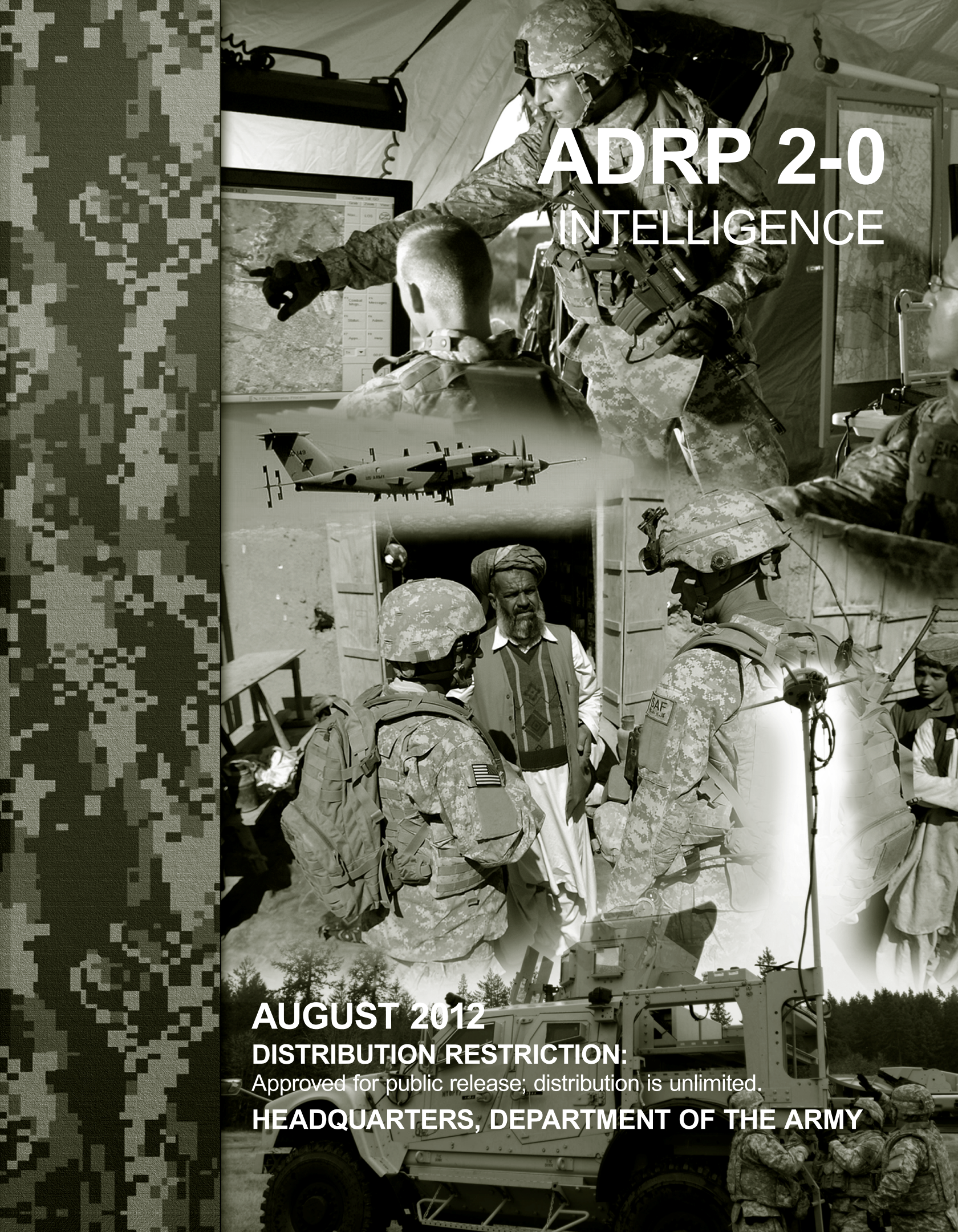

ADRP 2-0
INTELLIGENCE

AUGUST 2012

DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

*ADRP 2-0 (FM 2-0)

Army Doctrine Reference Publication
No. 2-0

Headquarters
Department of the Army
Washington, DC, 31 August 2012

Intelligence

Contents

Page

PREFACE iii
INTRODUCTION v

Chapter 1 INTELLIGENCE SUPPORT TO UNIFIED LAND OPERATIONS 1-1
Unified Land Operations 1-1
Operational Environment 1-1
Intelligence Support Within Decisive Action 1-2
Army Capabilities 1-4
Intelligence in Army Operating Forces 1-6

Chapter 2 THE ROLE OF INTELLIGENCE 2-1
The Purpose of Intelligence 2-1
Characteristics of Effective Intelligence 2-1
The Intelligence Warfighting Function 2-2
The Intelligence Enterprise 2-6
Intelligence Core Competencies 2-9
Fusion Centers 2-11

Chapter 3 THE INTELLIGENCE PROCESS 3-1
The Operations Process and the Intelligence Process 3-1
Commander's Guidance 3-3
Intelligence Process Steps 3-3
Intelligence Process Continuing Activities 3-9

Chapter 4 ARMY INTELLIGENCE CAPABILITIES 4-1
Employing Army Intelligence Capabilities 4-1
All-Source Intelligence 4-1
Single-Source Intelligence 4-2

Chapter 5 INTELLIGENCE STAFF SUPPORT 5-1
Intelligence Support to Commanders and Decisionmakers 5-1
Intelligence Support to the Army Design Methodology 5-1
Intelligence Support to the Military Decisionmaking Process 5-1
Information Collection 5-7
Intelligence Support to Targeting 5-8
Types of Intelligence Products 5-9

***This publication supersedes Chapters 1 through 13 and Appendix A of FM 2-0, dated 23 March 2010.**

Chapter 6 **FORCE PROJECTION OPERATIONS 6-1**
Force Projection 6-1
Force Projection Processes 6-2
GLOSSARY Glossary-1
REFERENCES References-1
INDEX Index-1

Figures

Figure 3-1. The intelligence process 3-2
Figure 3-2. Requirements development 3-5

Tables

Introductory table-1. New Army terms vii
Introductory table-2. Rescinded Army terms vii
Introductory table-3. Modified Army terms vii
Table 2-1. Intelligence warfighting function tasks overview 2-3
Table 5-1. Intelligence support to targeting 5-9

Preface

Army Doctrine Reference Publication (ADRP) 2-0 is the Army's reference publication for Army intelligence. It provides a common construct for intelligence doctrine from which Army forces adapt to conduct operations. It discusses—

- Intelligence in unified land operations.
- The purpose and role of intelligence.
- Intelligence core competencies.
- The intelligence warfighting function.
- The intelligence enterprise.
- The intelligence process.
- Intelligence capabilities.

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

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

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

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

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

Acknowledgment

The material in paragraph 2-63 has been used with permission from The Foundation for Critical Thinking, www.criticalthinking.org, *The Thinker's Guide to Analytic Thinking,* 2007, and *The Miniature Guide to Critical Thinking: Concepts and Tools,* 2008, by Dr. Linda Elder and Dr. Richard Paul. The copyright owners have granted permission to reproduce material from their works. With their permission, some of the text has been paraphrased and adapted for military purposes.

Introduction

SCOPE

Intelligence is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity that results in the product and to the organizations engaged in such activity (JP 2-0). Intelligence is both a process and a function that enables the Army to conduct unified land operations.

Intelligence is a function that facilitates situational understanding and supports decisionmaking. Intelligence is inherently joint, interagency, intergovernmental, and multinational and leverages the intelligence enterprise. The Army focuses its intelligence effort through the intelligence warfighting function.

To ensure the Army remains the dominant land force in the world, it requires a focused and intensive intelligence effort. The Army requires detailed intelligence on complex operational environments to support a range of military operations. Commanders have always required timely intelligence to enable operations. This continues to be true, especially for unified land operations. Operations and intelligence are inextricably linked. Intelligence is a continuous process that directly supports the operations process.

The Army focuses its intelligence effort and systematically answers requirements through the intelligence warfighting function. It must orchestrate and phase its effort to support unified land operations. The warfighting function includes specific intelligence structures and communications to leverage the intelligence enterprise at each echelon. This effort provides information and intelligence to all of the warfighting functions and directly supports the exercise of mission command.

The intelligence warfighting function is larger than military intelligence. Critical participants within the warfighting function include commanders, decisionmakers, all staff members, and intelligence leaders. The use of *intelligence leader* is new to doctrine. It refers to a larger group of military intelligence professionals than just senior leaders and commanders. *Intelligence leaders* is intended to address all military intelligence professionals who lead and supervise intelligence Soldiers, regardless of age, rank, or echelon.

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

This publication uses the term *threats*, which includes all enemies and adversaries that are a part of the operational environment. The term *hazards* refers to conditions or natural phenomena able to damage or destroy life, vital resources, and institutions, or prevent mission accomplishment.

SUMMARY OF CHANGES

ADRP 2-0 includes the following changes (located at the page number in parentheses):

Chapter 1—

- Introduces the following concepts into intelligence doctrine:
  - Unified action (1-1).
  - Unified land operations (1-1).
  - Unified action partners (1-1).
  - Intelligence support to decisive action tasks (1-2).
  - Defense support of civil authorities (1-3).
- Provides an overview of U.S. Army Intelligence and Security Command capabilities (1-6).
- Incorporates doctrine on *information collection* established in FM 3-55 (1-4).
- Adopts the joint definition of intelligence, surveillance, and reconnaissance (ISR) (1-1).

Chapter 2—

- Introduces the following *intelligence core competencies* (2-9) as the basic activities and tasks the Army uses to describe and drive the intelligence warfighting function and leverage the intelligence enterprise:
  - Intelligence synchronization (2-10).
  - Intelligence operations (2-10).
  - Intelligence analysis (2-11).
- Introduces *fusion centers* into intelligence doctrine and describes the importance of fusion centers in achieving greater efficiency between the intelligence enterprise and mission command (2-11).
- Updates the discussion on the *purpose of intelligence.* This information was addressed in FM 2-0, chapter 1 (2-1).
- Revises the discussion of the *intelligence warfighting function* found in FM 2-0, chapter 1, to more clearly account for threats, terrain and weather, and civil considerations (2-2).
- Revises the discussion of the *intelligence enterprise* found in FM 2-0, chapter 1. The discussion describes a communications-enabled intelligence network and an Army intelligence interaction with the intelligence community and enterprise in more detail (2-6).
- Revises the discussion of the *intelligence community* found in FM 2-0, chapter 1, to accurately reflect changes within joint doctrine (2-9).

Chapter 3—

- Contains a short discussion of the joint intelligence process and how it differs from the Army intelligence process (3-1).
- Modifies the *intelligence process* steps and continuing activities, replaces the *plan* step and *prepare* step with the *plan and direct* step, makes *disseminate* a step instead of a continuing activity, and deletes *generate intelligence knowledge* as a discrete continuing activity (3-1).
- Incorporates an overview of planning considerations into the *plan and direct* step of the intelligence process (3-3).

Chapter 4—

- Introduces the concept of Army intelligence capabilities (4-1).
- Introduces a discussion of single-source intelligence (4-2):
  - Describes single-source intelligence as consisting of the seven intelligence disciplines (4-2) plus the complementary intelligence capabilities (4-9).
  - Introduces cyber-enabled intelligence as a complementary intelligence capability that provides the ability to collect information and produce unique intelligence (4-10).
  - Introduces forensic-enabled intelligence as a complementary intelligence capability that can support intelligence collection and analysis (4-12).

- Introduces the concept of processing, exploitation, and dissemination (PED) as a single-source intelligence activity (4-12).
- Categorizes biometrics-enabled intelligence (4-9) and document and media exploitation (4-11) as complementary intelligence capabilities.

- Modifies the description of *all-source intelligence*. It is no longer considered an Army intelligence discipline, but an approach for developing intelligence. Army doctrine now recognizes only the seven joint intelligence disciplines (4-1).
- Removes imagery intelligence as a separate intelligence discipline. Imagery intelligence now falls under geospatial intelligence (4-3).

Chapter 5—

- Introduces and describes intelligence support to the Army design methodology (5-1).
- Moves the discussion of intelligence support to the military decisionmaking process section to chapter 5, formerly addressed under all-source intelligence in FM 2-0 (5-1).
- Adds an overview of *intelligence support to targeting* (5-8).
- Revises the discussion of the *types of intelligence products* (5-9):
  - Significantly expands the discussion of the *intelligence estimate* (5-9).
  - Incorporates material on the *intelligence summary* from FM 2-0, appendix A (5-10).

Chapter 6 updates the discussion of force projection from chapter 2 of FM 2-0.

NEW, RESCINDED, AND MODIFIED TERMS

ADRP 2-0 introduces four new Army terms (see introductory table-1), and rescinds and modifies several other terms (see introductory table-2 and introductory table-3, respectively).

Introductory table-1. New Army terms

Term	*Remarks*
fusion	Adds Army definition to existing joint term (see paragraph 4-4).
intelligence analysis	As a core competency (see paragraphs 2-61 through 2-64).
intelligence operations	As a core competency and as part of information collection (see paragraphs 2-55 through 2-60).
intelligence synchronization	As a core competency (see paragraphs 2-53 and 2-54).

Introductory table-2. Rescinded Army terms

Term	*Remarks*
broadcast dissemination	Rescinded.

Introductory table-3. Modified Army terms

Term	*Remarks*
all-source intelligence	Modified the definition—supersedes the definition in FM 2-0.
analysis	Retained based on common English usage. No longer formally defined.
biometrics-enabled intelligence	Modified the definition; new proponent publication—supersedes the definition in TC 2-22.82.
intelligence reach	Modified the definition—supersedes the definition in FM 2-0.
intelligence requirement	Adopts the joint definition.
open-source intelligence	Adopts the joint definition.

This page intentionally left blank.

Chapter 1
Intelligence Support to Unified Land Operations

UNIFIED LAND OPERATIONS

1-1. *Unified action* is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). Under unified action, commanders synchronize all military actions with activities of other governmental agencies, nongovernmental and intergovernmental organizations, and the private sector. Army contributions to unified action are called unified land operations.

1-2. Unified land operations is the Army's operational concept. It is based on the idea that Army units seize, retain, and exploit the initiative to gain a position of relative advantage over the threat. This is accomplished by decisive action. The integrated application of unified land operations enables Army forces to defeat or destroy threats, seize or occupy key terrain, protect or secure critical assets and populations, and prevent the enemy from gaining a position of advantage. The intelligence warfighting function must be adaptable to support the Army's conduct of unified land operations and decisive action.

1-3. The Army synchronizes its intelligence efforts with unified action partners to achieve unity of effort and to meet the commander's intent. Intelligence unity of effort is critical to accomplish the mission. Unified action partners are important to intelligence in all operations. Multinational and interagency partners provide cultural awareness, as well as unique perspectives and capabilities that reinforce and complement Army intelligence capabilities. Using appropriate procedures and established policy, Army intelligence leaders provide information and intelligence support to multinational forces. The G-2/S-2 staff leverages the intelligence enterprise to answer the commander's requirements.

1-4. The Army executes intelligence, surveillance, and reconnaissance (ISR) through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging the larger intelligence enterprise) and information collection. Consistent with joint doctrine, *intelligence, surveillance, and reconnaissance* is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function (JP 2-01).

1-5. Army forces often bring unique intelligence capabilities to unified action. The intelligence warfighting function provides the commander with intelligence to plan, prepare, execute, and assess operations. The two most important aspects of intelligence are enabling mission command and providing support to commanders and decisionmakers.

OPERATIONAL ENVIRONMENT

1-6. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An operational environment includes physical areas (air, land, maritime, and space domains) and the information environment, which includes cyberspace. An operational environment for any specific operation is not just isolated conditions of interacting variables that exist within a specific area of operations (AO). It also includes interconnected influences from the global or regional perspective (for example, politics and economics) that impact on conditions and operations. The operational environment in which a unit conducts operations should not be confused with training environments created by the commander for local training or the U.S. Army Training and Doctrine Command (TRADOC) common framework of scenarios used at Army training centers to prepare units for deployment.

1-7. Analysis of the broad aspects of an operational environment in terms of the operational variables provides relevant information that senior commanders use to understand, visualize, and describe the

operational environment. The operational variables are political, military, economic, social, information, infrastructure, physical environment, time (PMESII-PT). Upon receipt of a warning order (WARNORD) or mission, Army leaders filter relevant information and narrow their focus to six mission variables. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC). These variables are used during intelligence analysis and facilitate situational understanding. (See ADRP 3-0.)

INTELLIGENCE SUPPORT WITHIN DECISIVE ACTION

1-8. Within unified land operations, Army forces conduct decisive action. Army forces conduct decisive and sustainable land operations through the simultaneous combination of offensive, defensive, and stability tasks (or defense support of civil authorities [DSCA]) appropriate to the mission and environment. (See ADP 3-0.) Intelligence supports the commander within decisive action. It helps the commander visualize threats and relevant aspects of the operational environment in time and space. This support helps the commander and staff decide when and where to concentrate sufficient combat power to defeat the threat while mitigating risk.

1-9. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to visualize the operational environment and disrupt the threat simultaneously throughout the AO. The G-2/S-2 staff supports the commander with synchronization of the information collection plan to answer the commander's critical information requirements (CCIRs) and other requirements. Information collection activities are continuously assessed and updated during operations. The information collection plan should answer as many of the commander's requirements as possible. It is critical that the G-2/S-2 staff support the commander's ability to visualize threats and relevant aspects of the operational environment during the conduct of all decisive operations.

OFFENSE

1-10. Offensive tasks at all levels require effective intelligence to help the commander avoid the threat's main strength and to deceive and surprise the threat. The entire staff led by the G-2/S-2 staff develops intelligence preparation of the battlefield (IPB) products to assist the commander in identifying all aspects within the area of interest that can affect mission accomplishment. The IPB process is collaborative in nature and requires information from all staff elements and some subordinate units, who all use the results and products of the IPB process for planning.

1-11. The G-2/S-2 staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat courses of action (COAs). These assets also collect information concerning the civil considerations within the AO. The G-2/S-2 and G-3/S-3, in coordination with the rest of the staff, develop a synchronized and integrated information collection plan that satisfies the commander's information requirements.

DEFENSE

1-12. Intelligence supports the commander's defensive tasks with IPB products to identify probable threat objectives and various approaches; patterns of threat operations; the threat's vulnerability to counterattack, interdiction, electronic warfare, air attacks, and canalization by obstacles; and the threat's capability to conduct air attacks against friendly forces, insert forces behind friendly units, and employ chemical, biological, radiological, and nuclear (CBRN) weapons. The G-2/S-2 staff must also evaluate how soon the threat can employ follow-on forces.

1-13. Commanders choose to defend to create conditions for a counteroffensive that allows Army forces to regain the initiative. Other reasons for conducting a defense include to retain decisive terrain or deny a vital area to the enemy, to attrit or fix the enemy as a prelude to the offense in response to surprise action by the enemy, or to increase the enemy's vulnerability by forcing the enemy to concentrate forces. The G-2/S-2 staff supports the commander's use of information collection assets to visualize the terrain, determine threat strengths and dispositions, and confirm or deny threat COAs. Defending commanders can then decide where to arrange their forces in an economy-of-force role to defend and shape the battlefield. Intelligence analysis helps commanders decide on the precise time and place to counterattack.

STABILITY

1-14. Stability tasks encompass various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. Missions where stability tasks predominate are often much more complex than those where offensive and defensive tasks dominate. Obtaining the intelligence required is often more complex and requires leveraging the capabilities of the intelligence community and enterprise. Due to the complexity of stability tasks, commanders must be more involved in and knowledgeable of the intelligence warfighting function. Planning for stability tasks is characterized by complexity; the need to balance resources, capabilities, and activities; analyzing the significance of various activities over time; and avoiding operational pitfalls. Therefore, diverse and detailed intelligence products are important to support stability tasks.

1-15. For stability tasks, commanders often require more detailed intelligence and IPB products to determine how best to conduct operations and influence the local populace to enhance stability. The identification and analysis of threats, terrain and weather, and civil considerations are critical in determining the most effective missions, tasks, and locations in which stability tasks are conducted. For example, intelligence informs the commander well before actual deployment and drives the initial Army design methodology for each operation. A lack of knowledge concerning insurgents, local politics, customs, culture, and how to differentiate between local combatants often leads to U.S. actions that can result in unintended and disadvantageous consequences. Consequences can include attacking unsuitable targets or offending or causing mistrust among the local population. This lack of knowledge could potentially threaten mission accomplishment. (See ADP 3-07 and ADRP 3-07 for more information on stability tasks.)

DEFENSE SUPPORT OF CIVIL AUTHORITIES

1-16. *Defense support of civil authorities* is support provided by U.S. Federal military forces, Department of Defense civilians, Department of Defense contract personnel, Department of Defense component assets, and National Guard forces (when the Secretary of Defense, in coordination with the governors of the affected states, elects and requests to use those forces in Title 32, United States Code, status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events (DODD 3025.18). (For DSCA details, see JP 3-28 and ADP 3-28.)

1-17. All commanders must ensure intelligence support in DSCA remains within the guidelines of U.S. law and applicable policies. DOD 5240.1-R and AR 381-10 procedures ensure adherence to regulations, statutes, and laws concerning intelligence activities. In particular, intelligence operations must adhere to regulations and directives that implement restrictions in compliance with intelligence oversight requirements. Intelligence support of Army forces under Title 10, United States Code (USC), focus on specific missions authorized by the Secretary of Defense. Further, any use of intelligence capabilities for purposes other than traditional use must be expressly approved by the Secretary of Defense. Information collection conducted to support the incident commander focuses on saving lives and reducing risk to Army forces. Commanders executing DSCA tasks ensure their intelligence capabilities comply with applicable policies, regulations, U.S. law, or the missions authorized by the governor of that state. Commanders and intelligence professionals consult with staff judge advocates concerning any unclear areas of intelligence activities. (For more information on title considerations, see JP 3-28 and ADP 3-28.)

