailed analysis, and plan future operations. (FM 6-0)

main effort

A designated subordinate unit whose mission at a given point in time is most critical to overall mission success. (ADP 3-0)

maritime domain

The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

measurement and signature intelligence

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

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

mobile defense

A type of defensive operation that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force. (ADP 3-90)

mobilization

The process by which the Armed Forces of the United States, or part of them, are brought to a state of readiness for war or other national emergency. (JP 4-05)

movement to contact

(Army) A type of offensive operation designed to establish or regain contact to develop the situation. (FM 3-90)

multidomain operations

The combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders. (FM 3-0)

munitions effectiveness assessment

The assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon system, munitions, fusing, and/or weapon delivery parameters to increase force effectiveness. (JP 2-0)

offensive operation

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

open-source intelligence

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 or unifying theme. (JP 1, Volume 1)

operational approach

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

operational environment

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

operational framework

A cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations. (ADP 1-01)

physical damage assessment

The estimate of the quantitative extent of physical damage to a target resulting from the application of military force. (JP 3-60)

physical dimension

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

planning

The art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about. (ADP 5-0)

planning horizon

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

police information

Information collected during military police operations concerning crime, disorder, criminal activity, and criminal threats. (FM 3-39)

police intelligence

The product resulting from the collection, processing, analysis, and integration of criminal intelligence and crime analysis about crime, disorder, criminal activity, and criminal threats. (FM 3-39)

police intelligence operations

The application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order. (FM 3-39)

preparation

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

priority intelligence requirement

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

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. (ADP 2-0)

pursuit

A type of offensive operation to catch or cut off a disorganized hostile force attempting to escape, with the aim of destroying it. (FM 3-90)

rear operations

Tactical actions behind major subordinate maneuver forces that facilitate movement, extend operational reach, and maintain desired tempo. (FM 3-0)

reattack recommendation

An assessment, derived from the results of battle damage assessment and munitions effectiveness assessment, providing the commander systematic advice on reattack of a target. (JP 3-60)

reconnaissance

A mission undertaken to obtain information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, geographic, or other characteristics of a particular area, by visual observation or other detection methods. (JP 2-0)

reconnaissance in force

A form of reconnaissance operation designed to discover or test the enemy's strength, dispositions, and reactions or to obtain other information. (FM 3-90)

reconnaissance-pull

Reconnaissance that determines which routes are suitable for maneuver, where the enemy is strong and weak, and where gaps exist, thus pulling the main body toward and along the path of least resistance. (FM 3-90)

reconnaissance-push

Reconnaissance that refines the common operational picture, enabling the commander to finalize the plan and support main and supporting efforts. (FM 3-90)

redeployment

(Army) The transfer of forces and materiel to home and/or demobilization stations for reintegration or out-processing. (ATP 3-35)

relative advantage

A location or condition, in any domain, relative to an adversary or enemy that provides an opportunity to progress towards or achieve an objective. (FM 3-0)

reserve

(Army) That portion of a body of troops that is withheld from action at the beginning of an engagement to be available for a decisive movement. (ADP 3-90)

retirement

When a force out of contact moves away from the enemy. (ADP 3-90)

retrograde

(Army) A type of defensive operation that involves organized movement away from the enemy. (ADP 3-90)

risk management

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

route reconnaissance

A form of reconnaissance operation to obtain detailed information of a specified route and all terrain from which the enemy could influence movement along that route. (FM 3-90)

scientific and technical intelligence

Foundational all-source intelligence that covers: a. foreign developments in basic and applied research and applied engineering techniques and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. (JP 2-0)

screen

A type of security operation that primarily provides early warning to the protected force. (ADP 3-90)

sector

An operational area assigned to a unit in the defense that has read and lateral boundaries and interlocking fires. (FM 3-0)

security operations

Those operations performed by commanders to provide early and accurate warning of enemy operations, to provide the forces being protected with time and maneuver space within which to react to the enemy, and to develop the situation to allow commanders to effectively use their protected forces. (ADP 3-90)

