FM 2-0

INTELLIGENCE

HEADQUARTERS, DEPARTMENT OF THE ARMY

FINAL DRAFT

MARCH 2009

* This Publication Supersedes FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.

Field Manual
No. 2-0

Headquarters
Department of the Army
Washington, DC, (Final Draft)

Intelligence

Contents

***This publication supersedes FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.**

Figures

Tables

Preface

FM 2-0 is the Army's keystone manual for military intelligence (MI) doctrine. It describes—

- The fundamentals of intelligence operations.
- The operational environment.
- The intelligence warfighting function.
- The intelligence process.
- MI roles and functions within the context of Army operations.
- Intelligence in unified action.
- Intelligence considerations in strategic readiness.
- The intelligence disciplines.

The significant intelligence updates and changes in this manual from FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008, are detailed in the Introduction. This manual conforms to the overarching doctrinal precepts presented in FM 3-0.

This FM provides doctrinal guidance for the intelligence warfighting function in support of commanders and staffs. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and procedures (TTP); materiel and force structure; and institutional and unit training for intelligence operations.

This FM provides MI guidance for commanders, staffs, trainers, and MI personnel at all echelons. It forms the foundation for MI and intelligence warfighting function doctrine development.

This FM applies to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). It is also intended for commanders and staffs of joint and combined commands, US Naval and Marine Forces, units of the US Air Force, and the military forces of multinational partners.

Headquarters, US Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the US Army Intelligence Center and School. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATZS-FDT- (FM 2-0), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. Send comments and recommendations by email to ATZS-FDC-D@conus.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form 2028.

Introduction

FM 2-0 updates the Army's keystone doctrine on intelligence. The following paragraphs summarize the most important updates and changes from FM 2-0, 17 May 2004, with change 1 dated 11 September 2008.

Chapter 1 makes the following changes:

- Replaces the intelligence battlefield operating system with the intelligence warfighting function and discusses the mission variables for which the intelligence warfighting function is responsible: enemy, terrain (to include weather), and civil considerations.
- Updates the intelligence tasks (METL).
- Addresses the concept of actionable intelligence.
- Describes the Characteristics of Effective Intelligence which includes the six relevant information quality criteria plus three additional criteria.
- Updates the definition of priority intelligence requirements and describes intelligence requirements.
- Updates the intelligence process, adding a step (Generate Intelligence Knowledge), combining the Collect and Process steps, changing the Disseminate continuing activity to Propagate and describing and additional input to the intelligence process (Commander's Input).
- Introduces the concept of the intelligence survey as a means to provide the unit intelligence officer with an initial assessment for recommending intelligence asset apportionment within the area of operation (AO) and how best to use the unit's intelligence assets within the AO.
- Addresses the concept of critical thinking.
- Increases the number of intelligence disciplines from seven to nine by adding geospatial intelligence (GEOINT) and open-source intelligence (OSINT).

Chapter 2 makes the following changes:

- Updates Joint Intelligence Organizations based on JP 2-0 and JP 3-33.
- Updates Unified Action and Force Projection Operations sections based on FM 3-0.
- Discusses the concept and includes the Army definition of reconnaissance, surveillance, and target acquisition/intelligence, surveillance, and reconnaissance (RSTA/ISR).

Chapter 3 updates the operational concept, operations definitions, and Army capabilities and introduces the elements of combat power based on FM 3-0.

Chapter 4 makes the following changes:

- Further addresses the Generate Knowledge step during the intelligence and operations process interaction.
- Addresses the concept of Red Teaming.

Chapters 5 through 13 make the following changes:

- Incorporates the updated steps of the IPB process in accordance with FM 2-01.3.
- Updates the counterintelligence functions and organizations.
- Updates human intelligence (HUMINT) functions and organizations based on FM 2-22.3.
- Introduces GEOINT as an intelligence discipline and discusses the Army implementation of GEOINT.

- Updates the imagery intelligence (IMINT) definitions.
- Incorporates changes to the measurement and signature intelligence (MASINT) discipline.
- Introduces OSINT as an intelligence discipline.
- Updates signals intelligence (SIGINT) definitions and organizations.
- Provides an example format for the intelligence summary, intelligence estimate and the intelligence running estimate.
- Updates the linguist support section.
- Adds a short discussion of language technology.