1-18. Intelligence analysis can also assist civil authorities in identifying areas where the military can provide support to restoring essential services. Army forces involved in DSCA conduct *incident awareness and assessment* (IAA). Information collection assets and intelligence analysis assist in search and rescues, damage assessments, identifying potential hazards, and locating isolated persons. They also assist in detecting, locating, and identifying CBRN materiel and weapons. Employment of Active Army and Army Reserve intelligence activities and operations requires authorization from the Secretary of Defense or designated representative. (See TC 2-91.7 for more information on intelligence support to DSCA.)

ARMY CAPABILITIES

1-19. Army intelligence has responsibilities and functions that support decisive action at all echelons. The distribution of specific intelligence assets enhances the capability of the combined arms team to concentrate combat power and minimize risk. G-2/S-2 staffs conduct analysis and planning to tailor intelligence capabilities to support the mission. The task organization that follows force tailoring establishes an ordered command and support structure with technical channels for intelligence operations.

COMBINED ARMS

1-20. *Combined arms* is the synchronized and simultaneous application of arms to achieve an effect greater than if each arm was used separately or sequentially (ADRP 3-0). As an integral part of combined arms, staffs identify all information collection capabilities required to conduct operations. Specific intelligence capabilities that are not organic are requested from the force pool.

FORCE TAILORING

1-21. *Force tailoring* is the process of determining the right mix of forces and the sequence of their deployment in support of a joint force commander (ADRP 3-0). Force tailoring involves selecting the right force structure for a joint operation from available units within a combatant command or from the Army force pool. Based on mission analysis, the staff at each echelon identifies information collection capabilities and resources to support the commander's guidance, intent, and mission objectives.

TASK-ORGANIZING

1-22. *Task-organizing* is the act of designing an operating force, support staff, or sustainment package of specific size and composition to meet a unique task or mission (ADRP 3-0). Characteristics to examine when task-organizing the force include but are not limited to training, experience, equipping, sustainability, operational environment (including the threat), and mobility. For Army forces, it includes allocating available assets to subordinate commanders and establishing their command and support relationships.

1-23. Each echelon task-organizes intelligence assets to best support the mission. Intelligence assets are task-organized within a tailored force package for specific missions. As commanders reorganize units for subsequent missions, information collection assets may be redistributed to support new or changing requirements.

INFORMATION COLLECTION

1-24. *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 of systems in direct support of current and future operations (FM 3-55). (See FM 3-55 and ATTP 2-01 for more information on information collection and planning requirements and assessing collection.) The G-2/S-2 and G-3/S-3 staffs collaborate to collect, process, and analyze information the commander requires concerning threats, terrain and weather, and civil considerations that affect operations. The information collection tasks are—

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

1-25. Collection consists of collecting, processing, and reporting information in response to information collection tasks for a particular area of interest. A successful information collection effort results in the timely collection and reporting of relevant and accurate information, which either supports the production of intelligence or is disseminated as combat information. The information collection effort includes organic units and capabilities and support from the entire intelligence enterprise, as well as nonintelligence sources (that provide civil considerations and sociocultural information).

Plan Requirements and Assess Collection

1-26. The G-2/S-2 staff (in collaboration with the commander and staff) receives and validates requirements for collection, prepares the planning requirements tools, recommends information collection assets and capabilities to the G-3/S-3 staff, and maintains synchronization as operations progress. (See ATTP 2-01.) These specific requirements are focused in time and space to support decisionmaking.

Task and Direct Collection

1-27. In order to synchronize information collection, the G-2/S-2 staff recommends the tasking of information collection assets and capabilities to the G-3/S-3 staff, tracks the information collection effort, and recommends changes to collection as the situation changes. The G-3/S-3 (based on recommendations from the staff) tasks, directs, and, when necessary, retasks information collection assets.

Execute Collection

1-28. Executing collection focuses on specific requirements. This collection is accomplished through the execution of tactical missions (such as the primary means of information collection: reconnaissance, surveillance, security operations, and intelligence operations) based on the CCIRs and other requirements. Collection activities acquire data and information about threats and relevant aspects of the AO. They provide that information to intelligence processing and production elements. Typically, collection activities begin soon after receipt of the mission and continue throughout preparation and execution of operations. They do not cease at the conclusion of the operation but continue as required. This allows the commander to focus combat power, execute current operations, and prepare for future operations simultaneously.

COMMAND AND SUPPORT RELATIONSHIPS

1-29. Command and support relationships provide the basis for unity of command in operations. Commanders use Army command and support relationships when task-organizing military intelligence (MI) assets and units. Since most MI forces are task-organized to support operations, intelligence leaders at all echelons must understand the differences between joint and Army doctrine and the impact of command and support relationships on their units, personnel, and assets. (See JP 1 for a discussion of joint command relationships and authorities; see ADPR 5-0 for a discussion of Army command and support relationships.)

TECHNICAL CHANNELS

1-30. While not a command or support relationship, technical channels often affect intelligence operations. Through technical channels, commanders and staffs ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant U.S. law, the law of war, international law, Department of Defense (DOD) directives and instructions, and orders. Regulatory authority is maintained by national and DOD intelligence agencies for specific intelligence discipline collection and is passed through technical channels.

1-31. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess the unit's collection effort. Technical channels also involve translating information collection tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the information collection effort. Technical channels include but are not limited to—

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

INTELLIGENCE IN ARMY OPERATING FORCES

1-32. The Army employs brigade combat teams (BCTs) with division and corps headquarters that operate subordinate to the theater Army structure. G-2/S-2 staffs, units, and organizations within these structures operate as mutually supporting entities that ensure information and intelligence are shared across echelons to support commanders at all levels.

DIVISION AND ABOVE INTELLIGENCE ORGANIZATIONS

1-33. The Army Service component command (ASCC) G-2, corps G-2, and division G-2 provide intelligence support to each respective command and subordinate units. The G-2 provides information and intelligence required to facilitate situational understanding and support decisionmaking across the full range of military operations. The G-2 manages and directs the intelligence effort during operations.

1-34. The U.S. Army Intelligence and Security Command (INSCOM) conducts multidiscipline intelligence operations, aerial reconnaissance and surveillance, cyber warfare, and knowledge management for the intelligence enterprise. Additionally, INSCOM delivers specialized quick-reaction capabilities, advanced skills training, and linguist support for deploying forces to support Army and joint commands, coalition partners, and the intelligence community.

1-35. There are two types of units assigned to INSCOM—theater MI brigades and functional commands. There are five theater MI brigades, each one tailored for the theater it supports. These brigades provide collection, processing, analysis, and dissemination support to the ASCCs, combatant commanders, and the intelligence community. INSCOM theater MI brigades are assigned through the appropriate joint documentation process to regional combatant commands. Regional combatant commands routinely provide these brigades in an OPCON relationship to the supporting ASCCs.

1-36. Functional commands within INSCOM have missions and capabilities focused on a single discipline or operational function. Examples of this type of command are the 902d MI Group (Counterintelligence [CI]) and the Army Operations Group (Human Intelligence [HUMINT]) operating in direct support of Army requirements, and the 704th MI Brigade and 706th MI Group providing signals intelligence (SIGINT) functional capabilities in direct support of Director of National Intelligence (DNI) mandated missions. INSCOM's functional brigades, while not regionally aligned, work in coordination with INSCOM's theater MI brigades, to effectively create a seamlessly integrated tactical to national intelligence enterprise.

1-37. Divisions and corps can act as joint headquarters. In this capacity, they normally require augmentation with additional intelligence capabilities to effectively meet joint force requirements. Joint intelligence operations are wide-ranging activities conducted by G-2/S-2 staffs and organizations to provide commanders and national-level decisionmakers with timely, relevant, accurate, predictive, and tailored intelligence.

BRIGADE AND BELOW INTELLIGENCE CAPABILITIES

1-38. The BCT intelligence organization develops situational understanding of threats, terrain and weather, and civil considerations and synchronizes intelligence activities. The BCT S-2 uses available capabilities and leverages the intelligence enterprise to provide intelligence products and support the BCT commander. Information collection activities answer CCIRs and other requirements. The BCT is supported by an organic MI company. MI company support includes collection, processing, analysis, and dissemination of intelligence information and products. Information and intelligence from the BCT is critical to the intelligence enterprise, especially intelligence specific to the BCT's AO. (For more information on brigade and below intelligence capabilities, see FM 2-0.)

Chapter 2
The Role of Intelligence

THE PURPOSE OF INTELLIGENCE

2-1. The purpose of intelligence is to support commanders and staffs in gaining situational understanding of threats, terrain and weather, and civil considerations. Intelligence supports the planning, preparing, execution, and assessment of operations. The most important role of intelligence is to support commanders and decisionmakers. The Army generates intelligence through the intelligence warfighting function.

2-2. Intelligence leaders ensure that the intelligence warfighting function operates effectively and efficiently. They are the commander's primary advisors on employing information collection assets and driving information collection. Additionally, intelligence analysts support their commanders with analysis and production of timely, relevant, accurate, and predictive assessments and products tailored to the commander's specific needs.

2-3. Commanders require intelligence about the threat and other aspects of the operational environment before and during operations to effectively accomplish their missions. Intelligence helps commanders visualize the operational environment, organize their forces, and control operations to achieve their objectives by answering specific requirements focused in time and space.

2-4. Intelligence supports protection by alerting commanders to threats and assisting in preserving and protecting the force. All-source analysts depend on information collection assets for accurate and detailed information about threats and relevant aspects of the operational environment. They make their most significant contributions when they accurately assess (predictive assessment) possible threat events and actions.

2-5. Predictive assessments facilitate the commander's visualization and support decisionmaking. This is accomplished by answering specific requirements focused in time and space and identifying any threats to mission accomplishment. Intelligence leaders provide the commander with predictive assessments that consider all aspects of threats, terrain and weather, and civil considerations, and should provide the commander with an estimate regarding the degree of confidence the intelligence leader places in each analytic assessment. Intelligence analysis is not perfect and can be extremely time consuming and difficult. The G-2/S-2 staff must provide most likely and most dangerous threat COAs based on threat intent and capabilities during wargaming.

CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

2-6. The effectiveness of intelligence is measured against the relevant information quality criteria:

- **Accuracy.** Intelligence gives commanders an accurate, balanced, complete, and objective picture of the threat and other aspects of the operational environment. To the extent possible, intelligence should accurately identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and unbiased intelligence.
- **Timeliness.** Intelligence provided early supports operations and prevents surprise from threat actions. It must flow continuously to the commander before, during, and after an operation. Intelligence organizations, databases, and products must be available to develop estimates, make decisions, and plan operations.
- **Usability.** Intelligence must be in the correct data file specifications for databasing and display. Usability facilitates further analysis, production of intelligence, integration of the product across the staff, and use within operations.

- **Completeness.** Intelligence briefings and products convey all of the necessary components to be as complete as possible.
- **Precision.** Intelligence briefings and products provide the required level of detail and complexity to answer the requirements.
- **Reliability.** Intelligence evaluates and determines the extent to which the collected information and the information being used in intelligence briefings and products are trustworthy, uncorrupted, and undistorted. Any concerns with the reliability of intelligence must be stated up front.

2-7. Besides the relevant information quality criteria, intelligence must meet three additional criteria:

- **Relevant.** Intelligence supports the commander's requirements.
- **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 G-2/S-2 staff should anticipate the commander's intelligence needs.
- **Tailored.** Intelligence is shared and disseminated in the format requested by the commander, subordinate commanders, and staffs. It should support and satisfy the commander's priorities. The G-2/S-2 staff presents clear, concise intelligence that meets the commander's preferences, facilitates situational understanding, and is usable for decisionmaking or other action.

THE INTELLIGENCE WARFIGHTING FUNCTION

2-8. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations (ADRP 3-0). For purposes of the definition, the term *enemy* includes the entire range of threats, and the term *terrain* includes weather. Participation in the warfighting function is not related to who processes, collects, analyzes, and disseminates the information. The intelligence warfighting function is larger than MI.

2-9. The commander drives intelligence, intelligence facilitates operations, and operations are supportive of intelligence; this relationship is continuous. The intelligence warfighting function is always engaged in supporting the commander in offensive, defensive, stability tasks, and, when directed, DSCA tasks. The combination of space, aerial, seaborne, and collection systems and analytical organizations and elements provide the most comprehensive intelligence possible.

2-10. Commanders' considerations for the intelligence warfighting function include—

- Reducing operational uncertainty. Intelligence does not eliminate uncertainty entirely. Commanders determine prudent risks inherent in any operation.
- Determining the appropriate balance between the time allotted for collection and operational necessity. It takes time to collect information and then develop that information into detailed and precise intelligence products.
- Prioritizing finite resources and capabilities.
- Resourcing and prioritizing the warfighting function appropriately to have enough network capability and access to meet the commander's needs.
- Employing organic and supporting collection assets as well as planning, coordinating, and articulating requirements to leverage the entire intelligence enterprise.

INTELLIGENCE WARFIGHTING FUNCTION TASKS

2-11. The intelligence warfighting function facilitates support to the commander and staff through a broad range of supporting Army Universal Tasks List (AUTL) tasks. These tasks are interrelated, require the participation of the commander and staff, and are often conducted simultaneously. The intelligence warfighting function tasks facilitate the commander's visualization and understanding of the threat and other relevant aspects of the operational environment. The intelligence warfighting function tasks are—

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

2-12. Table 2-1 illustrates how these tasks support the commander. (See FM 7-15, chapter 2, for the complete list of tasks and their measures of performance.)

Table 2-1. Intelligence warfighting function tasks overview

Intelligence tasks ►	*Commander's focus ►*	*Commander's decisions*
Support to force generation • Provide intelligence readiness. • Establish an intelligence architecture. • Provide intelligence overwatch. • Generate intelligence knowledge. • Tailor the intelligence force.	Orient on contingencies.	Should the unit's level of readiness be increased? Should the operation plan be implemented?
Support to situational understanding • Perform intelligence preparation of the battlefield. • Perform situation development. • Provide intelligence support to protection. • Provide tactical intelligence overwatch. • Conduct police intelligence operations. • Provide intelligence support to civil affairs activities.	Plan an operation. Prepare. Execute. Assess. Secure the force. Determine 2d and 3d effects on operations and the populace.	Which course of action will be implemented? Which enemy actions are expected? What mitigation strategies should be developed and implemented to reduce the potential impact of operations on the population?
Conduct information collection • Plan requirements and assess collection. • Task and direct collection. • Execute collection.	Plan an operation. Prepare. Execute. Assess.	Which decision points, high-payoff targets (HPTs), and high-value targets (HVTs) are linked to the threat's actions? Are the assets available and in position to collect on the decision points, HPTs, and HVTs? Have the assets been repositioned for branches or sequels?
Support to targeting and information capabilities • Provide intelligence support to targeting. • Provide intelligence support to inform and influence activities. • Provide intelligence support to cyber electromagnetic activities. • Provide intelligence support to combat assessment.	Use lethal or nonlethal effects against targets. Destroy, suppress, disrupt, or neutralize targets. Reposition intelligence or attack assets.	Are the unit's lethal and nonlethal effects and maneuver effective? Which targets should be re-engaged? Are the unit's inform and influence activities effective?

2-13. There are intelligence-related AUTL tasks beyond the four most significant intelligence warfighting tasks in table 2-1. Soldiers, systems, and units from all branches conduct intelligence-related AUTL tasks. Every Soldier, as a part of a small unit, is a potential information collector. Soldiers develop a special awareness simply due to exposure to events occurring in the AO, and have the opportunity to collect and report information based on their observations and interactions with the local population. The increased awareness that Soldiers develop through personal contact and observation is a critical element of the unit's ability to understand the operational environment more fully.

2-14. Therefore, the Army established the every Soldier is a sensor (ES2) program, which is accomplished through Soldier surveillance and reconnaissance. The Soldier surveillance and reconnaissance AUTL task is designed to help units more effectively collect useful information in their AO. This task is critical because units often operate in an AO characterized by violence, uncertainty, and complex threats. (See FM 2-91.6 for a detailed discussion about Soldier surveillance and reconnaissance.)

2-15. In some cases, there are certain sensitivities and limitations to personnel conducting information collection—for example, civil affairs and medical Soldiers. Medical personnel cannot be assigned information collection tasks due to their Geneva Convention category status. If medical personnel do gain information through casual observation of activities in plain sight while conducting their duties, they will report the information to their chain of command.

FACILITATING UNDERSTANDING

2-16. Conducting (planning, preparing, executing, and assessing) military operations requires intelligence products regarding threats and relevant aspects of the operational environment. These intelligence products enable commanders to identify potential COAs, plan operations, employ forces effectively, employ effective tactics and techniques, and implement protection.

THREATS AND HAZARDS

2-17. Although threats are a fundamental part of an operational environment for any operation, they are discussed separately here simply for emphasis. 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 (ADRP 3-0). Threats may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances. (See ADRP 3-0.) The intelligence warfighting function analyzes nation-states, organizations, people, or groups to determine their ability to damage or destroy life, vital resources, and institutions, or prevent mission accomplishment. Threats are sometimes categorized as traditional, irregular, disruptive, and catastrophic. While helpful in generally describing the nature of the threat, these categories do not precisely describe the threat's goals, organizations, and methods of operating.

2-18. Intelligence provides a deep understanding of the threat and how the threat can affect mission accomplishment, which is essential to conducting operations. Commanders and staffs must understand how current and potential threats organize, equip, train, employ, and control their forces. Therefore, the intelligence warfighting function must continually identify, monitor, and assess threats as they adapt and change over time.

2-19. Hazards are conditions or natural phenomena able to damage or destroy life, vital resources, and institutions, or prevent mission accomplishment. Understanding hazards and their effects on operations allows the commander to better understand the terrain, weather, and various other factors that best support the mission. It also helps the commander visualize potential impacts on operations. Successful interpretation of the environment aids in correctly applying threat COAs within a given geographical region. Hazards include disease, extreme weather phenomena, solar flares, and areas contaminated by toxic materials.

TERRAIN AND WEATHER

2-20. Terrain aspects and weather conditions are inseparable, directly influence each other, and impact military operations based on the mission variables (METT-TC). Terrain analysis involves the study and interpretation of natural and manmade features of an area, their effects on military operations, and the

effects of weather and climate on these features. Terrain analysis is a continuous process. Analyzing military aspects of terrain includes collection, analysis, evaluation, and interpretation of geographical information on natural and manmade features of the terrain. Then analysts combine other relevant factors with the terrain and weather to predict their effects on military operations.

2-21. Weather analysis evaluates forecasted weather effects on operations and various systems. Analysts should evaluate the effects of each military aspect of weather. However, just as in terrain analysis, they should focus on the aspects that have the most bearing on operations and decisionmaking. The evaluation of each aspect should begin with operational climatology and current weather forecasts. Analysts fine-tune the evaluation to determine the effects based on specific weather sensitivity thresholds for friendly and threat forces and systems.

CIVIL CONSIDERATIONS AND SOCIOCULTURAL UNDERSTANDING

2-22. Civil considerations may be expressed using the joint systems perspective, the operational variables, or the mission variables. Intelligence analysts leverage information from many different sources, including open sources, to provide predictive intelligence and facilitate a broad understanding of the operational environment.

2-23. Analysts can draw relevant information from analysis of the operational environment using the operational variables (PMESII-PT). However, upon receipt of the mission, Army forces use ASCOPE (areas, structures, capabilities, organizations, people, and events) characteristics to describe civil considerations as part of the mission variables (METT-TC) during IPB. Additionally, a human terrain system team can provide detailed information and analysis pertaining to the sociocultural factors involved in the operation. (For additional information on ASCOPE and IPB, see FM 2-01.3.)

2-24. Culture is a key factor in understanding all of the ASCOPE characteristics. Understanding a culture has become an increasingly important competency for Soldiers. Culture is the shared beliefs, values, customs, behaviors, and artifacts members of a society use to cope with the world and each other. Individuals belong to multiple groups through birth, assimilation, or achievement. Individuals' groups influence their beliefs, values, attitudes, and perceptions. As such, culture is internalized—it is habitual, taken for granted, and perceived as natural by people in the society.

2-25. Cultures—

- Influence people's range of action and ideas including *what* to do and not do, *how* to do or not do it, and with *whom* to do it or not do it.
- Include the circumstances for shifting and changing rules.
- Influence how people make judgments about *what* is right and wrong and *how* to assess what is important and unimportant.
- Affect how people categorize and deal with issues that do not fit into existing categories.
- Provide the framework for rational thoughts and decisions. However, what one culture considers rational may not be rational to another culture. (See FM 3-24 for a discussion of sociocultural analysis.)

2-26. Army leaders seek to understand the situation in terms of the local cultures while avoiding their own cultural biases. Understanding other cultures applies to all operations, not only those dominated by stability. For example, different tactics may be used against a threat who considers surrender a dishonor worse than death, as compared to those threats for whom surrender remains an honorable option.

2-27. Sociocultural factors expand on cultural factors. *Sociocultural factors* are the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment (JP 2-01.3). Sociocultural research and analysis provides information that supports commander and staff situational awareness.

2-28. Cultural and sociocultural understanding is also crucial to the success of multinational operations. Army leaders take the time to learn customs and traditions as well as the operational procedures and doctrine of their multinational partners and those of the host nation. To operate successfully in multinational settings, Army leaders must recognize any cultural differences as well as differences in the interpretation of orders and instructions. They must learn how and why others think and act as they do.