signals intelligence

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

site exploitation

The synchronized and integrated application of scientific and technological capabilities and enablers to answer information requirements, facilitate subsequent operations, and support host-nation rule of law. (ATP 3-90.15)

situational understanding

The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables. (ADP 6-0)

space capability

1. The ability of a space asset to accomplish a mission. 2. The ability of a terrestrial-based asset to accomplish a mission in or through space. 3. The ability of a space asset to contribute to a mission from seabed to the space domain. (JP 3-14)

space control

Operations to ensure freedom of action in space for the United States and its allies and deny a threat freedom of action in space. (JP 3-14)

space domain

(Army) The area above the altitude where atmospheric effects on airborne objects become negligible. (FM 3-0)

space situational awareness

The requisite foundational, current, and predictive knowledge and characterization of space objects and the operational environment upon which space operations depend. (JP 3-14)

special reconnaissance

Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces. (JP 3-05)

stability mechanism

The primary method through which friendly forces affect civilians in order to attain conditions that support establishing a lasting, stable peace. (ADP 3-0)

stability operation

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

striking force

A dedicated counterattack force in a mobile defense constituted with the bulk of available combat power. (ADP 3-90)

supporting effort

A designated subordinate unit with a mission that supports the success of the main effort. (ADP 3-0)

sustainment

(Army) The provision of logistics, financial management, personnel services, and health services support necessary to maintain operations until successful mission completion. (ADP 4-0)

tactical command post

A portion of a unit headquarters designed to command and control operations as directed. (FM 6-0)

target

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

target development

The systematic examination of potential target systems—and their components, individual targets, and even elements of targets—to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objectives. (JP 3-60)

targeting

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

target intelligence

Intelligence that portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 3-60)

target location error

The difference between the coordinates generated for a target and the actual location of the target. (JP 3-09.3)

tear line

A visible line on an intelligence message separating categories of information that have been approved for foreign disclosure and release. (JP 2-0)

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 enemy's technological advantages. (JP 2-0)

tempo

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

threat

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

troop leading procedures

A dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation. (ADP 5-0)

warfighting function

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

warning intelligence

Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests. (JP 2-0)

withdraw

To disengage from an enemy force and move in a direction away from the enemy. (ADP 3-90)

working group

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

zone

An operational area assigned to a unit in the offense that only has rear and lateral boundaries. (FM 3-0)

zone reconnaissance

A form of reconnaissance operation that involves a directed effort to obtain detailed information on all routes, obstacles, terrain, and enemy forces within a zone defined by boundaries. (FM 3-90)

References

All websites accessed on 12 August 2023.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. August 2023.

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

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

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

FM 1-02.2. *Military Symbols*. 18 May 2022.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/Doctrine/.

Most Department of Defense publications are available online: https://www.esd.whs.mil/DD/.

Department of Defense Law of War Manual. July 2023. Available online: https://ogc.osd.mil/.

DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*. 07 December 1982.

DODD 2310.01E. *DOD Detainee Program*. 15 March 2022.

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.

DODD 5100.20. *National Security Agency/Central Security Service (NSA/CSS)*. 26 January 2010.

DODD 5148.13. *Intelligence Oversight*. 26 April. 2017.

DODD 5205.15E. *DOD Forensic Enterprise (DFE)*. 26 April 2011.

DODD 5240.01. *DOD Intelligence Activities*. 27 August 2007.

DODD 5240.02 *Counterintelligence (CI)*. 17 March 2015.

DODD 8521.01E. *DOD Biometrics*. 13 January 2016.

DODM 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities*. 08 August 2016.

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

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

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

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

JP 3-05. *Joint Doctrine for Special Operations*. 22 September 2020.

JP 3-09.3. *Close Air Support*. 10 June 2019.

JP 3-10. *Joint Security Operations in Theater*. 25 July 2019.

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

JP 3-14. *Space Operations*. 10 April 2018.

JP 3-27. *Homeland Defense*. 10 April 2018.