PART ONE

Intelligence in the Full Spectrum Operations

Part One discusses the role of intelligence from stable peace to general war and back to stable peace. The primary focus of the intelligence warfighting function is to provide timely, relevant, accurate, predictive, and tailored intelligence that focuses missions and operations in the right places at the right time.

Chapter 1 describes the operational environment and the roles of intelligence within the operational environment. It introduces the intelligence warfighting function, the intelligence tasks, and the intelligence process, which are the mechanisms through which the intelligence warfighting function supports the warfighter. This chapter also introduces the intelligence disciplines, which are explained in detail in Part Three of this manual.

Chapter 2 describes the interaction of the intelligence warfighting function within the nation's intelligence community structure; it provides an overview of the intelligence community at the national level and the unified action level—joint, interagency, intergovernmental, and multinational (JIIM) and aspects of full spectrum operations. This chapter also discusses the concepts and components of intelligence reach.

Chapter 1

Intelligence and the Operational Environment

THE OPERATIONAL ENVIRONMENT

1-1. **The operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decision of the commander** (JP 3-0). The operational environment encompasses physical areas and factors of the air, land, maritime, and space domains. It also includes the information environment and enemy, adversary, friendly, and neutral systems.

OPERATIONAL VARIABLES

1-2. Analysis of the operational environment—in terms of political, military, economic, social, information, infrastructure, with the addition of physical environment and time (PMESII-PT) variables—provides relevant information that senior commanders use to understand, visualize, and describe the operational environment. As a set, these operational variables are often abbreviated as PMESII-PT.

Political

1-3. The political variable describes the distribution of responsibility and power at all levels of governance.

1-4. Political structures and processes enjoy varying degrees of legitimacy with populations from the local through international levels. Formally constituted authorities and informal or covert political powers strongly influence events. Political leaders can use ideas, beliefs, actions, and violence to enhance their power and control over people, territory, and resources. Many sources of political motivation exist. These may include charismatic leadership; indigenous security institutions; and religious, ethnic, or economic communities. Political opposition groups or parties also affect the situation. Each may deal differently with US or multinational forces. Understanding the political circumstances helps commanders and staffs recognize key organizations and determine their aims and capabilities.

1-5. Understanding political implications requires analyzing all relevant partnerships—political, economic, military, religious, and cultural. This analysis captures the presence and significance of external organizations and other groups; these include groups united by a common cause. Examples are private security organizations, transnational corporations, and nongovernmental organizations (NGOs) that provide humanitarian assistance.

1-6. A political analysis also addresses the effect of will. Will is the primary intangible factor; it motivates participants to sacrifice to persevere against obstacles. Understanding the motivations of key groups (for example, political, military, and insurgent) helps clarify their goals and willingness to sacrifice to achieve their ends.

1-7. The political variable includes the US domestic political environment. Therefore, mission analysis and monitoring the situation includes an awareness of national policy and strategy.

Military

1-8. The military variable includes the military capabilities of all armed forces in a given operational environment. For many states, an army is the military force primarily responsible for maintaining internal and external security. Paramilitary organizations and guerrilla forces may influence friendly and hostile military forces. Militaries of other states not directly involved in a conflict may also affect them. Therefore, analysis should include the relationship of regional land forces to the other variables. Military analysis examines the capabilities of enemy, adversary, host nation (HN), and multinational military organizations. Such capabilities include—

- Equipment.
- Manpower.
- Doctrine.
- Training levels.
- Resource constraints.
- Leadership.
- Organizational culture.
- History.
- Nature of civil-military relations.

1-9. Understanding these factors helps commanders estimate the actual capabilities of each armed force. Analysis should focus on each organization's ability to field capabilities and use them domestically, regionally, and globally.

Economic

1-10. The economic variable encompasses individual and group behaviors related to producing, distributing, and consuming resources. Specific factors may include the influence of—

- Industrial organizations.
- Trade.
- Development (including foreign aid).
- Finance.
- Monetary policy and conditions.
- Institutional capabilities.
- Geography.
- Legal constraints (or the lack of them) on the economy.

1-11. While the world economy is becoming interdependent, local economies differ. These differences significantly influence political choices, including individuals' decisions to support or subvert the existing order. Many factors create incentives or disincentives for individuals and groups to change the economic status quo. These may include—

- Technical knowledge.
- Decentralized capital flows.
- Investment.
- Price fluctuations.
- Debt.
- Financial instruments.
- Protection of property rights.
- Existence of black market or underground economies.