THE INTELLIGENCE ENTERPRISE

2-29. The intelligence enterprise is the sum total of the intelligence efforts of the entire U.S. intelligence community. The intelligence warfighting function is the Army's contribution to the intelligence enterprise. The intelligence enterprise comprises all U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes supported by a network-enabled architecture. The most important element of the intelligence enterprise is the people that make it work.

2-30. The value of the intelligence enterprise is the ability it provides to leverage information from all unified action partners, including access to national capabilities, as well as nonintelligence information, larger volumes of information and intelligence, and specialized analysis by unified action partners. Collaboration is the central principle of conducting analysis within the intelligence enterprise. Army units provide accurate and detailed intelligence on the threats and relevant aspects of the operational environment (especially those related to Army activities), while other portions of the intelligence enterprise provide expertise and access not readily available to the Army. Additionally, the enterprise provides governance over certain intelligence methods and activities. Cooperation benefits everyone within the intelligence enterprise.

2-31. Analysts leverage the intelligence enterprise to create a more comprehensive and detailed assessment of threats and relevant aspects of the operational environment (such as civil and cultural considerations) to facilitate mission command. An example of achieving greater efficiency between the intelligence enterprise and mission command is the creation of fusion centers. Fusion centers are ad hoc cells designed to enable lethal and nonlethal targeting, facilitate current or future operations, and inform decisionmaking. (See paragraphs 2-65 through 2-69 for more information on fusion centers.)

INTELLIGENCE COMMUNICATIONS ARCHITECTURE

2-32. The intelligence enterprise is communications network-enabled. The backbone is based on a communications architecture that transmits intelligence and information to and from various collection elements, units, and agencies by means of different technologies and systems. With the continued development of sensors, processors, and communications systems, it is increasingly important to understand the requirements of establishing an effective communications architecture. Adequate communications and access to the intelligence enterprise is often the most critical enabler for the intelligence warfighting function. The G-2/S-2 staff must identify the specific intelligence warfighting function requirements to the unit's overall communications architecture.

2-33. The intelligence communications architecture provides specific intelligence and communications structures at each echelon, from the national level through the tactical level. These structures include all personnel, organizations, systems, and procedures necessary for planning, preparing, collecting, producing, and disseminating intelligence. The commander and staff must provide the resources and bandwidth necessary for the architecture based on realistic expectations for intelligence and information collection capabilities.

2-34. The G-2/S-2 staff must collaborate closely with the G-6/S-6 to coordinate for the required communications links. The G-2/S-2 staff requires classified and unclassified network connections for its equipment. If elements of the G-2/S-2 staff will be working outside the range of the unit's communications systems, then it is necessary to coordinate for global or extended-range communications. Leaders must obtain the required type and amount of communications equipment and related components. They must possess and be familiar with all of the instructions, passwords, policies, regulations, and directives required for operations security. They must also ensure Soldiers are trained in the use and procedures involved in operating communications equipment. Intelligence leaders must verify the fills, frequencies, alternate frequencies, and reactions during jamming, as well as reporting guidelines for specific information.

2-35. The following is a simple list of considerations (not all-inclusive) of the questions that the staff must answer to establish the intelligence communications architecture:

- Where are the unit's collectors?
- What are the unit's intelligence processing capabilities?
- What are the information exchange rates on each network relative to the network capacity?
- Where are the unit's intelligence production elements?

- Where are the unit's decisionmakers?
- How does the unit disseminate information to its decisionmakers and consumers?
- How long does it take to pass certain reports and products?
- Are the systems within the intelligence communications architecture (collection, production, and processing) compatible with each other? For example, satellite communications.
- How does the unit work around incompatibility within the warfighting function architectures?
- How can the unit access databases and information from higher and other agencies? Are there special requirements necessary to access these databases, such as a security clearance, polygraph, training, or certification?
- How are unified action partners integrated into the intelligence communications architecture?

LEVERAGING THE INTELLIGENCE ENTERPRISE

2-36. The effectiveness of the intelligence warfighting function hinges directly on access to the intelligence community through the intelligence enterprise. It also provides units the ability to leverage information and capabilities. This includes access to national capabilities, larger volumes of information and intelligence, and specialized analysis. Leveraging the enterprise allows analysts to collaborate with analysts throughout the theater and the intelligence community. Some of the most important activities that facilitate collaboration within the intelligence enterprise include intelligence reach, granting access, sharing, posting, updating the common operational picture (COP), and knowledge management.

Intelligence Reach

2-37. ***Intelligence reach*** **is the activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command**. The G-2/S-2 staff must determine how best to support the unit's mission with intelligence reach capabilities. Detailed planning and training are critical to the success of intelligence reach operations. Intelligence reach supports distributed analysis to answer CCIRs and other requirements. It allows intelligence analysts to retrieve existing information, intelligence products, and data that can support answering CCIRs and other requirements from outside the unit, in a timely manner, without waiting for an answer to a request for information (RFI) or an information collection task. The information, intelligence products, or data retrieved can then be evaluated for use in the unit's intelligence products or analysis. Procedures to gain and maintain access and permissions are an important part of intelligence reach.

2-38. Knowledge management is an important part of dissemination. The right information must flow to the right users at the right time without inundating the users. The intelligence warfighting function uses the intelligence process as the management tool to ensure the right information gets to the right user at the right time in a useable format. Intelligence leaders must also ensure users do not receive the same information from the same original source multiple times. Circular reporting can result in erroneous analysis by intelligence professionals or negatively impact commanders' decisionmaking.

Granting Access

2-39. Properly managing access to databases, information, or intelligence ensures personnel, units, or organizations that need all or part of the information can obtain the information they need. Information resides in classified and unclassified databases, programs, networks, systems, and other Web-based collaborative environments maintained by unified action partners. Granting access is governed by—

- Applicable national agencies.
- Multinational, joint, and Army regulations, policies, and procedures.
- Individual system accreditation.
- Specialized training for clearances and systems or database usage.
- Special security procedures and enforcement.

2-40. The G-2/S-2 staff must identify users who will require access to protected unit intelligence Web sites, Web postings, data files, and databases. The G-2/S-2 staff also processes requests from individuals, organizations, or agencies outside the unit who may require access.

2-41. The G-2/S-2 staff must ensure all accesses granted conform to the appropriate U.S. law, DOD regulations, classification guidelines, and security protocols. (See AR 380-28 [C], DHE-M 3301.001 [S], and DHE-M 3301.002 [S].)

Sharing

2-42. Sharing is most effectively accomplished through a Web-based collaborative environment, such as the use of cloud technology. Collaboration includes the sharing of knowledge, expertise, and information. Collaboration may take many forms. Collaborative tools include computer-based tools that help individuals work together and share information. They allow for virtual online meetings and data sharing. Sharing allows analysts, other intelligence professionals, and other subject matter experts to freely exchange information and intelligence.

2-43. The G-2/S-2 staff must identify the most effective methods to share intelligence with all required users—some users may require hardcopy printouts of new or updated intelligence, some may simply need to access the unit intelligence Web page, and some may simply require access to specific unit databases. Sharing applies to multinational partners who may be unable to access U.S. information systems or data files. Intelligence professionals must actively work with the foreign disclosure officer to ensure that information is shared. This may require the development of special systems or procedures to facilitate sharing.

Posting

2-44. Information may be posted to military Web sites for the widest possible dissemination. This makes the information available to personnel and units interested in the information or intelligence that are not part of the normal dissemination group for a unit or organization. When posting information to the Web or updating information on their Web site, it is critical for units or organizations to inform higher, subordinate, and lateral units or organizations that may require this information. Units rarely have enough personnel to dedicate a Soldier to continuously search Web sites for new or updated information that may be of use to that unit or organization. The G-2/S-2 staff must regularly review posted information to ensure it remains valid, relevant, and current.

Updating the Common Operational Picture

2-45. As required by unit standard operating procedures (SOPs), the G-2/S-2 section inputs new or updated intelligence and information in the COP to help the commander and staff visualize the operational environment. The *common operational picture* is a single 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 (ADRP 6-0). This display is the result of reports, automatic updates, and overlays common to all echelons and digitally stored in a common database. The COP facilitates mission command through collaborative interaction and real-time sharing of information between commanders and staffs. This convergence of intelligence and the other warfighting functions is critical to operations. The intelligence portions of the COP are those messages and overlays relating to threats, terrain and weather, and civil considerations in the common database. This intelligence and information originate from intelligence organizations at various echelons and combat information. The G-2/S-2 ensures the common database reflects the most current information and intelligence available in order to maintain the integrity of the intelligence portion of the COP.

THE INTELLIGENCE COMMUNITY

2-46. The effectiveness of the intelligence warfighting function hinges directly on collaboration and unity of effort within the intelligence community. Numerous DOD and non-DOD agencies and organizations in the intelligence community support Army operations by providing specific intelligence products and services. The intelligence community has become increasingly important as new technologies facilitate collaborative analysis and production. Intelligence community members establish standards in their

respective specialties. Effective G-2/S-2 staffs are familiar with these organizations and the methods of obtaining information from them as necessary. (See JP 2-0.)

2-47. The DNI has overall responsibility for intelligence support to the President and day-to-day management of the intelligence community. Specifically, the DNI establishes objectives and priorities for the intelligence community, and manages and directs the tasking of national intelligence collection, analysis, production, and dissemination. The DNI implements policies and procedures to ensure national all-source intelligence includes competitive analysis and alternative views. Additionally, the Office of the DNI exercises control over the National Intelligence Council, National CI Executive, National Counterterrorism Center, and National Counterproliferation Center. (See JP 2-0.)

2-48. The intelligence community consists of national-level organizations that provide intelligence support to the U.S. Government (including DOD). Maintaining cooperative relationships with the members of the intelligence community facilitates requirements management, complements Army intelligence capabilities, and promotes the timely flow of critical intelligence. Some of these agencies provide liaison elements to Army forces. (See JP 2-01 for a description of the support these agencies and organizations provide to joint operations and intelligence.)

Department of Defense Agencies

2-49. DOD members of the intelligence community include—

- Defense Intelligence Agency (DIA).
- National Geospatial-Intelligence Agency (NGA).
- National Reconnaissance Office (NRO).
- National Security Agency (NSA)/Central Security Service (CSS).
- Service components (U.S. Air Force, U.S. Army, U.S. Marine Corps, and the U.S. Navy).

Other Members of the Intelligence Community

2-50. Operations require knowledge of both military and nonmilitary aspects of the operational environment. Much of this expertise falls outside the purview of DOD members of the intelligence community. Intelligence professionals should be familiar with the roles and responsibilities of the following non-DOD members of the intelligence community:

- Central Intelligence Agency (CIA).
- Department of Energy (DOE).
- Department of Homeland Security (DHS).
- Department of State (DOS).
- Department of the Treasury (TREAS).
- Drug Enforcement Administration (DEA).
- Federal Bureau of Investigation (FBI).
- U.S. Coast Guard (USCG).

INTELLIGENCE CORE COMPETENCIES

2-51. The intelligence core competencies are the most basic activities and tasks the Army uses to describe and drive the intelligence warfighting function and leverage the intelligence enterprise. The core competencies are intelligence synchronization, intelligence operations, and intelligence analysis. The commander and staff must thoroughly understand the core competencies to apply the intelligence process and leverage the intelligence enterprise.

2-52. The intelligence core competencies also serve as those areas that all MI units and Soldiers must continuously train on in order to maintain a high degree of proficiency. Intelligence professionals have unique technical training and oversight requirements in order to operate as part of the intelligence enterprise. MI Soldiers must train in order to thoroughly understand unique authorities and guidelines, terms, and technical channel procedures.

INTELLIGENCE SYNCHRONIZATION

2-53. ***Intelligence synchronization*** **is the "art" of integrating information collection and intelligence analysis with operations to effectively and efficiently support decisionmaking**. This core competency ensures the intelligence warfighting function supports mission command. Intelligence synchronization balances time with collection, production, required accuracy, and specificity to meet the commander's and other requirements.

2-54. Intelligence synchronization requires an effective relationship with the commander, focused information collection, effective dissemination of predictive assessments, and adaptability to changing situations. Some critical aspects of effective intelligence synchronization include—

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

INTELLIGENCE OPERATIONS

2-55. Intelligence operations is one of the four primary means for information collection. The other three are reconnaissance, surveillance, and security operations. ***Intelligence operations*** **are the tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements.** These requirements are normally specified in the information collection plan. Intelligence operations collect information about the intent, activities, and capabilities of threats and relevant aspects of the operational environment to support commanders' decisionmaking.

2-56. MI units and Soldiers use the operations process to conduct intelligence operations. Intelligence operations are conducted using mission orders and standard command and support relationships. Successful intelligence synchronization and intelligence operations support the unit's ability to conduct focused intelligence analysis. Data and information collected during the course of intelligence operations is essential to the development of timely, relevant, accurate, predictive, and tailored intelligence products.

2-57. Intelligence operations, like reconnaissance, surveillance, and security operations, are shaping operations used by the commander for decisive action. Flexibility and adaptability to changing situations are critical for conducting effective intelligence operations.

2-58. Intelligence coordination is carried out by the intelligence section to facilitate active collaboration, laterally and vertically. It includes establishing and maintaining technical channels to direct, refine, and focus intelligence operations.

2-59. Deconfliction and coordination require a series of related activities that facilitate operations in another unit's AO. These activities facilitate successful intelligence operations and fratricide avoidance. At a minimum, the MI units coordinate for and report their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission—units should conduct thorough face-to-face coordination.

2-60. MI units must also coordinate with appropriate staff elements to establish fire support coordination measures around information collection assets, airspace control measures, and appropriate weapons control status (in reference to aerial information collection assets). Failure to conduct proper deconfliction and coordination may result in mission failure or unnecessary risk to personnel. MI units' leadership also coordinates with the supported unit's intelligence section for debriefings of returning members, convoy leaders, and others.

INTELLIGENCE ANALYSIS

2-61. Analysis is the basis for planning and staff activities. Analysis facilitates commanders' and other decisionmakers' ability to visualize the operational environment, organize their forces, and control operations in order to achieve their objectives.

2-62. Intelligence analysts use critical and creative thinking to conduct intelligence analysis and produce timely, predictive intelligence. Intelligence analysis is specific to the intelligence warfighting function. ***Intelligence analysis*** **is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production**. The purpose of intelligence analysis is to describe the current—and attempt to proactively assess—threats, terrain and weather, and civil considerations. The development of information collection requirements sets the stage for intelligence analysis, which supports the development of focused information collection requirements. Intelligence analysis is continuous, complements intelligence synchronization, and enables operations.

2-63. Some aspects that enable effective staff support and intelligence analysis include—

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

2-64. See TC 2-33.4 for more information about intelligence analysis.

FUSION CENTERS

2-65. Fusion centers mark a significant improvement to dynamic operational support by integrating mission command with focused analysis within a single centralized entity. These centers are not intelligence-led organizations. A fusion center is an ad hoc collaborative effort between several units, organizations, or agencies that provide resources, expertise, information, and intelligence to a center with the goal of supporting the rapid execution of operations by contributing members.

2-66. Fusion centers are primarily designed to focus collection and promote information sharing across multiple participants within a specific geographic area or mission type. These centers are not operations centers. Commanders at various echelons create fusion centers to manage the flow of information and intelligence; focus information collection to satisfy information requirements; and to process, exploit, analyze, and disseminate the resulting collection.

2-67. As an ad hoc effort, each fusion center is designed in a different manner. Historically, fusion centers have relied heavily on intelligence, operations, fires, and special operations personnel and systems. Fusion centers are most effective if they have participation from all of the key elements in the AO and representatives from all of the warfighting functions. When possible, fusion centers should include unified action partners. The centers require the ability to immediately leverage information collection assets to support current operations.

2-68. The intelligence portion of a fusion center typically comprises intelligence representatives from different tactical echelons, interagency partners, multinational organizations, host-nation organizations, and nongovernmental organizations operating in the AO. For example, if a division creates a fusion cell, the division will contribute intelligence professionals and may require brigade intelligence representatives. There are many other possible participants within the fusion center. Other participants could include representatives from NSA, NGA, the National Ground Intelligence Center (NGIC), the Joint Improvised Explosive Device Defeat Center, the Air Force, DEA, DOS, FBI, host-nation law enforcement agencies, civil affairs, aviation liaison officers, joint special operations task forces, and Army space support teams or elements. These representatives act as a conduit of requirements nominations and information or intelligence from their agency to the fusion center and from the fusion center back to their agency.

2-69. Fusion-center intelligence members focus on developing requirements for inclusion in information collection plans and to process, exploit, analyze, and disseminate the resulting collection. Representatives and analysts manage, share, and fuse their agency- or unit-specific information into the collective body of information for refined intelligence analysis. Conversely, intelligence representatives are the conduit back to their parent agency to communicate, monitor, and process new fusion-center information requirements. Intelligence representatives ensure intelligence collection, reporting, analytic products, and threat information are directed back to their parent agency or organization for proper dissemination.

Chapter 3
The Intelligence Process

THE OPERATIONS PROCESS AND THE INTELLIGENCE PROCESS

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

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

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

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

3-4. The Army views the intelligence process as a model that describes how the intelligence warfighting function facilitates situational understanding and supports decisionmaking. This process provides a common framework for Army professionals to guide their thoughts, discussions, plans, and assessments.

3-5. Commander's guidance drives the intelligence process. The intelligence process generates information, products, and knowledge about threats, terrain and weather, and civil considerations for the commander and staff. The intelligence process supports all of the activities of the operations process (plan, prepare, execute, and assess). The intelligence process can be conducted multiple times to support each activity of the operations process. The intelligence process, although designed similarly to the operations process, includes unique aspects and activities:

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

3-6. Intelligence support to operations requires input from the entire intelligence enterprise. This support is coordinated through the G-2/S-2 staff at each echelon by using the intelligence process. Figure 3-1, page 3-2, illustrates the intelligence process.

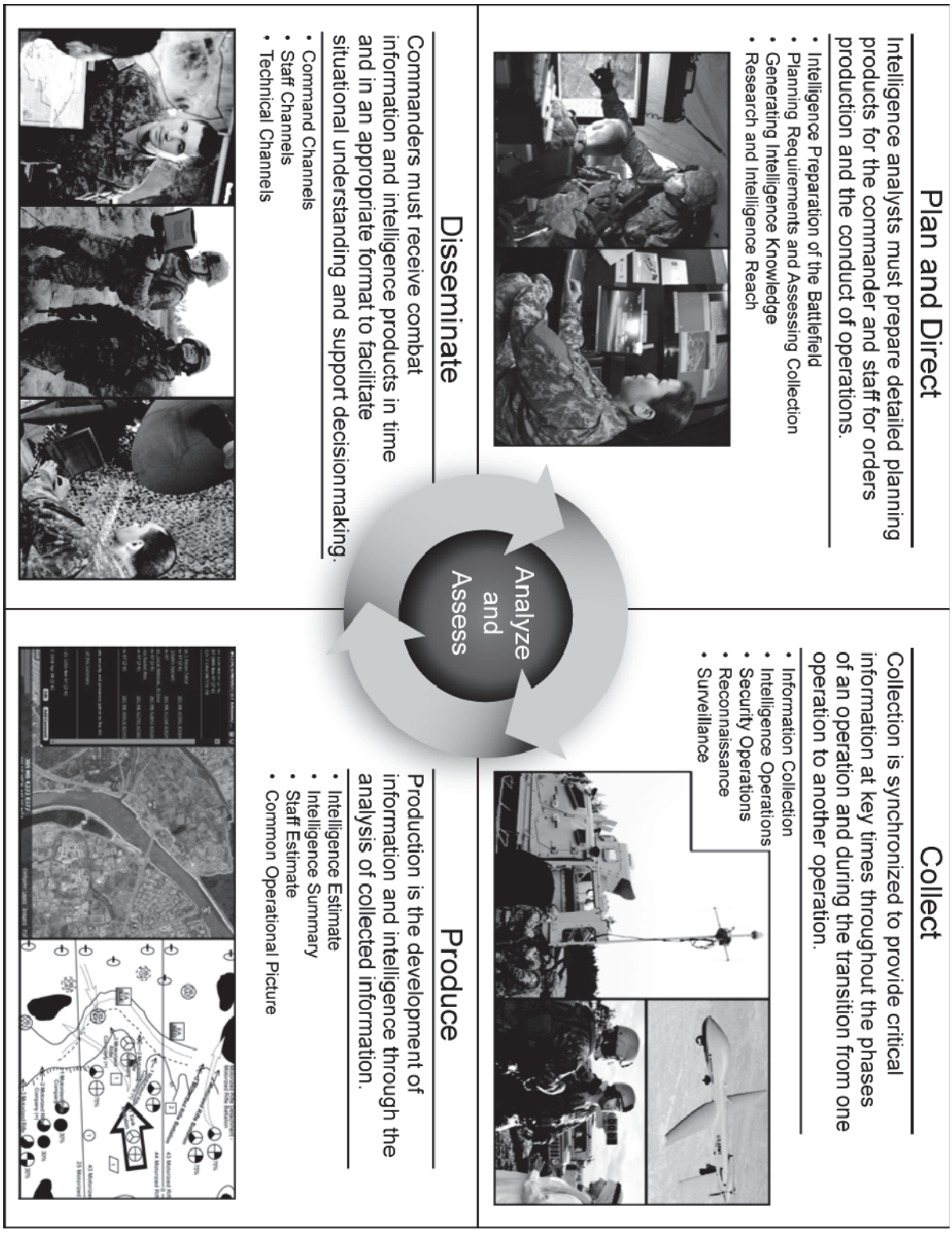

Figure 3-1. The intelligence process

3-7. The G-2/S-2 produces intelligence for the commander as part of a collaborative process. The commander drives the G-2's/S-2's intelligence production effort by establishing intelligence and information requirements with clearly defined goals and criteria. Differing unit missions and operational environments dictate numerous and varied production requirements to the G-2/S-2 and staff.