JP 3-30. *Joint Air Operations*. 25 July 2019.
JP 3-31. *Joint Land Operations*. 03 October 2019.
JP 3-32. *Joint Maritime Operations*. 08 June 2018.
JP 3-33. *Joint Force Headquarters*. 09 June 2022.
JP 3-35. *Joint Deployment and Redeployment Operations*. 31 March 2022.
JP 3-57. *Civil-Military Operations*. 09 July 2018.
JP 3-59. *Meteorological and Oceanographic Operations*. 10 January 2018.
JP 3-60. *Joint Targeting*. 28 September 2018.
JP 3-61. *Public Affairs*. 17 November 2015.
JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.
JP 4-05. *Joint Mobilization Planning*. 23 October 2018.
JP 5-0. *Joint Planning*. 01 December 2020.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.
ADP 1-01. *Doctrine Primer*. 31 July 2019.
ADP 3-07. *Stability*. 31 July 2019.
ADP 3-19. *Fires*. 31 July 2019.
ADP 3-28. *Defense Support of Civil Authorities*. 31 July 2019.
ADP 3-37. *Protection*. 31 July 2019.
ADP 3-90. *Offense and Defense*. 31 July 2019.
ADP 4-0. *Sustainment*. 31 July 2019.
ADP 5-0. *The Operations Process*. 31 July 2019.
ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.
AR 11-6. *Army Foreign Language Program*. 25 February 2022.
AR 34-1. *Interoperability*. 09 April 2020.
AR 115-10/AFI 15-157 (IP). *Weather Support for the U.S. Army.* 02 September 2021.
AR 350-32. *Army Foundry Intelligence Training Program*. 02 June 2015.
AR 380-10. *Foreign Disclosure and Contacts With Foreign Representatives*. 14 July 2015.
AR 381-10. *The Conduct and Oversight of U.S. Army Intelligence Activities*. 27 January 2023.
AR 381-20. *The Army Counterintelligence Program*. 09 June 2022.
AR 381-26. *Army Foreign Materiel Program*. 30 January 2023.
AR 381-47. *Offensive Counterintelligence Operations*. 27 September 2022.
AR 381-100. *The Army Human Intelligence (HUMINT) Collection Program*. 27 August 2020.
AR 381-102. *U.S. Army Cover Program*. 04 April 2022.
AR 381-141. *Intelligence Contingency Funds (ICF).* 29 June 2020.
AR 381-143. *Non-Standard Materiel Policy and Intelligence Procedures*. 28 April 2015.
AR 525-29. *Force Generation - Sustainable Readiness*. 01 October 2019.
AR 525-95. *Army Geospatial-Intelligence and Geospatial Information and Services*. 26 July 2022.
AR 530-1. *Operations Security*. 26 September 2014.
Army Directive 2016-37. *U.S. Army Open-Source Intelligence Activities.* 22 November 2016.
ATP 2-01. *Collection Management*. 17 August 2021.
ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 01 March 2019.
ATP 2-19.1-1. *Echelons Above Corps Intelligence Organizations*. 01 March 2022.

ATP 2-19.1-2. *Echelons Above Corps Intelligence Organizations Volume II: United States Army Intelligence and Security Command.* 01 March 2022.

ATP 2-19.3. *Corps and Division Intelligence Techniques*. 08 March 2023.

ATP 2-19.4. *Brigade Combat Team Intelligence Techniques*. 25 June 2021.

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

ATP 2-22.2-2. *Counterintelligence Volume II: Operations and Collection Activities*. 22 December 2016.

ATP 2-22.4. *Technical Intelligence*. 29 October 2021.

ATP 2-22.6. *Signals Intelligence Techniques*. 17 December 2015.

ATP 2-22.6-2. *Signals Intelligence Volume II: Reference Guide.* 20 June 2017.

ATP 2-22.7. *Geospatial Intelligence*. 26 March 2015.

ATP 2-22.8. *Measurement and Signature Intelligence*. 20 May 2014.

ATP 2-22.9/MCRP 2-10A.3. *Open-Source Intelligence*. 15 August 2019.

ATP 2-22.9-2. *Open-Source Intelligence Volume II*. 15 August 2019.