1-12. Thus, indicators measuring potential benefits or costs of changing the political-economic order may enhance understanding the social and behavioral dynamics of friendly, adversary, and neutral entities.

Social

1-13. The social variable describes societies within an operational environment. A society is a population whose members are subject to the same political authority, occupy a common territory, have a common culture, and share a sense of identity. Societies are not monolithic. They include diverse social structures. Social structure refers to the relations among groups of persons within a system of groups. It includes institutions, organizations, networks, and similar groups. (FM 3-24 discusses socio-cultural factors analysis and social network analysis.)

1-14. Culture comprises shared beliefs, values, customs, behaviors, and artifacts that society members use to cope with their world and with one another. Societies usually have a dominant culture but may have many secondary cultures. Different societies may share similar cultures, but societal attributes change over time. Changes may occur in any of the following areas:

- Demographics.
- Religion.
- Migration trends.
- Urbanization.
- Standards of living.
- Literacy and nature of education.
- Cohesiveness and activity of cultural, religious, or ethnic groups.

1-15. Social networks, social status and related norms, and roles that support and enable individuals and leaders require analysis. This analysis should also address societies outside the operational area whose actions, opinions, or political influence can affect the mission.

1-16. People base their actions on perceptions, assumptions, customs, and values. Cultural awareness helps identify points of friction within populations, helps build rapport, and reduces misunderstandings. It can improve a force's ability to accomplish its mission and provide insight into individual and group intentions. However, cultural awareness requires training before deploying to an unfamiliar operational environment and continuous updating while deployed. Commanders develop their knowledge of the societal aspects within their areas of operations (AO) to a higher level of cultural astuteness, one that allows them to understand the impact of their operations on the population and prepares them to meet local leaders face-to-face.

Information

1-17. Joint doctrine defines the *information environment* as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The environment shaped by information includes leaders, decision makers, individuals, and organizations. The global community's access and use of data, media, and knowledge systems occurs in the information shaped by the operational environment. Commanders use information engagement to shape the operational environment as part of their operations.

1-18. Media representatives significantly influence the information that shapes the operational environment. Broadcast and Internet media sources can rapidly disseminate competing views of military operations worldwide. Adversaries often seek to further their aims by controlling and manipulating how audiences at all levels perceive a situation's content and context. Media coverage influences US political decision making, popular opinion, and multinational sensitivities.

1-19. Complex telecommunications networks now provide much of the globe with a vast web of communications capabilities. Observers and adversaries have unprecedented access to multiple information sources. They often attempt to influence opinion by providing their own interpretation of events. Televised news and propaganda reach many people. However, in developing countries, information still may flow by less sophisticated means such as messengers and graffiti. Understanding the various means of communications is important. Observers and adversaries control information flow and influence audiences at all levels.

Infrastructure

1-20. Infrastructure comprises the basic facilities, services, and installations needed for a society's functioning. Degrading infrastructure affects the entire operational environment. Infrastructure also includes technological sophistication—the ability to conduct research and development and apply the results to civil and military purposes.

1-21. Not all segments of society view infrastructure in the same way. Improvements viewed by some as beneficial may not be perceived as such by all. One community may perceive certain improvements as favoring other communities at its expense. Effective information engagement is necessary to address such concerns. Actions affecting infrastructure require a thorough analysis of possible effects.

Physical Environment

1-22. The physical environment includes the geography and manmade structures in the operational area. The following factors affect the physical environment:

- Manmade structures, particularly urban areas.
- Climate and weather.
- Topography.

- Hydrology.
- Natural resources.
- Biological features and hazards.
- Other environmental conditions.

1-23. The enemy understands that less complex and open terrain often exposes their military weaknesses. Therefore, they may try to counteract US military advantages by operating in urban or other complex terrain and during adverse weather conditions.

Time

1-24. Time is a significant consideration in military operations. Analyzing it as an operational variable focuses on how an operation's duration might help or hinder each side. This has implications at every planning level. An enemy with limited military capability usually views protracted conflict as advantageous to them. They avoid battles and only engage when conditions are overwhelmingly in their favor. This is a strategy of exhaustion. Such a strategy dominated the American Revolution and remains effective today. The enemy concentrates on surviving and inflicting friendly and civilian casualties over time. Although the military balance may not change, this creates opportunities to affect the way domestic and international audiences view the conflict. Conversely, a hostile power may attempt to mass effects and achieve decisive results in a short period.