3-8. The G-2/S-2 and staff provide intelligence products that enable the commander to—

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

COMMANDER'S GUIDANCE

3-9. Commanders drive the intelligence process by both providing commander's guidance and approving CCIRs. While it is not part of the intelligence process, commander's guidance is one of the primary mechanisms used to focus the intelligence process. While issuing their guidance, commanders should limit the number of CCIRs so the staff can focus its efforts and allocate sufficient resources. Each commander dictates which intelligence products are required, when they are required, and in what format.

INTELLIGENCE PROCESS STEPS

3-10. 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

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

3-12. The initial generation of intelligence knowledge about the operational environment occurs far in advance of detailed planning and orders production. This intelligence helps focus information collection once a mission is received. Intelligence planning is also an inherent part of the Army design methodology and the military decisionmaking process (MDMP). Intelligence analysts must prepare detailed planning products for the commander and staff for orders production and the conduct of operations. Through thorough and accurate planning, the staff allows the commander to focus the unit's combat power to achieve mission success.

3-13. The plan and direct step also includes activities that identify key information requirements and develops the means for satisfying those requirements. The G-2/S-2 collaborates with the G-3/S-3 to produce a synchronized and integrated information collection plan focused on answering CCIRs and other requirements. CCIRs and other requirements drive the information collection effort. Intelligence planning and directing comprises a broad range of detailed tasks, to include—

- Conducting activities, such as research, intelligence reach, and analysis. These activities produce the initial intelligence knowledge about the operational environment.
- Generating intelligence knowledge.
- Preparing IPB products and overlays.
- Developing the initial intelligence estimate or briefings (usually as part of the mission analysis briefing).
- Establishing the intelligence architecture and testing access to the intelligence enterprise.

- Establishing effective analytic collaboration.
- Establishing liaisons.
- Establishing intelligence team cohesiveness.
- Establishing reporting procedures.
- Establishing formats and standards for products.
- Planning refinements, backbriefs, SOP reviews, and rehearsals, and coordinating with various elements and organizations.
- Establishing other troop leading procedures or coordination, as necessary, in accordance with the mission variables (METT-TC).
- Planning requirements and assessing collection.
- Assisting the G-3/S-3 with updating the information collection plan.
- Assessing continuously.
- Providing intelligence portions of the order.

Planning Considerations for the Intelligence Warfighting Function

3-14. The intelligence warfighting function is designed to systematically answer intelligence requirements. Commanders focus the effort by clearly articulating intent, stating requirements, prioritizing targets, and assessing effectiveness as operations progress. However, commanders and staffs must have realistic expectations of intelligence capabilities to drive intelligence. The following are intelligence warfighting function planning considerations:

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

3-15. Commanders must employ organic collection assets as well as plan, coordinate, and articulate requirements to leverage the intelligence enterprise. Commanders and staffs cannot expect higher echelons to automatically provide all of the information and intelligence they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from developing specific and detailed requirements. Commanders and staffs must focus requests for intelligence support by clearly articulating requirements. Intelligence activities are enabled by and subject to laws, regulations, and policies to ensure proper conduct of intelligence operations. While there are too many to list, legal authorities include USC, executive orders (EOs), National Security Council and DOD directives, Army regulations, U.S. SIGINT directives, status-of-forces agreements (SOFAs), rules of engagement (ROE), and other relevant international laws. Commanders should request assistance from their servicing judge advocate to interpret or deconflict these legal authorities when necessary.

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

- Evaluate information collection assets for suitability (availability, capability, vulnerability, and performance history) to execute information collection tasks and make appropriate recommendations on asset tasking to the G-3/S-3.
- Assess information collection against CCIRs and other requirements to determine the effectiveness of the information collection plan. They maintain awareness to identify gaps in coverage and identify the need to cue or recommend redirecting information collection assets to the G-3/S-3.
- Update the planning requirements tools as requirements are satisfied, added, modified, or deleted. They remove satisfied requirements and recommend new requirements as necessary.

Requirements

3-17. For requirements management, there are three types of requirements resulting from planning requirements and assessing collection. The following three types of validated information requirements are prioritized for purposes of assigning information collection tasks: priority intelligence requirements (PIRs), intelligence requirements, and information requirements. Figure 3-2 shows the process of developing requirements and integrating them into the information collection process. (See FM 3-55 and ATTP 2-01 for more details on requirements and indicators.)

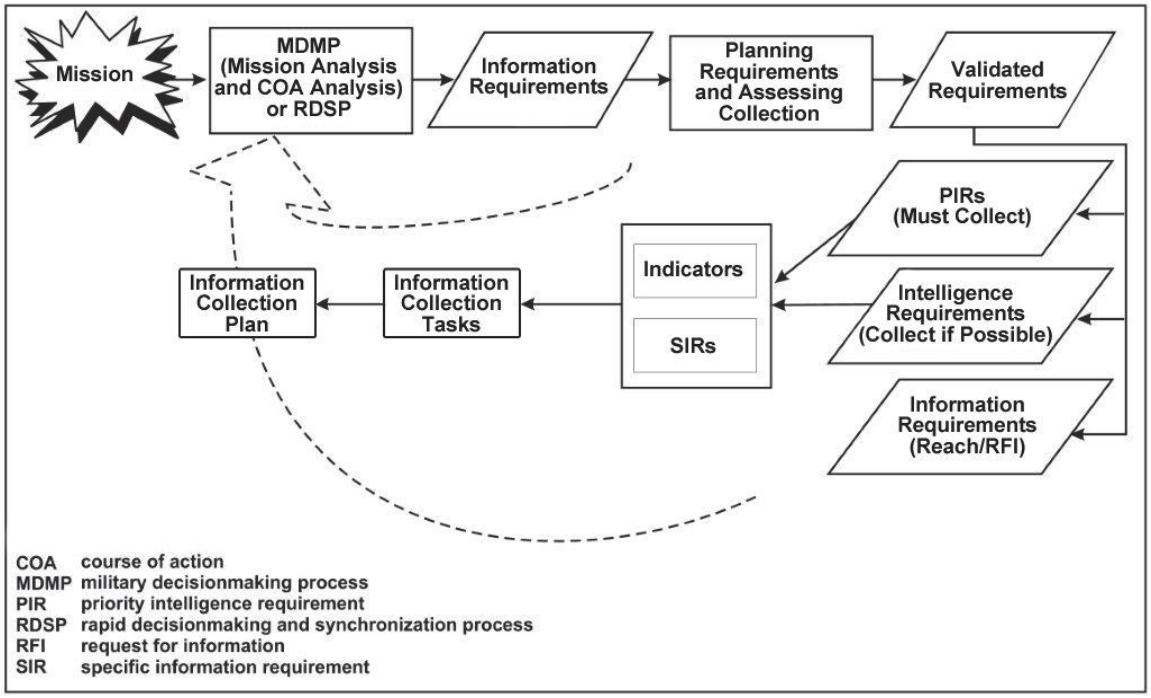

Figure 3-2. Requirements development

Intelligence Reach

3-18. Information can be acquired through the push and pull of information, databases, homepages, collaborative tools, and broadcast services. Intelligence reach also supports distributed analysis. Three important aspects of intelligence reach are searches and queries, data mining, and collaboration. (See paragraphs 2-37 and 2-38 for more discussion on intelligence reach.)

Searches and Queries

3-19. The ability to search networks and query databases is an essential skill for intelligence professionals. The basic search techniques used on the unclassified Internet also apply to the SECRET Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS). In order to conduct a search or query, intelligence professionals must plan the search, conduct the search, refine the search, and record the results. Intelligence professionals use their understanding of the supported unit's mission, specific information requirements, and available sources of information and intelligence to plan and execute their search. Because classified intelligence networks and systems are very compartmentalized, intelligence analysts should first determine which networks or databases are most likely to have the required information. Classified networks usually have specific access requirements, and intelligence professionals must coordinate for access to the classified networks.

Data Mining

3-20. Data mining is finding key pieces of intelligence that may be buried in the mass of data available. Data mining uses automated statistical analysis techniques to search for the specific data parameters that intelligence professionals predetermine will answer their information requirements. Data mining can help organize the mass of collected data.

Collaboration

3-21. Intelligence professionals work in an environment that is enhanced by collaboration. Collaboration facilitates parallel planning and enhances all aspects of the intelligence process by enriching analysis, incorporating different points of view, and broadening situational understanding. Intelligence professionals develop the ability to work effectively with others on a common task, respect the contributions of others, and contribute to consensus when warranted.

Request for Information

3-22. After having exhausted intelligence reach sources, a unit may decide to submit an RFI to higher headquarters, lateral units, or other organizations. Users enter RFIs into an RFI management system where every other system user can see and potentially answer them.

Liaison

3-23. In order to coordinate, synchronize, and integrate operations; exchange information and intelligence; move through certain areas; and ensure protection, it may be necessary to establish liaison with many different elements, organizations, and institutions of the host nation. These include the local police, town officials, foreign military forces, and political and other key figures within the AO. Operations may also necessitate coordination, synchronization, and integration with other U.S. and multinational forces. The most effective liaisons are physically co-located with the element, which enables them to build rapport and establish a close relationship. (See ATTP 5-0.1 for more information on liaison duties.)

COLLECT

3-24. Collection is synchronized to provide critical information at key times throughout the phases of an operation and during the transition from one operation to another operation. A successful information collection effort results in the timely collection and reporting of relevant and accurate information, which supports the production of intelligence. Collection consists of collecting, processing, and reporting information in response to information collection tasks. Different units and systems collect information and data about threats, terrain and weather, and civil considerations. Collected information is used in intelligence databases, intelligence production, and the G-2's/S-2's awareness—and ultimately supports the commander's situational understanding. Information collection activities transition as requirements change, the unit mission changes, the unit proceeds through the phases of an operation, and the unit prepares for future operations.

3-25. It is critical for the staff to plan for and use well-developed procedures and flexible planning to track emerging targets, adapt to changing operational requirements, and meet the requirement for combat

assessment. Once the information is collected, it is processed into a form that enables analysts to extract essential information and produce intelligence and targeting products. Processing involves converting, evaluating, analyzing, interpreting, and synthesizing raw collected data and information. Processing examples include—

- Preparing imagery for exploitation.
- Translating a document from a foreign language.
- Converting electronic data into a standardized reporting format (including database formats) that can be analyzed by a system operator.
- Correlating information that groups data into a form all analysts can use.

3-26. Collected and processed information must then be reported to the appropriate units, organizations, or agencies for analysis or action. The G-2/S-2 coordinates with the unit staff, subordinate and lateral commands, and higher echelon units to ensure specific reporting assets, personnel, equipment (especially communications), and procedures are in place. The G-2/S-2 staff evaluates the reported information for its responsiveness to information collection tasks.

3-27. The timely and accurate reporting of combat information and intelligence is critical to successful operations. The most critical information collected may be of little value if not reported in a timely manner. Unit SOPs must clearly state the transmission means of different types of reports (for example, sent by satellite communications, tactical radios, or by automated means). Generally, the transmission of reports for threat contact and actions, CCIRs, combat information, and CBRN is by voice, followed up with automated reports.

3-28. Intelligence and time-sensitive combat information that affect the current operation are disseminated immediately upon recognition. *Combat information* is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01). The routing of combat information proceeds immediately in two directions—directly to the commander and through routine reporting channels for use by intelligence analysis and production elements.

PRODUCE

3-29. Production is the development of intelligence through the analysis of collected information and existing intelligence. Analysts create intelligence products, conclusions, or projections regarding threats and relevant aspects of the operational environment to answer known or anticipated requirements in an effective format. The G-2/S-2 staff processes and analyzes information from single or multiple sources, disciplines, and complementary intelligence capabilities, and integrates the information with existing intelligence to create finished intelligence products.

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

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

3-32. Processing is often an important production activity. The G-2/S-2 staff processes information collected by the unit's assets as well as information received from higher, subordinate, and lateral echelons and other organizations. Processing includes sorting through large amounts of collected information and intelligence and converting relevant information into a form suitable for analysis, production, or immediate use.

3-33. Analysis occurs to ensure the information is relevant, to isolate significant elements of information, and to integrate the information into an intelligence product. Additionally, analysis of information and

intelligence is important to ensure the focus, prioritization, and synchronization of the unit's intelligence production effort is in accordance with the PIRs and other requirements.

DISSEMINATE

3-34. Commanders must receive combat information and intelligence products in time and in an appropriate format to facilitate situational understanding and support decisionmaking. Timely dissemination of intelligence is critical to the success of operations. Dissemination is deliberate and ensures consumers receive intelligence to support operations.

3-35. This step does not include the normal reporting and technical channels otherwise conducted by intelligence warfighting function organizations and units during the intelligence process. Each echelon with access to information may perform analysis on that information. Then each echelon ensures that resulting intelligence products are properly disseminated. Determining the product format and selecting the means to deliver it are key aspects of dissemination.

3-36. The commander and staff must establish and support a seamless intelligence architecture including an effective dissemination plan. A dissemination plan can be a separate product or integrated into existing products, such as the planning requirements tools.

3-37. Intelligence and communications systems continue to evolve in their sophistication, application of technology, and accessibility to the commander. Their increasing capabilities also create an unprecedented volume of information available to commanders at all echelons. The commander and staff must have a basic understanding of intelligence dissemination systems and their contribution to the intelligence warfighting function.

Dissemination Methods and Techniques

3-38. There are numerous methods and techniques for disseminating information and intelligence. The appropriate technique in any particular situation depends on many factors, such as capabilities and mission requirements. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, time allocated, and commander's preferences all influence the information format. Answers to PIRs require direct dissemination to the commander, subordinate commanders, and staff. Direct dissemination is conducted person-to-person, by voice communications, or electronic means. Other dissemination methods and techniques include—

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

3-39. Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods, and can be accomplished through various means—for example, push or broadcast. G-2s/S-2s must plan methods and techniques to disseminate information and intelligence when normal methods and techniques are unavailable. For example, information and intelligence can be disseminated using liaisons or regularly scheduled logistic packages as long as any classified information is properly protected and individuals are issued courier orders.

Dissemination Channels

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

- Command channels.
- Staff channels.
- Technical channels.

Command Channels

3-41. Command channels are direct chain-of-command links used by commanders or authorized staff officers for command-related activities. Command channels include command radio nets, video teleconferences, and mission command systems.

Staff Channels

3-42. Staff channels are staff-to-staff links within and between headquarters. The staff uses staff channels for control-related activities. Through these channels, the staff coordinates and transmits intelligence, controlling instructions, planning information, early warning information, and other information to support mission command. Examples of staff channels include the operations and intelligence radio net, voice-over-Internet phone (VOIP), the staff huddle, and video teleconferences, which provide information and intelligence to the rest of the intelligence architecture.

Technical Channels

3-43. Technical channels are the transmission paths between two technically similar units or offices that perform a technical function requiring special expertise. These channels are used to control the performance of technical functions. Technical channels are used only when that control is authorized by an operation order or for those authorities granted specifically in Army regulations or unit SOPs. Staffs typically use technical channels to control specific functions. These functions include fire direction and the technical reporting channels for intelligence operations, reconnaissance, and surveillance. The SIGINT tasking and reporting radio net, the common ground station (CGS), and the wide-area networks supporting single intelligence discipline collection, processing, and production are examples of technical channels.

Presentation Techniques and Procedures

3-44. Presentation is important and serves as the conclusion of the intelligence process. One of the most difficult challenges within mission command is effectively visualizing the operational environment. The G-2/S-2 staff must provide the commander with relevant information that supports the commander's visualization, facilitates situational understanding, and enables decisionmaking. The presentation method is based on the commander's guidance but often requires creative solutions to most effectively and efficiently present the intelligence and other information.

3-45. Presentations can be formal or informal. The three general methods the staff uses to present information are written narrative, verbal narrative, and graphic format. Intelligence systems contain standard report formats, maps, and mapping tools that assist the staff in presenting information. Audio and video systems, such as large format displays and teleconferencing systems, enable the staff to use a combination of these methods in multimedia presentations.

INTELLIGENCE PROCESS CONTINUING ACTIVITIES

3-46. Analyze and assess are two continuing activities that shape the intelligence process. They occur continually throughout the intelligence process.

ANALYZE

3-47. Analysis assists commanders, staffs, and intelligence leaders in framing the problem, stating the problem, and solving it. Leaders at all levels conduct analysis to assist in making many types of decisions. Analysis occurs at various stages throughout the intelligence process and is inherent throughout intelligence support to situational understanding and decisionmaking. Collectors perform initial analysis before reporting. For example, a HUMINT collector analyzes an intelligence requirement to determine the best possible collection strategy to use against a specific source.

3-48. Analysis in requirements management is critical to ensuring information requirements receive the appropriate priority for collection. The G-2/S-2 staff analyzes each requirement to determine—

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

3-49. Analysis is used in situation development to determine the significance of collected information and its significance relative to predicted threat COAs and PIRs and other requirements. Through predictive analysis, the staff attempts to identify threat activity or trends that present opportunities or risks to the friendly force. They often use indicators developed for each threat COA as the basis for their analysis and conclusions.

ASSESS

3-50. Assess is part of the overall assessment activity of the operations process. For intelligence purposes, assessment is the continuous monitoring and evaluation of the current situation, particularly significant threat activities and changes in the operational environment. Assessing the situation begins upon receipt of the mission and continues throughout the intelligence process. This assessment allows commanders, staffs, and intelligence leaders to ensure intelligence synchronization. Friendly actions, threat actions, civil considerations, and events in the area of interest interact to form a dynamic operational environment. Continuous assessment of the effects of each element on the others, especially the overall effect of threat actions on friendly operations, is essential to situational understanding.

3-51. The G-2/S-2 staff continuously produces assessments based on operations, the information collection effort, the threat situation, and the status of relevant aspects of the operational environment. These assessments are critical to—

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

3-52. The G-2/S-2 staff continuously assesses the effectiveness of the information collection effort. This type of assessment requires sound judgment and a thorough knowledge of friendly military operations, characteristics of the area of interest, and the threat situation, doctrine, patterns, and projected COAs.

Chapter 4
Army Intelligence Capabilities

EMPLOYING ARMY INTELLIGENCE CAPABILITIES

4-1. The intelligence warfighting function executes the intelligence process by employing intelligence capabilities. All-source intelligence and single-source intelligence are the building blocks by which the intelligence warfighting function facilitates situational understanding and supports decisionmaking. The intelligence warfighting function receives information from a broad variety of sources. Some of these sources are commonly referred to as single-source capabilities. Single-source capabilities are employed through intelligence operations with the other means of information collection (reconnaissance, surveillance, and security operations). The intelligence produced based on all of those sources is called all-source intelligence.

ALL-SOURCE INTELLIGENCE

4-2. Army forces conduct operations based on all-source intelligence assessments and products developed by the G-2/S-2 staff. ***All-source intelligence*** **is the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations**. All-source intelligence is used to develop the intelligence products necessary to aid situational understanding, support the development of plans and orders, and answer information requirements. Although all-source intelligence normally takes longer to produce, it is more reliable and less susceptible to deception than single-source intelligence.

4-3. In joint doctrine, all-source intelligence also refers to intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence (MASINT), SIGINT, and open-source data in the production of finished intelligence. (See JP 2-0.)

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

4-5. All-source intelligence production is continuous and occurs throughout the intelligence and operations processes. Most of the products resulting from all-source intelligence are initially developed during planning and updated as needed throughout preparation and execution based on information gained from continuous assessment.

4-6. The fundamentals of all-source intelligence analysis are intelligence analysis, all-source production, situation development, generating intelligence knowledge, support to IPB, support to targeting, and support to information collection.

4-7. Through the receipt and processing of incoming reports and messages, the G-2/S-2 staff determines the significance and reliability of incoming information, integrates incoming information with current intelligence holdings, and through analysis and evaluation determines changes in threat capabilities, vulnerabilities, and probable COAs. The G-2/S-2 staff supports the integrating processes (IPB, targeting, and risk management) and continuing activities (information collection) by providing all-source analysis of threats, terrain and weather, and civil considerations.

SINGLE-SOURCE INTELLIGENCE

4-8. Single-source intelligence includes the joint intelligence disciplines and complementary intelligence capabilities. One important aspect within single-source intelligence is processing, exploitation, and dissemination (PED) activities.

THE INTELLIGENCE DISCIPLINES

4-9. In joint operations, the intelligence enterprise is commonly organized around the intelligence disciplines. The intelligence disciplines are—

- CI.
- Geospatial intelligence (GEOINT).
- HUMINT.
- MASINT.
- Open-source intelligence (OSINT).
- SIGINT.
- Technical intelligence (TECHINT).

4-10. The intelligence disciplines are integrated to ensure a multidiscipline approach to intelligence analysis, and ultimately all-source intelligence facilitates situational understanding and supports decisionmaking. Each discipline applies unique aspects of support and guidance through technical channels. (See JP 2-0.)

Counterintelligence

4-11. CI counters or neutralizes intelligence collection efforts through collection, CI investigations, operations, analysis, production, and technical services and support. CI includes all actions taken to detect, identify, track, exploit, and neutralize multidiscipline intelligence activities of foreign intelligence and security services (FISS), international terrorist organizations, and adversaries, and is the key intelligence community contributor to protect U.S. interests and equities. (See FM 2-22.2.)