ATP 2-22.31. *Human Intelligence Military Source Operations Techniques*. 17 April 2015.

ATP 2-33.4. *Intelligence Analysis*. 10 January 2020.

ATP 2-91.7. *Intelligence Support to Defense Support of Civil Authorities*. 29 June 2015.

ATP 3-01.16. *Air and Missile Defense Intelligence Preparation of the Battlefield* (AMD IPB). 31 March 2016.

ATP 3-11.37/MCRP 10-10E.7/NTTP 3-11.29/AFTTP 3-22.44. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Reconnaissance and Surveillance*. 31 March 2021.

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

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

ATP 3-21.51. *Subterranean Operations*. 01 November 2019.

ATP 3-34.10. *Engineer Platoons*. 02 February 2021.

ATP 3-34.81/MCWP 3-17.4. *Engineer Reconnaissance*. 01 March 2016.

ATP 3-35. *Army Deployment and Redeployment*. 09 March 2023.

ATP 3-37.2. *Antiterrorism*. 19 July 2021.

ATP 3-39.20. *Police Intelligence Operations*. 13 May 2019.

ATP 3-90.15. *Site Exploitation*. 28 July 2015.

ATP 3-91. *Division Operations*. 17 October 2014.

ATP 3-93. *Theater Army Operations*. 27 August 2021.

ATP 3-94.1. *Digital Liaison Detachment*. 28 December 2017.

ATP 3-94.2. *Deep Operations*. 01 September 2016.

ATP 4-32. *Explosive Ordnance Disposal (EOD) Operations*. 12 May 2022.

ATP 5-0.1. *Army Design Methodology*. 01 July 2015.

ATP 5-0.2-1. *Staff Reference Guide Volume I, Unclassified Resources*. 07 December 2020.

ATP 5-19. *Risk Management*. 09 November 2021.

ATP 6-01.1. *Techniques for Effective Knowledge Management*. 06 March 2015.

ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 30 April 2019.

ATP 7-100.3. *Chinese Tactics*. 09 August 2021.

DA PAM 25-40. *Army Publishing Program Procedures*. 14 June 2021.

FM 2-22.3. *Human Intelligence Collector Operations*. 06 September 2006.

FM 3-0. *Operations*. 01 October 2022.

FM 3-04. *Army Aviation*. 06 April 2020.
FM 3-05. *Army Special Operations*. 09 January 2014.
FM 3-12. *Cyberspace Operations and Electromagnetic Warfare*. 24 August 2021.
FM 3-13.4. *Army Support to Military Deception*. 26 February 2019.
FM 3-14. *Army Space Operations*. 20 October 2019.
FM 3-16. *The Army in Multinational Operations*. 08 April 2014.
FM 3-18. *Special Forces Operations*. 28 May 2014.
FM 3-39. *Military Police Operations*. 09 April 2019.
FM 3-50. *Army Personnel Recovery*. 02 September 2014.
FM 3-53. *Military Information Support Operations*. 04 January 2013.
FM 3-55. *Information Collection*. 03 May 2013.
FM 3-57. *Civil Affairs Operations*. 28 July 2021.
FM 3-60. *Army Targeting*. 11 August 2023.
FM 3-90. *Tactics*. 23 May 2023.
FM 3-94. *Armies, Corps, and Division Operations*. 23 July 2021.
FM 3-96. *Brigade Combat Team*. 19 January 2021.
FM 3-98. *Reconnaissance and Security Operations*. 10 January 2023.
FM 4-0. *Sustainment Operations*. 31 July 2019.
FM 4-30. *Ordnance Operations*. 01 April 2014.
FM 5-0. *Planning and Orders Production*. 16 May 2022.
FM 6-0. *Commander and Staff Organization and Operations.* 16 May 2022.
FM 6-02. *Signal Support to Operations*. 13 September 2019.
FM 6-05/MCRP 3-30.4, NTTP 3-05.19/AFTTP 3-2.73/USSOCOM PUB 3-33. *Multi-Service Tactics, Techniques, and Procedures for Conventional Forces and Special Operations Forces Integration, Interoperability, and Interdependence*. 25 January 2022.
FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.
TC 2-19.01. *Military Intelligence (MI) Company and Platoon Reference Guide*. 09 March 2021.
TC 2-19.400. *Military Intelligence Training Strategy*. 01 August 2019.
TC 2-19.401. *Military Intelligence Training Strategy for the Brigade Combat Team Tier 1*. 14 May 2019.
TC 2-19.402. *Military Intelligence Training Strategy for the Brigade Combat Team Tier 2*. 20 May 2019.
TC 2-19.403. *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3*. 25 February 2020.
TC 2-19.404. *Military Intelligence Training Strategy for the Brigade Combat Team Tier 4*. 02 March 2020.
TC 2-19.405. *Military Intelligence Training Strategy for the Brigade Combat Team Evaluator Handbook*. 05 August 2019.