4-12. The mission of Army CI is to conduct aggressive, comprehensive, and coordinated investigations, operations, collection, analysis and production, and technical services. These functions are conducted worldwide to detect, identify, assess, counter, exploit, or neutralize the FISS, international terrorist organization, and adversary collection threat. Army CI has four primary mission areas:

- **Counterespionage.** Counterespionage refers to those CI defensive and offensive endeavors to detect, identify, assess, counter, neutralize, or exploit the foreign intelligence threat.
- **CI support to force protection.** While force protection is the responsibility of commanders at all levels, Army CI contributes to protection of the force. CI collection, analysis, investigations, and operations are designed to identify foreign intelligence and international terrorist activities that threaten military personnel, civilian employees, and units. Army CI exercises every available authority to support the force protection plans of Army and supported DOD commanders worldwide in accordance with AR 381-20 (S//NF), DOD 5240.1-R, and AR 381-10. In the performance of this function, CI will collect and report information that satisfies standing CI collection requirements.
- **CI support to research, development, and acquisition.** This support is accomplished to prevent the illegal diversion or loss of critical technology essential to the strategic advantage of the United States in future conflicts.
- **Cyber CI.** Cyber CI refers to any and all of those activities in the functional areas of investigations, operations, collection, and analysis and production that have digital media or cyberspace as a central component.

4-13. CI core functions are interrelated, mutually supporting, and can be derived from one another. No single function can defeat the FISS, international terrorist organization, and adversary intelligence collection. The CI core functions are—

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

4-14. CI organizations and force structure are designed to support Army forces through scalable team, operations management, and technical channel packages. The G-2X/S-2X structure supports decentralized CI operations. The establishment of the 2X and the CI coordinating authority throughout the Army ensures a trained and experienced cadre of CI professionals to support operations.

4-15. For more information on CI, see FM 2-22.2.

Geospatial Intelligence

4-16. *Geospatial intelligence* is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (JP 2-03). (Section 467, Title 10, USC [10 USC 467], establishes GEOINT.)

Note. GEOINT consists of any one or any combination of the following components: imagery, IMINT, and geospatial information and services.

4-17. *Imagery* is a likeness or presentation of any natural or manmade feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including: products produced by space-based national intelligence reconnaissance systems; and likenesses and presentations produced by satellites, aircraft platforms, unmanned aircraft systems, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations) (JP 2-03).

4-18. *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03).

4-19. *Geospatial information and services* is the collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a

precise location on the Earth's surface. Geospatial services include tools that enable users to access and manipulate data, and also include instruction, training, laboratory support, and guidance for the use of geospatial data (JP 2-03).

4-20. GEOINT supports the multidirectional flow and integration of geospatially referenced data from all sources to achieve shared situational understanding of the operational environment, near real-time tracking, and collaboration between forces.

4-21. GEOINT activities necessary to support operations include the capability to define GEOINT requirements, discover and obtain GEOINT, put GEOINT in a useable form, and then maintain, use, and share GEOINT. The GEOINT cell interfaces directly with the user to define user requirements. Then it interfaces with the National System for Geospatial Intelligence to obtain and provide the best quality GEOINT possible directly to the Soldier. The GEOINT cell supports operations through five tasks:

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

4-22. The use of GEOINT can be categorized into six general areas:

- General military intelligence and indications and warning (I&W).
- Safety of navigation.
- Operational awareness.
- Mission planning.
- Mission command products.
- Target intelligence.

4-23. For more information on GEOINT, see TC 2-22.7.

Human Intelligence

4-24. *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 (FM 2-0).

4-25. A HUMINT source is a person from whom foreign information is collected for the purpose of producing intelligence. HUMINT sources can include friendly, neutral, or hostile personnel. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Categories of HUMINT sources include but are not limited to detainees, enemy prisoners of war, refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and nongovernmental organizations.

4-26. A HUMINT collector is a person who is trained and authorized to collect information from individuals (HUMINT sources) for the purpose of answering requirements. HUMINT collectors are the only personnel authorized to conduct HUMINT collection operations. They are trained and certified enlisted personnel in military occupational specialty (MOS) 35M, warrant officers in 351M, commissioned officers in MOS 35F, and their federal civilian employee counterparts. However, in order to conduct interrogations trained HUMINT collectors must successfully complete one of the following courses, which are the only accepted sources of interrogation training for military personnel:

- 35M Basic HUMINT Collector course at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona.
- U.S. Marine Corps Basic Marine Air-Ground Task Force CI/HUMINT course at the Navy and Marine Corps Intelligence Center, Dam Neck, Virginia.
- Joint Interrogation Certification course at the HUMINT Training-Joint Center of Excellence, Fort Huachuca, Arizona.
- DIA I-10 course, Alexandria, Virginia.

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

4-27. HUMINT collection operations must be conducted in accordance with all applicable U.S. law and policy, which include EO 12333, DOD 5240.1-R, the law of war; relevant international law; relevant directives including DODD 2310.1E and DODD 3115.09, DOD instructions, FM 2-22.3, and military orders including fragmentary orders. Additional policies and regulations apply to the management of contractors engaging in HUMINT collection. Commanders should request assistance from their servicing judge advocate to interpret or deconflict these legal authorities when necessary. (See FM 2-22.3, appendix K.)

4-28. HUMINT operations focus on determining the capabilities, threat characteristics, vulnerabilities, and intentions of threat and potential threat forces. HUMINT operations target actual and potential threat decisionmaking architectures with the intent of helping to facilitate friendly forces' visualization.

4-29. Every HUMINT questioning session, regardless of the methodology used or the type of operation, consists of five phases. The five phases of HUMINT collection are—

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

4-30. The phases are generally sequential; however, reporting may occur at any point within the process when critical information is obtained and the approach techniques used will be reinforced as required through the questioning and termination phases.

4-31. HUMINT collection methodologies include five general categories:

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

4-32. For more information on HUMINT, see FM 2-22.3.

Measurement and Signature Intelligence

4-33. *Measurement and signature intelligence* is intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted (JP 2-0).

4-34. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, radio frequency, and seismic sensors, as well as techniques for collecting CBRN signatures and other materiel samples.

4-35. MASINT requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communications, data, and display processing technologies now provide MASINT to support operations.

4-36. MASINT provides intelligence to the commander to facilitate situational understanding and support targeting. Many sensors can defeat many of the camouflage, concealment, and deception techniques currently used to deceive information collection systems. Specifically, MASINT sensors have unique capabilities to detect missile launch; detect and track aircraft, ships, and vehicles; perform noncooperative target identification and combat assessment; and detect and track fallout from nuclear detonations. Often, these sensors provide the first indicators of hostile activities.

4-37. The MASINT systems most familiar to Soldiers are employed by ground surveillance and CBRN reconnaissance elements. These systems span the entire electromagnetic spectrum and their capabilities complement the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—

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

4-38. Within DOD, DIA provides policy and guidance for MASINT. DIA's policy and guidance do not interfere with Service component operations. Each Service has a primary command or staff activity to develop requirements and coordinate the MASINT effort. The Army G-2 staff is the functional manager for Army MASINT resources, policy, and guidance. Army weapons systems programs that require MASINT information to support system design or operations submit requests through INSCOM channels for data collection and processing.

4-39. The scientific and technical intelligence (S&TI) community also performs MASINT collection and processing primarily to support research and development programs and signature development. Every S&TI center has some involvement in MASINT collection or production that reflects that center's overall mission (for example, NGIC has responsibility for armored vehicles and artillery). Service research and development centers, such as the Communications-Electronics Command Research, Development, and Engineering Center, the Army Research Laboratory, and the Night Vision and Electronic Systems Laboratory, are also involved in developing sensor systems for collecting and processing MASINT. Elements within the Army Space and Missile Defense Command also exploit satellite-collected data for the purpose of MASINT exploitation.

4-40. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based operational collection to support the ASCCs and subordinate units.

4-41. For more information on MASINT, see JP 2-0.

Open-Source Intelligence

4-42. *Open-source intelligence* is information of potential intelligence value that is available to the general public (JP 2-0). For the Army, OSINT is the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. OSINT operations are integral to Army intelligence operations.

4-43. The Army does not have a specific MOS, additional skill identifier, or special qualification identifier for OSINT. With the exception of the Asian Studies Detachment, the Army does not have base tables of organization and equipment for OSINT units or staff elements. OSINT missions and tasks are embedded within existing missions and force structure or accomplished through task-organizing.

4-44. OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements. Two important related terms are open source and publicly available information:

- **Open source** is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.

- **Publicly available information** is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

Note. All OSINT operations conducted by intelligence professionals must comply with the legal restrictions in EO 12333, DODD 5100.20, and AR 381-10.

4-45. Open sources broadcast, publish, or otherwise distribute unclassified information for public use. The collection means (techniques) for obtaining publicly available information from these media of communications are nonintrusive.

4-46. The following characteristics address the role of publicly available information and OSINT in Army operations:

- **Provides the foundation.** The U.S. social structures, education system, news services, and entertainment industry shape worldview awareness of international events and perceptions of non-U.S. societies. This foundation can be essential to generating intelligence knowledge.
- **Answers requirements.** The availability, depth, and range of public information enable intelligence and nonintelligence organizations to satisfy many PIRs and information requirements without the use of specialized human or technical means of collection. Given the volume, scope, and quality of publicly available information, OSINT operations can often proceed directly from the *plan and direct* step to the *produce* step of the intelligence process.
- **Enhances collection.** Open-source research and information collection support other requirements and provide information (biographies, cultural information, geospatial information, technical data) that optimizes the employment and performance of sensitive human and technical means of collection.
- **Enhances production.** As part of single-source and all-source intelligence production, the use and integration of OSINT ensure commanders have the benefit of all sources of available information.

4-47. For more information on OSINT, see ATP 2-22.9.

Signals Intelligence

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

- Communications intelligence (COMINT).
- Electronic intelligence (ELINT).
- Foreign instrumentation signals intelligence (FISINT).

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

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

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

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

4-51. *Foreign instrumentation signals intelligence* is technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links (JP 2-01).

4-52. SIGINT provides intelligence on threat intentions, capabilities, composition, and dispositions. In addition, SIGINT provides targeting information for the delivery of lethal and nonlethal fires effects.

4-53. The G-2/S-2 staff needs to understand how SIGINT assets are organized not only within the Army but also throughout DOD and the intelligence enterprise. The majority of SIGINT assets from all of the Armed Services, combined with national SIGINT assets, collaborate to support commanders from tactical to strategic levels. Only by understanding the SIGINT structure that transcends traditional Service components can the G-2/S-2 staff understand how to use SIGINT effectively.

Technical Intelligence

4-54. *Technical intelligence* is intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0). The role of TECHINT is to ensure Soldiers understand the threat's full technological capabilities. With this understanding, U.S. forces can adopt appropriate countermeasures, operations, and tactics, techniques, and procedures.

4-55. A comprehensive TECHINT enterprise is vital to providing precise direction and purpose to DOD research and development and exploitation processes. This ensures quick and efficient neutralization of threat technological advantages and networks in direct support of the commander and S&TI community.

4-56. TECHINT has three goals:

- To ensure U.S. forces maintain a technological advantage against any threat.
- To provide timely, relevant, accurate, predictive, and tailored support using captured enemy materiel to provide U.S. forces intelligence, information, and training on foreign weapons systems.
- To assess the capabilities and vulnerabilities of captured materials and provide detailed assessments of foreign technological threat capabilities, limitations, and vulnerabilities.

4-57. TECHINT's two main components are the Army Foreign Materiel Program and weapons technical intelligence (WTI), which applies forensic science and other critical enablers across the following categories: communications and electronics, automation systems, weapons, munitions, medical materiel, and mobility systems. TECHINT also complies with theater chain of custody procedures.

4-58. The Army Foreign Materiel Program is managed by the Army G-2 and divided into the foreign materiel acquisition phase, foreign materiel exploitation phase, and disposition of materiel no longer needed. The formal program responds to PIRs, intelligence requirements, information requirements, and training requirements.

4-59. Soldiers assigned to conduct TECHINT activities, in concert with the S&TI community, determine capabilities of enemy materiel and provide U.S. materiel developers with data and technical specifications to improve the survivability of U.S. Soldiers and equipment.

4-60. As a function of counter-improvised explosive device operations, *weapons technical intelligence* is a category of intelligence and processes derived from the technical and forensic collection and exploitation of improvised explosive devices, associated components, improvised weapons, and other weapon systems (JP 3-15.1).

4-61. As a specific application of TECHINT, WTI combines technical assessments, forensic science, and other critical enablers with all-source intelligence for use against irregular and nontraditional threats. WTI operationalizes TECHINT and focuses on immediate exploitation of captured weapons to rapidly respond to the tactical commander's PIRs and other requirements. WTI integrates a range of collection, exploitation, and analysis capabilities to support four critical outputs:

- To enable targeting by identifying, selecting, prioritizing, and tracking individuals and matching them with groups, weapons materiel, financiers, suppliers, insurgent leaders, and other related elements.
- To technically and forensically examine events and devices or weapons to identify observables, signatures, and better understand linkages between technical design and tactical use to guide efforts of the protection warfighting function, as well as tip and cue information collection.
- To provide trend, pattern, and forensic analysis of improvised explosive devices, improvised weapons, and weapon components usage to identify the origin of materiel and components.
- To use information from captured enemy materiel collected during site exploitation activities to further detain and potentially support the prosecution of individuals for criminal activity.

4-62. Every TECHINT mission supports tactical through strategic requirements by the timely collection and processing of materiel and information, follow-on analysis and resulting production of intelligence, and dissemination to a wide range of consumers. Commanders rely on TECHINT to provide them with tactical and technological advantages to successfully synchronize and execute operations. TECHINT combines information to identify specific individuals, groups, and nation states, matching them to events, places, devices, weapons, equipment, or contraband that associates their involvement in hostile or criminal activity.

4-63. For more information on TECHINT, see TC 2-22.4.

COMPLEMENTARY INTELLIGENCE CAPABILITIES

4-64. Complementary intelligence capabilities contribute valuable information for all-source intelligence to facilitate the conduct of operations. The complementary intelligence capabilities are specific to the unit and circumstances at each echelon and can vary across the intelligence enterprise. These capabilities include but are not limited to—

- Biometrics-enabled intelligence (BEI).
- Cyber-enabled intelligence.
- Document and media exploitation (DOMEX).
- Forensic-enabled intelligence (FEI).

Biometrics-Enabled Intelligence

4-65. Joint doctrine defines *biometric* as a measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual (JP 2-0). Biometrics as a process of confirming identity is not exclusive to the intelligence warfighting function. This enabler supports multiple activities and tasks of other warfighting functions. ***Biometrics-enabled intelligence*** **is the information associated with and/or derived from biometric signatures and the associated contextual information that positively identifies a specific person and/or matches an unknown identity to a place, activity, device, component, or weapon.**

4-66. Commanders are employing biometrics with increasing intensity during operations to identify insurgents, verify local and third-country nationals accessing U.S. bases and facilities, and link people to events. Biometric systems are employed to disrupt threat forces freedom of movement within the populace and to positively identify known threat forces and personnel. These systems collect biometric data and combine them with contextual data to produce an electronic biometric dossier on the individual. Affixing an individual's identification using his or her unique physical features and linking this identity to the individual's past activities and previously used identities provide more accurate information about the individual. For example, during counterinsurgency operations, biometric collections and forensic exploitation of improvised explosive devices, cache sites, safe houses, and vehicles provide commanders additional tools to separate insurgents and criminals from the populace.

4-67. Biometric collection devices used by U.S. and multinational forces typically collect fingerprints, iris scans, and facial images. Biometrics positively identifies an encountered person and unveils terrorist or criminal activities regardless of paper documents, disguises, or aliases. This data is combined with local and national databases. The intelligence data, coupled with verifiable biometrics, enables the commander to perform more precise and effective targeting missions.

4-68. Biometric collection and the analysis of data and information occur at tactical units and at NGIC:

- **Tactical analysis.** Numerous biometric collection devices, deployed to DOD units, are classified as Secret and higher. The systems not only allow for biometric collection but also for the association of interrogation reports, link analysis, tracking reports, and other useful analytical data and information. This contextual data is combined with the electronic file transmission to create an electronic biometric dossier. Biometric dossiers can be used by analysts with access to local or regional databases.
- **NGIC analysis.** NGIC stores biometric systems that receive biometric and contextual data from authoritative databases and biometric servers located globally. NGIC uses biometric systems along with other data and analysis to create data associated with a biometric identity. NGIC makes this data available over the Internet to intelligence personnel. NGIC also manages the watchlist.

4-69. Division and above echelons develop many BEI products to support operations, including—

- **Biometric identity analysis reports (BIARs).** The BIAR is a "processed" intelligence product that associates a biometric match with an individual in the biometric database. The BIAR is produced by sorting, analyzing, and linking the biometric match with the individual's history, along with all-source intelligence. It contains the identification, background, assessment, and intelligence value of the subject. The report is produced for all latent matches, other high-threat matches, and matches from specified mission areas.
- **Watchlisting.** One of the primary duties of the intelligence analyst and staff is managing watchlist processes for the unit's collected biometric identities and linking related contextual information and intelligence for future reference or further analysis.

4-70. Intelligence-related functions that biometrics can support or enhance include—

- Intelligence analysis (including link and pattern analysis).
- Forensic analysis.
- Site exploitation.
- Base access and local security (to include screening of foreign-national and local-employee hires).
- Force protection.
- Interrogation and detention tasks.
- High-value target (HVT) confirmation (including high-value individuals and individuals killed in action).
- Population control or census (screening, enrolling, and badging tasks).
- Personnel recovery tasks.
- Disaster relief operations.
- HUMINT and CI vetting of sources.

4-71. For more information on BEI, see TC 2-22.82.

Cyber-Enabled Intelligence

4-72. The cyber domain provides another means to collect intelligence. Cyber-enabled intelligence is a complementary intelligence capability providing the ability to collect information and produce unique intelligence. All-source intelligence, the intelligence disciplines, and the other complementary intelligence capabilities are facilitated by using computers, technology, and networks. However, their use of computers, technology, and networks does not mean these are cyber operations. The guiding methods and regulations for the conduct of each intelligence discipline or complementary intelligence capability are governed under the appropriate title authority for each specific discipline or capability. Hence, the mission, authority, and oversight of an activity determine whether an activity is cyber-enabled intelligence or cyber-controlled.

4-73. Cyber-enabled intelligence is produced through the combination of intelligence analysis and the collaboration of information concerning activity in cyberspace and the electromagnetic spectrum. This intelligence supports cyber situational understanding. Unlike cyber operations, cyber-enabled intelligence is intelligence-centric based on collection within cyberspace and does not include operations and dominance within the electromagnetic spectrum. The results of cyber electromagnetic activities can provide intelligence professionals with a significant amount of information concerning both the physical and information domains.

4-74. Cyber-enabled intelligence facilitates decisionmaking at all levels through the analysis and production of relevant and tailored intelligence. Additionally, this complementary intelligence capability includes the integration of intelligence products into staff processes, such as IPB and targeting. The intelligence can range from broadly disseminated products targeted to general users to very specific and narrowly focused analysis and reports distributed via classified channels. The use of cyber-enabled intelligence facilitates an understanding of the threat's capabilities, intentions, potential actions, vulnerabilities, and impact on the environment.

Document and Media Exploitation

4-75. *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 (TC 2-91.8). Threat intent, capabilities, and limitations may be derived through the exploitation of captured materials. Captured materials are divided into captured enemy documents and captured enemy materiel.

4-76. DOMEX is an increasingly specialized, full-time mission requiring advanced automation and communications support, analytical support, and expert linguists. When conducted properly, DOMEX tasks are intended to—

- Maximize the value of intelligence gained from captured enemy documents.
- Provide the commander with timely and relevant intelligence to effectively enhance awareness of the threat's capabilities, operational structures, and intent.
- Assist in criminal prosecution or legal proceedings by maintaining chain of custody procedures and preserving the evidentiary value of captured materials.

4-77. DOMEX products become a force multiplier only when captured materials are rapidly exploited at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and accurate intelligence support. This practice not only enables rapid exploitation and evacuation of captured materials but also hastens the feedback commanders receive from the higher echelon analysis.

4-78. The traditional methodology for intelligence dissemination sends reports through an echeloned structure from national, to joint force, to corps, to division, and so on, then back up through the same rigid structure. Recent military operations have shown that this methodology seldom results in lower tactical echelons receiving timely intelligence critical to their operations. G-2/S-2 staffs need to use any available communications medium to pass vital information down to the lowest echelon and especially down to the capturing unit.

4-79. It is essential to pass critical information quickly to those who need it, specifically, tactical commanders. G-2/S-2 staffs are responsible for reporting and disseminating DOMEX-derived information in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

4-80. DOMEX personnel are usually not available below the battalion level except in MI organizations. This requires maneuver battalion G-2/S-2 staffs to prepare their subordinate units for DOMEX tasks. When intelligence and target language personnel are available, they can be task-organized as intelligence support teams and placed with companies or platoons. Alternatively, the intelligence section can train company or platoon personnel in specific handling, screening, and inventorying techniques.

4-81. When tactical assets are insufficient, members of the intelligence community can provide specialized processing and support to units, through personnel augmentation or virtual or long-distance support. DOMEX support elements provide this support worldwide. These organizations use specialized techniques and procedures to extract additional information from captured audio and video materials. Application of specialized processing techniques and procedures may require the classification of the processed information and restrict its dissemination. (For more information on DOMEX, see TC 2-91.8.)

Forensic-Enabled Intelligence

4-82. Forensics involves the application of a broad spectrum of scientific processes and techniques to establish facts. Battlefield or expeditionary forensics refers to the use of forensic techniques to provide timely and accurate information that facilitates situational understanding and supports decisionmaking. This includes collecting, identifying, and labeling portable items for future exploitation, and the collection of fingerprints, deoxyribonucleic acid (DNA), and other biometric data, which can aid in personnel recovery, from nontransportable items at a scene. Intelligence personnel can use information from forensic analysis and send it as combat information or incorporate it in the intelligence analysis effort.

4-83. FEI helps accurately identify networked and complex threats and attributes them to specific incidents and activities. The effort is often critical in supporting the targeting process. FEI can identify and determine the source of origin of captured materials. Accurate site documentation of incidents or events, material and structural analysis, and supporting data and information from the various forensic processes and techniques provide valuable data and facilitate adjusting friendly tactics and modifying equipment to enhance protection. Additionally, timely trace detection or material analysis of unknown substances can help protect the force from contaminants, toxins, and other hazards. Through toxicology, pathology and other forensic techniques, FEI supports Army medical intelligence. This intelligence includes detailed information on medical conditions of a specific area or of a threat.

PROCESSING, EXPLOITATION, AND DISSEMINATION

4-84. *Processing and exploitation* in intelligence usage, is the conversion of collected information into forms suitable to the production of intelligence (JP 2-01). *Dissemination and integration*, in intelligence usage, is the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions (JP 2-01). These two definitions are routinely combined into the acronym PED. PED is exclusive to single-source intelligence and fits within the larger intelligence process.

4-85. In joint doctrine, PED is a general concept that facilitates the allocation of assets to support intelligence operations. Under the PED concept, planners examine all collection assets and then determine if allocation of additional personnel and systems is required to support the exploitation of the collected information. Accounting for PED facilitates processing collected information into usable and relevant information for subsequent all-source production in a timely manner. Beyond doctrine, PED plays an important role within larger DOD intelligence programmatics.

4-86. There are many enablers that support PED activities. PED enablers are the specialized intelligence and communications systems, advanced technologies, and the associated personnel that conduct intelligence processing as well as single-source analysis within intelligence units. These enablers are distinct from intelligence collection systems and all-source analysis capabilities. PED activities are prioritized and focused on intelligence processing, analysis, and assessment to quickly support specific intelligence collection requirements and facilitate improved intelligence operations. PED began as a processing and analytical support structure for unique systems and capabilities like full motion video from unmanned aircraft systems. Unlike previous GEOINT collection capabilities, full motion video did not have supporting personnel and automated capability to process raw data into a usable format and conduct initial exploitation. PED enablers receive collection from many different intelligence sensors across the terrestrial, aerial, and space layers of the intelligence enterprise.

PED Activities Within Intelligence Operations

4-87. Every intelligence discipline and complementary intelligence capability is different, but each conducts PED activities to support timely and effective intelligence operations. Effective intelligence operations allow flexibility and responsiveness to changing situations and adaptive threats. In general, PED activities are part of the single-source information flow into all-source intelligence, allow for single-source intelligence to answer intelligence requirements, and are inextricably linked to the intelligence architecture. PED activities facilitate timely, relevant, usable, and tailored intelligence.

4-88. Some PED enablers are organic to the intelligence unit while other enablers are task-organized or distributed through the network. PED activities are key components of the intelligence communications networks, data/information repositories, and the organizational backbone (sometimes referred to as the foundation layer of the intelligence enterprise). These capabilities are also an important part of the Army's contribution to the intelligence enterprise.

4-89. PED enablers often enhance a unit's ability to—

- **Task:** Provide input to the tasking of intelligence collection systems and conduct dynamic retasking. PED activities also improve the flow of information and guidance through technical channels.
- **Collect:** Receive collection from systems that would otherwise be inaccessible.
- **Process:** Transform a larger volume of data and convert that data into a useable format. Augmenting the intelligence unit's organic ability to process massive amounts of data is often valuable and improves the unit's operational effectiveness.
- **Exploit:** Quickly use the processed information to refine guidance (using technical channels) and identify specific impacts on the mission. The multifunctional team is an example of a unit specifically designed to accomplish these goals to support time-sensitive requirements.
- **Disseminate:** Report collected information to other intelligence and operational elements and to the commander to support decisionmaking. This reporting facilitates all-source intelligence, targeting, and cueing other collectors.

4-90. System developers often combine PED capabilities into intelligence systems, but that is not possible in all cases. In the past, many have viewed PED enablers as systems. Trained operators, analysts, and maintainers are necessary to conduct and sustain some PED activities. PED enablers include a broad list of systems and supporting personnel across the intelligence enterprise.

4-91. The effective employment of PED activities within the intelligence architecture allows for the dynamic execution of intelligence operations. The intelligence process moves at significantly different speeds depending on the mission, situation, and other factors. To adapt to the changing pace of the intelligence process, intelligence leaders adjust the pace of intelligence operations. Successfully supporting time-sensitive requirements requires the intelligence process steps (plan and direct, collect, produce, and disseminate) and continuity activities (analyze and assess) to occur almost simultaneously. This results in a rapid or compressed intelligence process and is supported by dynamic intelligence operations. The execution of dynamic intelligence operations depends on a mature intelligence architecture, thorough planning, sufficient PED enablers, and all-source driven situational understanding.

PED Enablers Within the Intelligence Architecture

4-92. There are not enough PED enablers to support all intelligence operations, and support often depends on allocation from the joint force. Like other aspects of intelligence, commanders prioritize and resource PED enablers to intelligence units within the intelligence architecture based on thorough planning. Due to the complexity of this task, the G-2/S-2 plans the PED portion of the intelligence architecture and then advises the commander on prioritizing and resourcing PED activities. A thorough assessment of PED activities requires an understanding of the capabilities and requirements for many different types of systems and personnel from across the intelligence enterprise.

4-93. When requesting PED enablers, the gaining G-2/S-2 and intelligence unit commander are responsible for coordinating and planning for PED activities. However, the allocating echelon is also responsible for ensuring adequate planning, coordination, and use of PED enablers. Some PED enabler employment considerations for the gaining G-2/S-2 and intelligence unit commander include—

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

Chapter 5
Intelligence Staff Support

INTELLIGENCE SUPPORT TO COMMANDERS AND DECISIONMAKERS

5-1. There is an ever-growing volume of data and information from numerous sources on the operational environment that can improve the commander's visualization of the battlefield in time and space. Situational understanding enables the commander to better—

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

5-2. The commander depends on a skilled G-2/S-2 staff to answer PIRs and other requirements through the synchronization of the intelligence warfighting function with mission command. The G-2/S-2 staff does this by providing IPB products, supporting the information collection effort, supporting the targeting effort, and providing all-source intelligence analysis (including conclusions and projections of future conditions or events).

5-3. Using information from all intelligence disciplines, complementary intelligence capabilities, and available sources, the G-2/S-2 staff conducts all-source analysis and produces timely, relevant, accurate, predictive, and tailored intelligence that satisfies the commander's requirements. Thorough and disciplined all-source analysis reduces the possibility of error, bias, and misinformation through the consideration of multiple sources of information and intelligence.

INTELLIGENCE SUPPORT TO THE ARMY DESIGN METHODOLOGY

5-4. The G-2/S-2 staff plays a key role within the Army design methodology by assisting the commander and planning team in understanding the operational environment, identifying the problem, and developing an operational approach to solve the problem. The G-2/S-2 staff participates in the Army design methodology and provides relevant products. These products include the initial intelligence survey, intelligence estimates, studies, area studies, and any specialized products required by the commander. (See ADP 5-0 for further discussion on Army design methodology.)

INTELLIGENCE SUPPORT TO THE MILITARY DECISIONMAKING PROCESS

5-5. 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 operational environment 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. During the MDMP, the G-2/S-2 staff is responsible for providing well-defined, specific all-source intelligence products and tools. The staff tailors the all-source products and tools to the commander's requirements and the operation. The commander and staff require the following products throughout the planning process:

- Threat characteristics.
- Threat templates and models.
- Threat COAs.

- Event templates and matrices.
- High-value target lists (HVTLs).
- Lines of communications overlays (to include broadcast and communications).
- Weather effects matrices.
- Modified combined obstacle overlays (MCOOs) and terrain effects matrices.
- Hazards overlays (that accurately depict the affected areas).
- Civil considerations overlays (such as population, religion, network diagrams, and link and node overlays).

Note. Possible products are limited only by the G-2/S-2 staff's initiative and creativity.

MISSION ANALYSIS

5-6. A thorough mission analysis is crucial to planning. The contributions of the entire staff during mission analysis facilitate integrating activities and other staff processes. Most G-2/S-2 staff section actions during mission analysis support the commander's situational understanding. The G-2/S-2 staff generates intelligence, products, and knowledge to support mission analysis. The intelligence portion of mission analysis is an evaluation of threats, terrain and weather, and civil considerations during IPB. Additionally, it includes an analysis of the higher headquarters' plan or order to determine critical facts and assumptions; specified, implied, and essential tasks; and constraints that affect information collection activities. Intelligence section actions during mission analysis result in the development of an initial information collection plan and refinement of intelligence estimates and intelligence running estimates.

5-7. Collaboration across the intelligence warfighting function is essential. The G-2/S-2 staff provides intelligence input to other command post cells and elements needed to perform their tasks. Concurrently, G-2/S-2 staffs perform parallel and collaborative planning with higher and lower echelon G-2/S-2 staffs. Parallel and collaborative development promotes a common situational understanding among staffs at all echelons.

Analyze the Higher Headquarters' Order

5-8. Mission analysis begins with an analysis of the higher headquarters' order. The unit G-2/S-2 staff focuses its analysis on determining how the higher headquarters' commander and G-2/S-2 staff view threats and other relevant aspects of the operational environment. This knowledge helps shape the IPB effort. The higher headquarters' order also contains information collection tasks assigned to the unit and the task organization of information collection assets. This information contributes to planning requirements and assessing collection.

Perform Initial Intelligence Preparation of the Battlefield

5-9. The G-2/S-2 leads the staff through the IPB process. The other staff sections assist the G-2/S-2 staff in developing the IPB products required for planning. IPB starts immediately upon receipt of the mission, is refined throughout planning, and continues during preparation and execution based on the continuous assessment of operations. The following aspects of IPB support mission analysis. (See FM 2-01.3 for the IPB steps.)

Evaluate Military Aspects of the Terrain

5-10. Using the geospatial engineer team, the G-2/S-2 staff conducts a detailed analysis of the terrain within the area of interest, focusing on identifying natural and manmade features that may affect operations. The G-2/S-2 staff briefs the commander and staff on the effects the terrain may have on both friendly and threat forces, in terms of the military aspects of terrain—observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (OAKOC). Weather effects on operations are also briefed. The general product resulting from terrain analysis is the MCOO. (For a detailed explanation of terrain analysis and IPB products, see FM 2-01.3.)

Evaluate Weather Effects

5-11. The G-2/S-2 staff, with the support of the staff weather officer (SWO), is responsible for providing the commander with a thorough understanding of terrestrial and solar weather effects and their impact on friendly and threat systems and operations, as well as civil considerations. The G-2/S-2 staff provides this information during the planning process and incorporates significant weather effects into all of the primary intelligence products (intelligence estimates, intelligence summaries, and the intelligence portion of the COP). Weather effects are analyzed based on the military aspects of weather (visibility, wind, precipitation, cloud cover, temperature, and humidity).

5-12. The G-2/S-2 staff is responsible for requesting weather effects to operations and other relevant environmental information from the Air Force SWO. SWOs are typically assigned to support corps, divisions, aviation brigades, and special operations forces. For all other units, the G-2/S-2 is responsible for coordinating with the SWO assigned to the next higher headquarters or the appropriate local weather office. The G-2/S-2 or G-3/S-3 provides the SWO weather sensitivity thresholds on friendly and threat forces, named areas of interest (NAIs), and objective areas.

5-13. The SWO is responsible for coordinating operational weather support and weather services through the G-2/S-2. The SWO, an Air Force officer or noncommissioned officer, leads a combat weather team of two or more personnel. SWO responsibilities include—

- Coordinating weather support procedures for garrison, and before and during deployments with the supported Army command.
- Advising the Army commander on Air Force weather capabilities, limitations, and the ways in which weather support can enhance operations.
- Helping the G-2/S-2 arrange weather support for subordinate units.
- Helping the G-2/S-2 and staff produce weather displays, graphic COP overlays, and weather-effects tactical decision aids displaying weather effects on friendly and threat forces, weapons systems and sensor payloads, and information collection units and assets.
- Evaluating and disseminating weather products and data.
- Advising the Air Force on Army operational weather support requirements.
- Helping the G-2/S-2 monitor the weather support mission, identify responsibilities, and resolve weather support deficiencies.

5-14. See FM 2-01.3 for a detailed explanation of weather analysis.

Evaluate Civil Considerations

5-15. ASCOPE characteristics (area, structures, capabilities, organizations, people, and events) are used to analyze and describe civil considerations that may affect operations. Included in civil considerations analysis are the effects urban centers may have on friendly and threat forces. There is no standard product resulting from this analysis. The G-2/S-2 generally develops products that fit the information needed to describe the situation and support the commander's situational understanding. This is especially critical when conducting stability tasks. (See FM 2-01.3 and ADRP 3-07 for discussions on analyzing civil considerations.)

Develop Threat Capabilities

5-16. In order to accurately predict threat activities in time and space, the G-2/S-2 staff must first understand threat capabilities. Accurately depicting how a threat commander might employ forces requires the G-2/S-2 staff to understand how the threat is organized and equipped, the threat's capabilities, and how the threat has employed forces in the past. An understanding of threat characteristics and detailed organizational charts assist in this analysis. This information and intelligence provide potential threat signatures for collection by friendly information collection assets. Maintaining accurate threat characteristics is also essential in conducting combat assessment. This applies to regular and irregular forces and complex threats. The analyst generally has to develop threat characteristics for threats such as terrorists and insurgents.

Develop Threat Models

5-17. When feasible, the G-2/S-2 staff develops threat models for use during planning. Threat models can depict any number of conventional, irregular, or complex threat activities (for example, how the threat may execute offensive, defensive, and unconventional tactics). Threat models include a text and graphic depiction of the threat's disposition, objectives, goals, and end state. Threat models also explain the capabilities, strengths, weaknesses, and vulnerabilities of the threat. They can focus on the threat's intent for fires, information collection, inform and influence activities, cyber electromagnetic activities, and logistics. Threat models are presented in the mission analysis briefing.

Identify High-Value Target List

5-18. Every threat situation template and threat COA statement is accompanied by an HVTL that describes and prioritizes, relative to their worth, those assets that the threat commander requires to achieve threat objectives. A *high-value target* is a target the enemy commander requires for the successful completion of the mission. The loss of a high-value target would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest (JP 3-60). The G-2/S-2 staff develops the HVTL in coordination with the rest of the staff. The HVTL can include specific individuals (often referred to as high-value individuals) and organizations.

Develop an Event Template and Matrix

5-19. Developed as the basis for the decision support template and the collection overlay, the event template and matrix help identify the commander's decision points and determine information collection strategies. The event template and matrix ensure a consistent and well-reasoned portrayal of threat capabilities and activities in time and space. They are critical in tying information collection to the concept of operations. The event template and matrix are not briefed during mission analysis, but they must be ready for COA development. These products aid the commander in visualization and situational understanding.

Determine Specified, Implied, and Essential Tasks

5-20. The analyst analyzes the higher headquarters' order to identify specified tasks assigned to the unit and develop any implied tasks that must be performed to accomplish the specified tasks. The G-2/S-2 staff then provides a list of specified and implied tasks to the G-3/S-3 staff and assists in determining essential tasks for inclusion in the unit's restated mission.

Review Available Assets

5-21. The staff reviews the status of the unit's information collection assets, any additions or deletions made by the higher headquarters' order, and what higher echelon support is available for the operation. From this analysis, the G-2/S-2 staff then determines if the unit has the assets needed to accomplish all assigned collection tasks. If there are shortages, the G-2/S-2 staff identifies them and makes recommendations for additional resources.

Determine Constraints

5-22. A higher commander normally places some constraints on subordinate commanders. *Constraints* are restrictions placed on the command by a higher command. Constraints dictate an action or inaction, thus restricting the freedom of action of a subordinate commander (ATTP 5-0.1). Constraints are normally contained in the scheme of maneuver paragraph, concept of operations paragraph, or coordinating instructions paragraph in the base order. They might also be stated in the annexes to the order.

Identify Critical Facts and Assumptions

5-23. Along with the rest of the staff members, the G-2/S-2 staff is responsible for collecting two categories of information concerning assigned tasks—facts and assumptions—which are relevant to the mission and decisionmaking. In the absence of facts, the commander and staff consider assumptions from their higher headquarters and develop assumptions necessary for continued planning. An *assumption* is a

supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action (JP 5-0).

5-24. Threat COAs are a good example of necessary staff assumptions. However, the staff must be careful when making assumptions about threats and other relevant aspects of the operational environment. It is important to limit assumptions to only those suppositions necessary to continue planning because of the negative consequences of planning based on too many assumptions. The staff must maintain a clear distinction between facts and assumptions over the course of an operation. It is important to discard assumptions not supported by logic or events over an extended period of time.

5-25. In determining initial intelligence requirements, the G-2/S-2 staff examines facts and assumptions developed by the staff. Information required to confirm or refute an assumption about threats or relevant aspects of the operational environment may produce intelligence requirements. Similarly, it may be necessary to monitor the situation for any changes to facts about threats or relevant aspects of the operational environment that might affect the plan or order.

5-26. Throughout planning, commanders and staffs periodically review all facts and assumptions. New facts may alter requirements and require a review of the mission analysis. Assumptions may become facts or may become invalid. Whenever facts or assumptions change, the commander and staff assess the impact of these changes on the plan and make the necessary adjustments, including changing the CCIRs and other requirements if necessary.

Begin Risk Management

5-27. Risk management is the Army's primary process for identifying hazards and controlling risks during operations. *Risk management* is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (JP 3-0).

5-28. 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 G-2/S-2 staff participates in overall risk management and integrates risk management into requirements planning when recommending tasks for information collection assets.

Determine Initial Commander's Critical Information Requirements

5-29. Mission analysis identifies gaps in information required for further planning and decisionmaking. During mission analysis, the staff develops *information requirements*, those information elements the commander and staff require to successfully conduct operations (ADRP 6-0); that is, all elements necessary to address the mission variables (METT-TC). Some information requirements are of such importance to the commander that they are nominated to the commander to become CCIRs.

5-30. Commanders consider the nominations of the staff and then determine their CCIRs. CCIRs are situation dependent and specified by the commander for each operation. Commanders continuously review CCIRs during the planning process and adjust them as situations change. The initial CCIRs developed during mission analysis normally focus on decisions the commander needs to make to focus planning. Once the commander selects a COA, the CCIRs shift to information the commander needs in order to make decisions. Commanders designate CCIRs to let the staff and subordinates know what information they deem essential for making decisions. The fewer the CCIRs, the better the staff can focus its efforts and allocate sufficient resources for information collection. PIRs and other requirements are critical to the intelligence warfighting function.

Determine the Initial Information Collection Plan

5-31. As the staff completes the mission analysis and finalizes the initial IPB products, intelligence gaps are identified and the staff develops an initial information collection strategy on how to answer the gaps. The G-3/S-3 and the remaining staff should have a thorough understanding of unit missions, tasks, and purpose. The G-2/S-2 and staff should have developed the initial collection requirements. These collection

requirements are the basis of the initial information collection plan, requests for collection support to higher and lateral units, and RFIs to higher and lateral units and other organizations.

5-32. The G-3/S-3 section is the staff proponent for the information collection plan. It is an integrated staff product executed by the unit as assigned tasks. The information collection plan tasks and directs available information collection assets to answer CCIRs and other intelligence requirements. The G-2/S-2 staff provides planning requirements products ready for inclusion as part of the WARNORD issued after mission analysis.

Update the Operational Timeline

5-33. Using projected threat operational timelines developed during IPB and illustrated by the event template and matrix, the commander and staff compare the operational timeline established by the higher headquarters' order to determine windows of opportunity to exploit threat vulnerability or times when the unit may be at risk from threat activity.

Deliver a Mission Analysis Briefing

5-34. Time permitting, the staff briefs the commander on its mission analysis using the outline provided in ADRP 5-0. Throughout the mission analysis briefing, the commander and staff discuss the various facts and assumptions about the threat situation and civil considerations. The G-2/S-2 staff presents a summary of the intelligence running estimate, initial IPB products, and initial planning requirements and assessing collection tools and how its findings impact or are impacted by other areas. This helps the commander and staff as a whole to focus on the interrelationships among the mission variables (METT-TC) and to develop a deeper understanding of the situation. The commander issues guidance to the staff for continued planning based on situational understanding gained from the mission analysis briefing.

Derive Input from the Initial Commander's Guidance

5-35. The G-2/S-2 staff is generally concerned with the commander's guidance as it applies to all warfighting functions. However, as the staff proponent, the G-2/S-2 staff is most concerned with the intelligence warfighting function and understanding the commander's guidance for intelligence. Ideally, the commander holds informal meetings with key staff members before developing the initial guidance. These meetings include assisting the commander in developing CCIRs, the mission statement, intent for intelligence and information collection, and planning guidance.

Issue a Warning Order

5-36. Immediately after the commander gives planning guidance, the G-3/S-3 issues a WARNORD to start information collection. (See ADRP 5-0 for information on the content of this WARNORD.) At a minimum, the WARNORD that starts information collection should include—

- A threat situation paragraph.
- CCIRs.
- The priority of collection.
- Information collection tasks.
- The initial information collection plan, to include planning requirements and assessing collection tools.
- Initial IPB products.