OTHER PUBLICATIONS

The ICDs are available on the Office of the Director of National Intelligence, ICDs, website: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.
Titles under the USC are available on the Office of the Law Revision Counsel, USC, website: https://uscode.house.gov/.
AJP-2. *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. 24 July 2020. Available online at the NATO Standardization Office website: https://nso.nato.int/nso/.

AJP-2.1. *Allied Joint Doctrine for Intelligence Procedures*. Edition B, Version 1. 04 May 2022. Available online at the NATO Standardization Office website: https://nso.nato.int/nso/.

EO 12333. *United States Intelligence Activities*. 04 December 1981. Amended by Executive Order 13284 (2003) and 13470 (2008). Available online: https://www.archives.gov/federal-register/codification/executive-order/12333.html.

Geneva Conventions (1949). Available online: https://www.loc.gov/rr/frd/Military_Law/pdf/ASubjScd-27-1_1975.pdf.

Geneva Conventions, Protocol I (1977). Available online: https://www.loc.gov/rr/frd/Military_Law/pdf/ASubjScd-27-1_1975.pdf.

Hague Convention (1899 and 1907). Available online: https://www.loc.gov/rr/frd/Military_Law/pdf/ASubjScd-27-1_1975.pdf.

ICD 104. *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation*. 30 April 2013.

ICD 113. *Functional Managers*. 19 May 2009.

ICD 116. *Intelligence Planning, Programming, Budgeting, and Evaluation System*. 14 September 2011.

ICD 203. *Analytic Standards*. 02 January 2015.

ICD 204. *National Intelligence Priorities Framework*. 07 January 2021.

ICD 302. *Document and Media Exploitation*. 06 July 2007.

ICD 304. *Human Intelligence*. 06 March 2008.

ICD 310. *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*. 27 June 2016.

ICD 311. *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Inside the United States*. 27 June 2016.

IC Police Guidance 107.1. *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*. 11 January 2018. Available online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance.

MISC PUB 27-7. *Manual for Courts-Martial United States (2019 Edition)*. Available online through the Army Publishing Directorate website at https://armypubs.army.mil.

Public Law 109-163. *National Defense Authorization Act for Fiscal Year 2006*. 06 January 2006. Available online at https://www.govinfo.gov/app/collection/plaw.

Title 5, USC. *Government Organization and Employees*. Section 552a. *Privacy Act of 1974*.

Title 10, USC. *Armed Forces*.

Title 18, USC. *Crimes and Criminal Procedure.*

Title 32, USC. *National Guard*.

Title 50, USC. *War and National Defense*.

Uniform Code of Military Justice. Available online: https://www.loc.gov.

WEBSITES

ABCANZ Armies' Program. Available online through the All Partners Access Network website: https://community.apan.org.

Army MI Data Fundamentals. Available online through Percipio, the Army eLearning website: https://usarmy.percipio.com/.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available online: https://armypubs.army.mil/.

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

Index

Entries are by paragraph number.

Entries are by paragraph number.

D

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

This page intentionally left blank.

FM 2-0
01 October 2023

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, Acting United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2324902

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

This page intentionally left blank.

This page intentionally left blank.

This page intentionally left blank.

PIN: 081441-000