COURSE OF ACTION DEVELOPMENT

5-37. The purpose of COA development is to update the running estimates and prepare COA options for the commander's consideration. A COA is a broad potential solution to an identified problem. The COA development step of the MDMP generates options for follow-on analysis and comparison that satisfy the commander's intent and planning guidance. The staff develops friendly COAs based on facts and assumptions identified during mission analysis. Incorporating mission analysis results into COA development ensures that each friendly COA takes advantage of the opportunities the threat situation and

operational environment offer and attempts to mitigate the most significant risks. The G-2/S-2 staff collaborates closely with the rest of the staff to analyze relative combat power and develop friendly COAs. All friendly COAs are developed based on the threat situation template, the threat event template and matrix, and civil considerations templates and matrices produced during mission analysis. At the conclusion of COA development, the G-2/S-2 staff has draft information requirements for each friendly COA as well as a draft collection overlay and synchronization tools in preparation for COA analysis.

COURSE OF ACTION ANALYSIS (WARGAMING)

5-38. Analysis of COAs is a disciplined process that includes sequential rules and steps. It relies heavily on an understanding of doctrine, tactical judgment, and experience. An effective wargame requires participants to come prepared with the full knowledge of their warfighting function. The G-2/S-2 staff has three responsibilities in the wargame—to role-play the threat commander, take the lead in role-playing civil considerations that may impact operations, and act as the information collection officer. COA analysis identifies critical points in time and space during operations where intelligence must support commanders' decisions.

5-39. As the threat commander, using the threat situation template as a start-point and the event template and matrix as a guide, the G-2/S-2 staff develops critical threat decision points in relation to friendly COAs, projects threat reactions to friendly actions, and projects threat losses. The G-2/S-2 staff captures the results of each threat action and counteraction as well as the corresponding friendly and threat strengths and vulnerabilities. By role-playing the threat commander, the G-2/S-2 staff ensures the staff fully addresses friendly responses for each threat COA. The staff also takes into account civil considerations when assessing friendly and threat actions.

5-40. For the friendly force, the G-2/S-2 staff—

- Identifies information requirements.
- Refines the situation and event templates, including NAIs that support decision points.
- Refines the event template with corresponding decision points, target areas of interest (TAIs), and HVTs.
- Participates in targeting to select high-payoff targets (HPTs) from HVTs identified during IPB.
- Recommends PIRs and other requirements that correspond to the decision points.

COURSE OF ACTION APPROVAL

5-41. Following an analysis of the COAs, the staff identifies its preferred COA and makes a recommendation to the commander. This usually occurs during a decision briefing presented by the G-3/S-3. During this briefing, the G-2/S-2 staff briefs any changes to the threat situation, terrain and weather, and civil considerations.

ORDERS PRODUCTION, DISSEMINATION, AND TRANSITION

5-42. The staff, led by the G-3/S-3, prepares the order by turning the selected COA into a clear, concise concept of operations and supporting information. The order provides all of the information subordinate units need to conduct their operations. However, this is not the first time subordinate commanders and their G-2/S-2 staffs have seen this data. Parallel and collaborative planning involves G-2/S-2 staffs at all echelons. They review each other's intelligence products as they are developed. At this point, they clarify changes and submit requests for additional information and product support. (See ATTP 5-0.1 for a further discussion of orders production, dissemination, and transition.)

INFORMATION COLLECTION

5-43. Information collection activities, a key component of ISR and the intelligence enterprise, provide commanders with detailed and timely intelligence, enabling them to gain situational understanding of the threat and relevant aspects of the operational environment. Information collected from multiple sources and analyzed becomes intelligence that provides answers to CCIRs and other requirements.

5-44. When conducting information collection, the G-2/S-2 staff considers six criteria to achieve an effective and efficient information collection plan:

- **Anticipate.** The G-2/S-2 staff identifies new or refines existing requirements and presents them to commanders for approval. They recognize when and where to recommend to the G-3/S-3 staff a change in collection. Anticipating and developing new requirements are based on solid situational understanding, a thorough review of IPB products and existing intelligence, and an understanding of the concept of operations, including branches, sequels, and the need to transition into follow-on operations.
- **Coordinate.** The G-2/S-2 staff coordinates and collaborates with all staff sections and higher headquarters and subordinate and adjacent units in order to continuously synchronize the information collection plan with operations.
- **Prioritize.** G-2s/S-2s prioritize each validated intelligence requirement—based on its importance in supporting the commander's intent and decisions. Prioritization, based on the commander's guidance and the current situation, ensures limited collection assets are directed towards the most critical requirements. Effective prioritization requires assessing the operation and changing situations.
- **Balance.** Balance is achieving maximum efficiency using an appropriate mix of information collection assets to satisfy as many competing intelligence requirements as possible. Balance involves using a combination of redundancy, mix, and cueing.
- **Reach.** Higher, lateral, subordinate, or other organizations may reliably answer the unit's requirements. The G-2/S-2 staff can use intelligence reach to answer initial information requirements without having to use organic and supporting information collection assets.
- **Control.** The object of control is influencing situations and providing guidance and direction to synchronize the force while allowing subordinate information collection units and assets freedom of action. Commanders use mission orders to assign information collection missions and issue guidance.

5-45. The G-2/S-2 staff (in collaboration with the commander and staff) receives and validates requirements, prepares the planning requirements tools, recommends collection assets and capabilities to the G-3/S-3, and maintains synchronization as operations progress. (For additional details on planning requirements and assessing collection, see ATTP 2-01.)

INTELLIGENCE SUPPORT TO TARGETING

5-46. G-2/S-2 staffs provide intelligence support to targeting for both lethal and nonlethal actions. It includes intelligence support to the planning (target development) and execution of direct and indirect fires, cyber electromagnetic activities, and the information-related capabilities executing inform and influence activities, as well as assessing their effects. The G-2/S-2 staff also ensures the information collection plan supports the targeting plan. Table 5-1 lists the most important subtasks, products, and considerations associated with intelligence support to targeting. (See FM 3-60 for more information on the targeting process; see FM 2-01.3 for more information on intelligence support to targeting.)

Table 5-1. Intelligence support to targeting

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

TYPES OF INTELLIGENCE PRODUCTS

5-47. The G-2/S-2 staff produces and maintains a broad variety of products tailored to its consumers. These products are developed and maintained in accordance with the commander's guidance. For all of these products, the primary focus of the G-2/S-2 staff's analysis is presenting predictive intelligence to support operations. The intelligence products include the—

- **Intelligence estimate.** The most detailed product developed for capturing the analysis and conclusions about threats and other relevant aspects of the operational environment.
- **Intelligence summary (INTSUM).** The current assessment of the threat situation and civil considerations. Information and intelligence used to develop the INTSUM is ultimately applied to develop and update the staff estimate.
- **Intelligence running estimate.** The intelligence running estimate details the ability of the G-2/S-2 staff to support current and future operations.
- **COP (intelligence portion of the COP).** The primary tool for supporting the commander's situational understanding. The COP provides the baseline for operations.

INTELLIGENCE ESTIMATE

5-48. An intelligence estimate is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the threat and the order of probability of their adoption. The G-2/S-2 staff develops and maintains the intelligence estimate. The primary purpose of the intelligence estimate is to—

- Determine the full set of COAs open to the threat and the probable order of their adoption.
- Disseminate information and intelligence.
- Determine requirements concerning threats and other relevant aspects of the operational environment.

5-49. The intelligence estimate is a logical and orderly examination of intelligence factors affecting the accomplishment of a mission (threats, terrain and weather, and civil considerations). It provides commanders with an analysis of the area of interest and threat strengths and capabilities that can influence their mission. It is used as a basis for planning and disseminating intelligence.

5-50. An intelligence estimate may be prepared at any level. It may be formal or informal and detailed or summarized. It is normally written at division and higher levels and briefed down to the battalion level. The following is an example of the basic information and intelligence that could be included in an intelligence estimate:

- **Mission.**
- **Analysis of the AO.** This analysis of the terrain is based on—
  - The military aspects of terrain (OAKOC).
  - Other significant characteristics.
  - The effects of the terrain on friendly and threat operations and civil considerations.
  - The effects of weather on friendly and threat operations and civil considerations:
    - Operational climatology data and information, light data, and predictive weather effects based on specific weather sensitivity thresholds.
    - The current weather conditions based on the military aspects of weather (visibility, wind, precipitation, cloud cover, temperature, and humidity).
    - Projected weather forecasts with significant seasonal trends for that specific geographic location.
  - An analysis of the civil considerations and projected effects of civil considerations on friendly and threat operations, and vice versa.
- **Current threat situation.** This is based on the threat characteristics (see FM 2-01.3) and includes estimates of the strength of threat forces, recent significant threat activities and trends, and threat peculiarities and weaknesses.
- **Threat capabilities.** These are the broad COAs and supporting operations that threats can take to achieve their goals and objectives. The G-2/S-2 staff considers each threat's ability to conduct each operation based on the mission variables (METT-TC) related to the current situation.
- **Threat characteristics.** These provide a framework for the consistent evaluation of any force. The G-2/S-2 staff considers composition, disposition, strengths, weaknesses, combat effectiveness, doctrine and tactics, command and support relationships, electronic technical data, capabilities and limitations, current operations, and historical data when analyzing threat characteristics.
- **Summary of the most significant points.** This includes—
  - The most significant terrain and weather and civil considerations effects on operations.
  - Potential impacts of operations on terrain and civil considerations.
  - At a minimum, the most likely and most dangerous threat COAs.
  - The most significant threat strengths and vulnerabilities.

5-51. The intelligence estimate also includes four tabs:

- **Tab A (Terrain).** Terrain is developed primarily by the engineer coordinator.
- **Tab B (Weather).** Weather is developed primarily by the SWO.
- **Tab C (Civil Considerations).** Civil considerations products are developed primarily by the G-2/S-2, in coordination with the rest of the staff.
- **Tab D (IPB).** IPB products are developed primarily by the G-2/S-2, in coordination with the rest of the staff.

INTELLIGENCE SUMMARY

5-52. INTSUMs provide the context for commander's situational understanding. The INTSUM reflects the G-2's/S-2's interpretation and conclusions regarding threats, terrain and weather, and civil considerations over a designated period of time. This period will vary with the desires of the commander and the requirements of the situation. The INTSUM provides a summary of the threat situation, threat capabilities, the characteristics of terrain and weather and civil considerations, and COAs. The INTSUM can be presented in written, graphic, or oral format, as directed by the commander.

5-53. The INTSUM assists in assessing the current situation and updating other intelligence reports. It is disseminated to higher, lower, and adjacent units. The INTSUM has no prescribed format. The following is an example of the basic information and intelligence that should be included in an INTSUM:

- **Date-time group (DTG)** of the INTSUM and the period of time the INTSUM covers.
- **Weather and weather effects** that include current and forecast meteorological parameters and analysis based on the military aspects of weather and weather sensitivity thresholds.
- **Significant threat activities** over the reporting period and a near-term analysis of threat intent and activity.
- **Significant impacts of civil considerations** on operations and vice versa.
- **Subunit assessments of significant threat activities and civil considerations** in the AO over the reporting period and a near-term analysis of threat intent and activity.
- **Notable trends in threat activity** over a designated period of time (such as the previous 14 days). This may be presented as an all-source analysis product or focused on specific threat activities of interest to the commander—or both. This portion of the INTSUM should highlight new or emerging threats and the level of impact that each threat may present to the unit's operations.
- **Combat damage assessment roll-up** includes known or estimated threat unit strengths, significant threat systems degraded or destroyed, and all known captured, wounded, or killed threat personnel during the reporting period.
- **Written threat situation or situation template** (as of a specific DTG).
- **Assessments** include a near-term and long-term assessment of threat activities with as much detail as possible based on available information and current intelligence analysis. INTSUMs are predictive in nature. When specific intelligence or information is not available, INTSUMs must contain the G-2/S-2's best assessment of probabilities of threat actions based on experience and professional military judgment.
- **HVTLs** (in coordination with the targeting officer) may include high-value individuals, depending on the unit mission.
- **Current PIRs and projected PIRs** by phase.
- **Planning requirements tools and products**.
- **Special assessments** are developed for any unique circumstance that requires additional analysis.

INTELLIGENCE RUNNING ESTIMATE

5-54. Effective plans and successful execution hinge on accurate and current running estimates. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if the planned future operations are supportable (ADP 5-0). Failure to maintain accurate running estimates may lead to errors or omissions that result in flawed plans or bad decisions during execution.

5-55. Running estimates are principal knowledge management tools used by the commander and staff throughout the operations process. In their running estimates, the commander and each staff section continuously consider the effect of new information and update the following:

- Facts.
- Assumptions.
- Friendly force status.
- Threat activities and capabilities.
- Civil considerations.
- Recommendations and conclusions.

5-56. Each staff section builds and maintains running estimates. The running estimate helps the staff to track and record pertinent information as well as provides recommendations (especially for anticipated decisions) to commanders. Running estimates represent the analysis and expert opinion of each staff section by functional area. Staffs maintain running estimates throughout the operations process to assist in exercising mission

command. The basic outline for the running estimate comprises situation and considerations, mission, COAs, analysis, comparison, and recommendations and conclusions. (See ATTP 5-0.1 for more information on running estimates and the running estimate format.)

5-57. Unlike most other intelligence products, the intelligence running estimate combines both an analysis of friendly force intelligence activities and the ability to support current and/or future operations with intelligence analysis of threats, terrain and weather, and civil considerations. Combining this analysis facilitates projections regarding the—

- Effects of key terrain and weather on operations.
- Impact of civil considerations on operations.
- Impact of friendly operations and threat activities on civil considerations.
- Significant cultural factors to consider during planning.
- Threat intent, characteristics, and capabilities.
- Threat COAs.
- Significant conclusions drawn from a thorough and complete analysis.

COMMON OPERATIONAL PICTURE

5-58. A *common operational picture* is a single 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 (ADRP 6-0). The COP is the primary tool for supporting the commander's situational understanding. All staff sections provide input from their area of expertise to the COP.

5-59. The portion of the COP that depicts the threat situation and civil considerations is currently limited to displaying the locations and dispositions of threat forces in a relatively static manner, sometimes referred to as "snapshots in time." The threat situation portion of the COP requires analysis to provide the required level of detail.

5-60. With the complexity of the operational environment, the G-2/S-2 staff must be prepared to—

- Build 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 mission and operational variables are displayed.
- Effectively display the multiple types and layers of information the commander requires.

Chapter 6
Force Projection Operations

FORCE PROJECTION

6-1. Force projection is the military component of power projection. It is 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.

6-2. Unstable conditions worldwide often preclude a significant period of time to produce intelligence to meet contingency operation requirements. Therefore, MI units and staffs prepare for potential contingencies by building their intelligence readiness, including their skills and systems expertise, on a daily basis. When a unit has an indication that it may be deployed or is assigned a contingency mission, it can begin to generate intelligence knowledge on the projected area of interest.

6-3. 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 staff must exercise judgment when providing information to subordinate G-2/S-2 staffs to avoid overwhelming them.

6-4. Key planning factors for intelligence in force projection include—

- Staying out front in intelligence planning:
  - Begin to generate intelligence knowledge as soon as possible.
  - Develop a steady effort.
  - Prioritize intelligence requirements for development of the initial PIR.
  - Identify intelligence training requirements (to include augmentees).
- Understanding how to get intelligence support:
  - Identify asset, sensor, and PED-enabler requirements.
  - Identify personnel augmentation requirements.
  - Leverage the intelligence enterprise.
  - Integrate into the intelligence enterprise.

6-5. 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 operational environment. Intelligence leaders should—

- Review available databases on assigned contingency areas, begin collaboration and generating intelligence knowledge, and develop initial IPB products concerning these areas of interest.
- Develop the intelligence survey.
- 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 will use when deployed.
- Plan, train, and practice surging intelligence analysis on likely or developing contingencies.

- Prepare and practice coordination with other elements and organizations (for example, intelligence units and analytical elements, the G-7, SWO, civil affairs, military information support operations, the space support element, and special operations forces units).
- Include the following as a part of daily (sustainment) operations:
  - A linguist plan with proficiency requirements.
  - Training (individual and collective), to include augmentees.
- Establish formal or informal intelligence links, relationships, and networks to meet developing contingencies.
- Conduct analysis of threats, terrain and weather, and civil considerations requirements or forward RFIs in accordance with unit SOPs.
- Determine the need for additional civil considerations and sociocultural research and analysis to generate intelligence knowledge.
- Establish statements of intelligence interests and develop production and I&W requirements.

6-6. Intelligence leaders support peacetime contingency planning with intelligence knowledge and IPB 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 G-2/S-2 staff identifies requirements to include—

- Collection assets providing support throughout the area of interest.
- 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. Composition of initial and follow-on deploying assets is influenced by the mission variables (METT-TC), availability of communications, and availability of lift.
- Communications architectures supporting both G-2/S-2 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.
- Time-phased force and deployment data (TPFDD) requirements. When necessary, the staff should recommend changes to priority of movement, unit, or capability to enable information collection.

6-7. Intelligence leaders continually monitor and update applicable plans and orders to reflect the evolving situation, especially during crises. National intelligence activities monitor regional threats worldwide and can answer some intelligence requirements supporting the development of plans and orders.

FORCE PROJECTION PROCESSES

6-8. Force projection encompasses five processes that occur in a continuous, overlapping, and repeating sequence throughout an operation. The five processes, as they pertain to intelligence, include—

- Mobilization.
- Deployment.
- Employment.
- Sustaining intelligence capabilities.
- Redeployment.

MOBILIZATION

6-9. Mobilization is the process by which the Armed Forces or part of them are brought to a state of readiness for war or other national emergency. It assembles and organizes resources to support national objectives. Mobilization includes activating all or part of the Reserve Component, and assembling and organizing personnel, supplies, and materiel. (See ADRP 4-0.)

6-10. The G-2/S-2 staff updates estimates, databases, IPB products, and other intelligence products needed to support command decisions on force composition and deployment priorities and sequence. Units reassess their collection requirements immediately after alert notification. The G-2/S-2 staff begins verifying planning assumptions within the operation plan. The G-2/S-2 staff, with CI personnel support, provides force protection support and recommends antiterrorism measures.

6-11. During mobilization, intelligence leaders—

- Monitor intelligence reporting on threat activity, civil considerations, and I&W 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 operation plan.
- Support augmentation units and personnel by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify information collection force requirements for the different types of operations and contingency plans.
- Identify individual military, civilian, and contractor augmentation requirements.

6-12. During mobilization, intelligence leaders, in conjunction with the rest of the staff, ensure 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.

6-13. 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. The Distributed Common Ground-Army (DCGS-A) provides the BCT S-2 access to theater and national databases with the ability to collaborate with knowledge centers. Intelligence readiness training helps to ensure intelligence professionals and assets are able to 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.

6-14. Throughout mobilization, unit intelligence activities provide deploying forces with the most recent intelligence on the contingency area. The G-2/S-2 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 SOFAs, ROE, 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 information collection force deployment priorities 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 information collection assets, processing systems, and databases.
- Execute an intelligence survey.

- 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 intelligence capability, as well as links to joint, Service, multinational, and host-nation databases and repositories.

DEPLOYMENT

6-15. Deployment is the movement of forces and materiel from their point of origin to an operational area. During deployment, intelligence organizations at the home station or deployed with the early-entry force take advantage of the communications architecture and the intelligence enterprise to provide graphic and textual intelligence updates to the forces en route. En route updates help reduce information gaps and allow commanders to adjust plans in response to changes in the situation before arriving at the operational area. In a mature theater, intelligence handoff is conducted between arriving units and those previously deployed. The three primary areas of intelligence handoff are operations, targets and targeting, and technical channel requirements.

6-16. Intelligence units extend established networks to connect G-2/S-2 staffs and collection assets at various stages of the deployment flow. Where necessary, units establish new communications paths to meet mission requirements. If deployed, joint force and corps analysis and control elements play a critical role in making communications paths, networks, and intelligence databases available to deploying forces.

6-17. The Army relies on space-based capabilities and systems, such as global positioning satellites, communications satellites, weather satellites, 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 professionals. Space-enabled capabilities are key to supporting intelligence during deployment and employment by—

- Monitoring terrestrial areas of interest to help reveal the threat's location and disposition.
- Providing communications links between deploying forces and the United States and its territories.
- Permitting MI collection assets to determine their position accurately through the Global Positioning System (GPS).
- 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.

6-18. Situation development dominates intelligence activities during early-entry operations. The G-2/S-2 staff attempts to identify all threats to arriving forces and assists the commander in developing force protection measures. During entry operations, echelons above corps organizations provide intelligence. This support includes providing access to the intelligence enterprise and deploying scalable intelligence elements. The entire effort focuses on providing tailored support to deploying and deployed echelons in response to their PIRs and other requirements.

6-19. Processing and collection capabilities are enhanced, as collection assets buildup in the AO, with emphasis on the buildup of the in-theater capability required to conduct sustained information collection activities. As the buildup continues, the G-2/S-2 staff strives to reduce total dependence on intelligence reach and overwatch. As assigned collection assets arrive into the AO, the G-2/S-2 staff begins to rely on them for intelligence although higher echelon organizations continue to provide support.

6-20. 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. Liaison personnel, basic communications, and an intelligence network should be in place before the scheduled arrival of parent commands. Information collection units increase operations.

6-21. 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.

6-22. During entry operations the G-2/S-2 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

6-23. Intelligence and information collection support operations by meeting 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.

SUSTAINING INTELLIGENCE CAPABILITIES

6-24. Sustainment involves providing and maintaining the appropriate numbers and skill levels of intelligence professionals and materiel required for the duration of operations. Sustainment may be provided from locations within and outside the United States and its territories. For intelligence, sustainment may be focused on force rotation, ensuring intelligence professionals or units entering the AO have current intelligence and a detailed knowledge of ongoing intelligence operations. This includes—

- Providing data-file updates.
- Ensuring a coordinated intelligence handoff of ongoing intelligence operations such as military source operations.
- Ensuring units have the right MI assets to include personnel (including linguists), communications systems, information collection systems, and appropriate maintenance support.

REDEPLOYMENT

6-25. Redeployment is the process by which units and materiel reposture themselves in the same operational area, transfer forces and materiel to support another joint force commander's operational requirements, or return personnel and materiel to the home or demobilization station upon completion of the mission. As with deployment, there is a requirement to conduct intelligence handoff from the redeploying to the deploying unit. A well-prepared intelligence handoff ensures a smooth and seamless transition between units. (See FM 2-0.)

6-26. As combat power and resources decrease in the operational area, protection and I&W 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 I&W data.
- Continues to conduct intelligence support to protection.
- Requests information collection support (combatant command and national systems) and intelligence to support redeployment.

6-27. After redeployment, MI personnel and units recover and return to predeployment activities. Information collection units resume contingency-oriented peacetime intelligence operations. The G-2/S-2 staff—

- Monitors intelligence reporting on threat activity and civil considerations for contingencies.
- Updates or consolidates databases.
- Maintains intelligence readiness.
- Provides input into the force design update process to refine modified tables of organization and equipment and to evaluate the need for individual mobilization augmentee personnel.
- Prepares after-action reports and lessons learned.
- Submits organizational needs requests.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ADRP 2-0 is the proponent are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	human intelligence and counterintelligence staff element
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AO	area of operations
AR	Army regulation
ASCC	Army Service component command
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
ATTP	Army tactics, techniques, and procedures
AUTL	Army Universal Task List
BCT	brigade combat team
BEI	biometrics-enabled intelligence
BIAR	biometric identity analysis report
C	Confidential
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
CGS	common ground station
CI	counterintelligence
CIA	Central Intelligence Agency
COA	course of action
COMINT	communications intelligence
COP	common operational picture
CSS	Central Security Service
DEA	Drug Enforcement Administration
DCGS-A	Distributed Common Ground-Army
DHE-M	Defense HUMINT Enterprise-manual
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNA	deoxyribonucleic acid
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense directive

DODI	Department of Defense instruction
DOE	Department of Energy
DOMEX	document and media exploitation
DOS	Department of State
DSCA	defense support of civil authorities
DTG	date-time group
ELINT	electronic intelligence
EO	executive order
ES2	every Soldier is a sensor
FBI	Federal Bureau of Investigation
FEI	forensic-enabled intelligence
FISINT	foreign instrumentation signals intelligence
FISS	foreign intelligence and security services
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
G-7	assistant chief of staff, information management
GEOINT	geospatial intelligence
GPS	Global Positioning System
HPT	high-payoff target
HUMINT	human intelligence
HVT	high-value target
HVTL	high-value target list
I&W	indications and warning
IAA	incident awareness and assessment
INSCOM	U.S. Army Intelligence and Security Command
INTSUM	intelligence summary
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
JP	joint publication
JWICS	Joint Worldwide Intelligence Communications System
MASINT	measurement and signature intelligence
MCOO	modified combined obstacle overlay
MDMP	military decisionmaking process
METT-TC	mission, enemy, terrain and weather, troops and support availble, time available, civil considerations (mission variables)
MI	military intelligence
MOS	military occupational specialty
NAI	named area of interest
NF (NOFORN)	Not Releasable to Foreign Nationals

NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NRO	National Reconnaissance Office
NSA	National Security Agency
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain)
OSINT	open-source intelligence
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, time (operational variables)
RFI	request for information
ROE	rules of engagement
S	Secret
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
S&TI	scientific and technical intelligence
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
SOFA	status-of-forces agreement
SOP	standard operating procedure
SWO	staff weather officer
TAI	target area of interest
TC	training circular
TECHINT	technical intelligence
TPFDD	time-phased force and deployment data
TRADOC	U.S. Army Training and Doctrine Command
TREAS	Department of the Treasury
U.S.	United States
USC	United States Code
USCG	U.S. Coast Guard
VOIP	voice-over-Internet phone
WARNORD	warning order
WTI	weapons technical intelligence

SECTION II – TERMS

***all-source intelligence**

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

***biometrics-enabled intelligence**

The information associated with and/or derived from biometric signatures and the associated contextual information that positively identifies a specific person and/or matches an unknown identity to a place, activity, device, component, or weapon.

commander's critical information requirement

An information requirement identified by the commander as being critical to facilitating timely decisionmaking. (JP 3-0)

counterintelligence insider threat

Counterintelligence insider threat. A person, known or suspected, who uses their authorized access to Department of Defense facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise Department of Defense information, or commit espionage on behalf of an foreign intelligence entity. (DODI 5240.26)

***fusion**

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

information collection

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

intelligence

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity that results in the product and to the organizations engaged in such activity. (JP 2-0)

***intelligence analysis**

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

intelligence community

All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. (JP 1-02)

***intelligence operations**

(Army) The tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements.

***intelligence reach**

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

intelligence, surveillance, and reconnaissance

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

***intelligence synchronization**

The "art" of integrating information collection and intelligence analysis with operations to effectively and efficiently support decisionmaking.

intelligence warfighting function

The related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations. (ADRP 3-0)

priority intelligence requirement

An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or other aspects of the operational environment. (JP 2-01)

This page intentionally left blank.

References

REQUIRED PUBLICATIONS

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

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

JP 2-0. *Joint Intelligence*. 22 June 2007.

ARMY PUBLICATIONS

ADP 2-0. *Intelligence*. 31 August 2012.

ADP 3-0. *Unified Land Operations*. 10 October 2011.

ADP 5-0. *The Operations Process*. 17 May 2012.

ADP 6-0. *Mission Command*. 17 May 2012.

ADRP 1-02. *Operational Terms and Military Symbols*. 31 August 2012.

ADRP 3-0. *Unified Land Operations*. 16 May 2012.

ADRP 5-0. *The Operations Process*. 17 May 2012.

ADRP 6-0. *Mission Command*. 17 May 2012.

FM 2-0. *Intelligence*. 23 March 2010.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

DHE-M 3301.001. (S) *Defense Intelligence Agency (DIA) Human Intelligence (HUMINT) Manual, Vol I: Collection Requirements, Reporting, and Evaluation Procedures* (U). 30 January 2010.

DHE-M 3301.002. (S) *Defense Intelligence Agency (DIA) Human Intelligence (HUMINT) Manual, Vol II: Collection Operations* (U). 23 November 2010.

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

DODD 2310.1E. *The Department of Defense Detainee Program*. 5 September 2006.

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

DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 9 October 2008.

DODD 5100.20. *National Security Agency/Central Security Service (NSA/CSS)*. 26 January 2010.

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

JP 1. *Doctrine for the Armed Forces of the United States*. 2 May 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 5 January 2012.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 16 June 2009.

JP 2-03. *Geospatial Intelligence Support to Joint Operations*. 22 March 2007.

JP 3-0. *Joint Operations*. 11 August 2011.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.
JP 3-15.1. *Counter-Improvised Explosive Device Operations*. 9 January 2012.
JP 3-28. *Civil Support*. 14 September 2007.
JP 3-60. *Joint Targeting*. 13 April 2007.
JP 5-0. *Joint Operation Planning*. 11 August 2011.

ARMY PUBLICATIONS

ADP 3-07. *Stability*. 31 August 2012.
ADP 3-28. *Defense Support of Civil Authorities*. 26 July 2012.
ADRP 3-07. *Stability*. 31 August 2012.
ADRP 4-0. *Sustainment*. 31 July 2012.
AR 380-28. (C) *Department of the Army Special Security System* (U). 16 September 1991.
AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.
AR 381-20. (S//NF) *The Army Counterintelligence Program* (U). 26 May 2010.
ATP 2-22.9. *Open-Source Intelligence*. 10 July 2012.
ATTP 2-01. *Planning Requirements and Assessing Collection*. 23 April 2012.
ATTP 5-0.1. *Commander and Staff Officer Guide*. 14 September 2011.
FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009.
FM 2-22.2. *Counterintelligence*. 21 October 2009.
FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.
FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*. 10 October 2007.
FM 3-24. *Counterinsurgency*. 15 December 2006.
FM 3-55. *Information Collection*. 23 April 2012.
FM 3-60. *The Targeting Process*. 26 November 2010.
FM 7-15. *The Army Universal Task List*. 27 February 2009.
TC 2-22.4. *Technical Intelligence*. 19 November 2009.
TC 2-22.7. *Geospatial Intelligence Handbook*. 18 February 2011.
TC 2-22.82. *Biometrics-Enabled Intelligence*. 21 March 2011.
TC 2-33.4. *Intelligence Analysis*. 1 July 2009.
TC 2-91.7. *Intelligence Handbook for Civil Support Operations*. 26 January 2011.
TC 2-91.8. *Document and Media Exploitation*. 8 June 2010.

OTHER PUBLICATIONS

Elder, Linda and Richard Paul. *The Miniature Guide to Critical Thinking: Concepts and Tools.* 2008.
EO 12333. *United States Intelligence Activities.* 4 December 1981.
Title 10, USC. *Armed Forces*.

WEB SITES

The Foundation for Critical Thinking. "*The Thinker's Guide to Analytic Thinking*." www.criticalthinking.org, accessed May 2012.

REFERENCED FORMS

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

Index

Entries are by paragraph number.

A

all-source intelligence, 4-2 through 4-7. *See also* Army intelligence capabilities.

analysis, 3-47 through 3-49. *See also* intelligence process, continuing activities.

Army capabilities, 1-19
- combined arms, 1-20
- force tailoring, 1-21
- task-organizing, 1-22

Army intelligence capabilities, 4-1

Army design methodology, 3-12, 5-4

assess
- assessment, 3-50 through 3-52. *See also* intelligence process, continuing activities.
- predictive assessment, 2-4, 2-5, 2-54

assumptions, 5-23 through 5-26, 5-55

B

BEI, 4-65 through 4-71. *See also* complementary intelligence capabilities.
- defined, 4-65
- products, 4-69

biometric identity analysis report (BIAR). *See* BEI, products.

biometrics-enabled intelligence. *See* BEI.

brigade and below intelligence capabilities, 1-32, 1-38

C

CBRN. *See* reconnaissance.

CCIR,1-28, 5-36. *See also* information collection; information collection plan; requirements.

chemical, biological, radiological, and nuclear. *See* CBRN.

civil considerations, 5-15, 6-5. *See also* intelligence warfighting function; situational understanding.
- in the intelligence running estimate, 5-55, 5-57
- in the intelligence summary, 5-52
- intelligence estimate tab, 5-51

COA, 5-52. *See also* threat; MDMP.

collaboration, 2-30, 3-21, 6-5. *See also* intelligence analysis, defined; intelligence reach, aspects of.

collection, 3-24 through 3-28. *See also* information collection, tasks; intelligence process, steps.
- biometric collection, 4-66 through 4-68
- human intelligence collection, 4-31
- measurement and signature intelligence collection, 4-34
- PED enablers enhance, 4-89

combat information, 3-27, 3-28, 3-34

command and support relationships, 1-29. *See also* Army capabilities.

command channels, 3-41. *See also* dissemination, channels.

commanders and decisionmakers
- support to, 2-1, 5-1 through 5-3. *See also* intelligence, aspects of.

commander's critical information requirement. *See* CCIR.

commander's guidance, 3-9
- development of intelligence products, 5-47
- input from, 5-35

common operational picture. *See* COP.

communications intelligence. *See* signals intelligence.

complementary intelligence capabilities, 4-64. *See also* single-source intelligence.

constraints, 5-22

COP, 5-58 through 5-60. *See also* intelligence products, types of.
- updating, 2-45. *See* also intelligence enterprise, leveraging.

counterintelligence, 4-11 through 4-15. *See also* intelligence disciplines.

course of action. *See* COA.

critical thinking. *See* intelligence analysis, defined.

culture, 5-57. *See also* sociocultural (pertaining to).

cyber-enabled intelligence, 4-72 through 4-74. *See also* complementary intelligence capabilities.

D

data mining, 3-20. *See also* intelligence reach, aspects of.

decisive action. *See also* intelligence warfighting function.
- support to, 1-19
- tasks, 1-8

defense support of civil authorities. *See* DSCA.

defensive tasks, 1-12 through 1-14. *See also* decisive action, tasks.

Deparment of Defense. *See* DOD.

dissemination, 3-34 through 3-37. *See also* intelligence process, steps.
- channels, 3-40
- methods and techniques, 3-38, 3-39
- PED enablers enhance, 4-89
- presentation techniques and procedures, 3-44, 3-45

Entries are by paragraph number.

division and above intelligence organizations, 1-32 through 1-37

document and media exploitation, 4-75 through 4-81. *See also* complementary intelligence capabilities.

DOD
- agencies. *See* intelligence community.
- non-DOD members. *See* intelligence community.

DSCA, 1-16 through 1-18. *See also* decisive action, tasks.

E

electronic intelligence. *See* signals intelligence.

event template and matrix, 5-19, 5-33

F

facts, 5-23 through 5-26, 5-55

force projection, 6-1 through 6-7
- key planning factors, 6-4
- processes, 6-8 through 6-27

foreign instrumentation signals intelligence. *See* signals intelligence.

Foreign Materiel Program, 4-57, 4-58

forensic-enabled intelligence, 4-82, 4-83. *See also* complementary intelligence capabilities.

fusion, 4-4

fusion centers, 2-31, 2-65 through 2-68

G

G-2/S-2
- support to the commander, 1-11, 1-9, 1-13

generating intelligence knowledge, 6-2, 6-4
- as a fundamental of all-source intelligence, 4-6

geospatial information and services. *See* geospatial intelligence.

geospatial intelligence, 4-16 through 4-23. *See also* intelligence disciplines.

granting access, 2-39 through 2-41. *See also* intelligence enterprise, leveraging.

H

hazards, 2-19

high-value target list, 5-18

human intelligence, 4-24 through 4-32. *See also* intelligence disciplines.

I

imagery. *See* geospatial intelligence.

imagery intelligence. *See* geospatial intelligence.

incident awareness and assessment (IAA), 1-18

information collection, 5-43 through 5-45
- answers CCIRs and other requirements, 1-38
- defined, 1-24
- primary means of, 1-28, 2-57, 2-59, 4-1
- support to, 4-6, 4-7, 6-6
- tasks, 1-24 through 1-28, 1-31, 5-8, 5-36. *See also* Army capabilities.
- to support the incident commander, 1-17

information collection asset
- assists DSCA, 1-18
- availability, 5-21
- employing, 2-2, 2-4
- evaluate for suitability, 3-16
- task-organizing, 1-22
- use of, 1-11, 1-13

information collection plan, 5-36
- answering CCIRs, 1-9
- criteria for effective plan, 5-44
- determine effectiveness, 3-16
- determine initial, 5-31, 5-32
- support to targeting, 5-46

INSCOM. *See* division and above intelligence organizations.

intelligence
- aspects of, 1-5
- effectiveness criteria, 2-6, 2-7
- survey, 6-5, 6-14

intelligence analysis
- as a fundamental of all-source intelligence, 4-6
- assist DSCA, 1-18
- defined, 2-61 through 2-64. *See also* intelligence core competencies.

intelligence communications architecture. *See* intelligence enterprise.

intelligence community, 2-46 through 2-48
- DOD agencies, 2-49
- efforts of, 2-29
- non-DOD members, 2-50

intelligence core competencies, 2-51, 2-52

intelligence disciplines, 4-9, 4-10. *See also* single-source intelligence.

intelligence enterprise, 2-29 through 2-31
- intelligence communications architecture, 2-32 through 2-34
- leveraging, 2-36, 6-4

intelligence estimate, 5-48 through 5-51. *See also* intelligence products, types of.

intelligence operations. *See also* information collection, primary means of.
- affected by technical channels, 1-30
- defined, 2-55 through 2-60. *See also* intelligence core competencies.
- PED activities within, 4-87 through 4-91
- support in DSCA, 1-17

intelligence preparation of the battlefield. *See* IPB.

intelligence process
- continuing activities, 3-3 through 3-6
- joint, 3-2
- steps, 3-3 through 3-6
- supporting requirements, 4-91

intelligence products, 2-16, 3-8. *See also* production.
- develop, 4-2
- types of, 5-47

intelligence reach
- aspects of, 3-18
- defined, 2-37, 2-38. *See also* intelligence enterprise, leveraging.

intelligence running estimate, 5-54 through 5-57. *See also*

Entries are by paragraph number.

intelligence products, types of.
intelligence summary, 5-52, 5-53. *See also* intelligence products, types of.
intelligence, surveillance, and reconnaissance, 1-4, 5-43
intelligence synchronization, 2-53, 2-54. *See also* intelligence core competencies.
intelligence warfighting function, 1-3
  civil considerations and sociocultural understanding, 2-22 through 2-28
  defined, 2-8 through 2-10
  during stability tasks, 1-14
  planning considerations, 3-14 through 3-23
  support to unified land operations and decisive action, 1-2
  tasks, 2-11 through 2-15
  terrain and weather, 2-20, 2-21
  threats and hazards, 2-17 through 2-19
IPB
  and civil considerations, 2-23
  intelligence estimate tab, 5-51
  support to mission analysis, 5-9 through 5-19
  support to, 4-6, 4-7
IPB products
  develop initial, 6-5
  for offense, 1-10
  for stability, 1-15
  initial, 5-36
  for defense, 1-12

K

knowledge management, 2-38. *See also* intelligence enterprise, leveraging.

L

liaison, 3-23, 4-31

M

MDMP, 3-12, 5-5
  COA analysis (wargaming), 5-36 through 5-40
  COA approval, 5-41
  COA development, 5-37
  mission analysis, 5-6 through 5-36
  orders production 5-42
measurement and signature intelligence, 4-33 through 4-41. *See also* intelligence disciplines.
military decisionmaking process. *See* MDMP.
mission analysis
  briefing, 5-34
mission command. *See also* intelligence, aspects of.
  and fusion centers, 2-65
  and intelligence synchronization, 2-53
  and the intelligence enterprise, 2-31
  intelligence warfighting function synchronization, 5-2
  support from the intelligence process, 3-1
mission variables. *See also* operational environment.
  to express civil considerations, 2-22, 2-23

O

offensive tasks, 1-10, 1-11, 1-14. *See also* decisive action, tasks.
open-source intelligence, 4-42 through 4-47. *See also* intelligence disciplines.
operational environment
  defined, 1-6
  operational and mission variables, 1-7
operational variables. *See also* operational environment.
  to express civil considerations, 2-22, 2-23
operations process, 3-1, 3-5
order
  high headquarters, 5-8
  production, 3-4, 3-12. *See also* MDMP.

P

PED, 4-84 through 4-93, 6-4. *See also* single-source intelligence.
plan and direct step, 3-11 through 3-23. *See also* intelligence process, steps.
plan requirements and assess collection, 1-26. *See also* information collection, tasks
  requirements resulting from, 3-17
  to identify intelligence gaps, 3-16
planning requirements tools, 3-16, 3-36
posting, 2-44. *See also* intelligence enterprise, leveraging.
predictive assessment. *See* assess.
priority intelligence requirement, 3-31, 6-4. *See also* requirements.
processing. *See* production.
  PED enablers enhance, 4-89
processing, exploitation, and dissemination. *See* PED.
production, 3-29 through 3-33. *See also* intelligence process, steps.

R

reconnaissance. *See also* information collection, primary means of.
  CBRN elements, 4-37
request for information, 3-22
requirements, 3-17, 6-6
risk management, 4-7, 5-27, 5-28

S

searches and queries, 3-19. *See also* intelligence reach, aspects of.
security operations. *See* information collection, primary means of.
sharing, 2-42, 2-43. *See also* intelligence enterprise, leveraging.
signals intelligence, 4-48 through 4-53. *See also* intelligence disciplines.
single-source intelligence, 4-8. *See also* Army intelligence capabilities.
situational understanding
  COP as primary tool to support commander, 5-58
  enables commanders, 5-1

Entries are by paragraph number.

of threats, terrain and weather, and civil considerations, 2-1

sociocultural (pertaining to), 1-25, 6-5. *See also* intelligence warfighting function.

stability tasks, 1-14, 1-15. *See also* decisive action, tasks.

staff channels, 3-42. *See also* dissemination, channels.

surveillance, 4-37. *See also* information collection, primary means of.

sustainment, 4-93, 6-5

T

targeting, 4-93
support to, 4-6, 4-7, 5-46

tasks
essential, 5-20
implied, 5-20, 6-14
specified, 5-20, 6-14

technical channels, 1-30, 1-31, 3-43, 4-93. *See also* Army capabilities; dissemination, channels.

technical intelligence, 4-54 through 4-63. *See also* intelligence disciplines.

terrain. *See also* intelligence warfighting function; situational understanding.
effects on operations, 5-57
in the intelligence summary, 5-52
intelligence estimate tab, 5-51
military aspects of, 5-10

threat, 2-17, 2-18. *See also* intelligence products; IPB products; situational understanding.
capabilities, 5-50, 5-52, 5-55, 5-57
characteristics, 5-50, 5-57
COAs, 1-11, 5-57
defeat of, 1-2
develop capabilities, 5-16
develop models, 5-17
identification and analysis in stability tasks, 1-15
monitoring, 6-7

U

U.S. Army Intelligence and Security Command. *See* INSCOM.

unified action partners, 1-3, 1-4

unified action, 1-1

unified land operations, 1-1, 1-2

W

warfighting functions, 2-45

wargaming. *See* MDMP.

warning order, 5-36

watchlisting. *See* BEI, products.

weapons technical intelligence, 4-57, 4-60, 4-61

weather, 5-11 through 5-14. *See also* intelligence warfighting function; situational understanding.
effects on operations, 5-57
in the intelligence summary, 5-52
intelligence estimate tab, 5-50

ADRP 2-0
31 August 2012

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1220803

DISTRIBUTION:

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

PIN: 103030-000