1-25. While the operational variables are directly relevant to campaign planning, they may be too broad to be applied directly to tactical planning. That does not mean they are not of value at all levels; they are fundamental to developing the understanding of the operational environment necessary to conduct planning at any level, in any situation.

1-26. When identifying threats based on the systems approach to PMESII, there are three primary components of the operational environment for which the intelligence warfighting function is responsible: threat, terrain (to include the weather), and civil considerations.

1-27. The degree to which each operational variable provides useful information depends on the situation and echelon. Once the G-2/S-2 has completed their overall analysis, they must go back and factor in small unit leaders' intelligence requirements. For example, social and economic variables often receive close analysis as part of enemy and civil considerations at brigade and higher levels. They may affect the training and preparation of small units. However, they may not be relevant to a small-unit leader's mission analysis. That leader may only be concerned with questions, such as "Who is the tribal leader for this village?" "Is the electrical generator working?" "Does the enemy have antitank missiles?

MISSION VARIABLES

1-28. Upon receipt of a warning order (WARNO) or mission, Army leaders narrow their focus to six mission variables. Mission variables are those aspects of the operational environment that directly affect a mission. They outline the situation as it applies to a specific Army unit. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). These are the categories of relevant information used for mission analysis. Army leaders use the mission variables to synthesize operational variables and tactical-level information with local knowledge about conditions relevant to their mission. The intelligence warfighting function is responsible for describing the enemy, terrain and weather, and civil considerations:

- **Enemy.** Relevant information regarding the enemy may include the following:
  - Threat characteristics (previously order of battle factors).
  - Threat courses of action (COAs).
- **Terrain and Weather.** Terrain and weather are natural conditions that profoundly influence operations. Terrain and weather are neutral; they favor neither side unless one is more familiar with—or better prepared to operate in—the environment.

- **Civil Considerations.** Civil considerations comprise six characteristics expressed in the memory aid ASCOPE:
  - **A**reas.
  - **S**tructures.
  - **C**apabilities.
  - **O**rganizations.
  - **P**eople.
  - **E**vents.

Note. For additional information on ASCOPE and the intelligence preparation of the battlefield (IPB) process, see FM 2-01.3. Understanding the operational environment requires understanding the civil aspects of the area of influence. Civil considerations reflect how the manmade infrastructure, civilian institutions, and the attitudes and activities of the civilian leaders, populations, and organizations within an AO influence the conduct of military operations.

1-29. METT-TC enables leaders to synthesize operational level information with local knowledge relevant to their missions and tasks in a specified AO. Tactical and operational leaders can then anticipate the consequences of their operations before and during execution. See FM 3-0 for a detailed discussion of PMESII-PT and METT-TC.

THE INTELLIGENCE WARFIGHTING FUNCTION

1-30. *The intelligence warfighting function is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, and civil considerations* (FM 3-0). It includes tasks associated with intelligence, surveillance, and reconnaissance (ISR) operations and is driven by the commander. Intelligence is more than just collection. It is a continuous process that involves analyzing information from all sources and conducting operations to develop the situation. The intelligence warfighting function includes the following tasks:

- Support to force generation.
- Support to situational understanding.
- Perform ISR.
- Support to targeting and information superiority.

1-31. The intelligence warfighting function is one of six warfighting functions—movement and maneuver, intelligence, fires, sustainment, command and control (C2), and protection. *A warfighting function is a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives* (FM 3-0). (See FM 3-0, chapter 4, for a detailed discussion of the warfighting functions.) The intelligence warfighting function is a flexible force of personnel, organizations, and equipment that, individually or collectively, provide commanders with the timely, relevant, accurate, predictive, and tailored intelligence required to visualize the AO, assess the situation, and direct military actions. Additionally, the intelligence warfighting function—

- Is a complex system that operates worldwide, from below ground to space, in support of an operation, to include the ability to leverage theater and national capabilities.
- Requires cooperation and division of ISR and analysis efforts internally, higher, lower, adjacent, and across components and multinational forces.

1-32. The intelligence warfighting function not only includes assets within the MI branch but also includes the assets of all branches or warfighting functions that conduct intelligence warfighting function tasks. Every Soldier, as a part of a small unit, is a potential information collector and an essential component to

help reach situational understanding. Each Soldier develops a special level of awareness simply due to exposure to events occurring in the AO and has the opportunity to collect and report information by observation and interaction with the population (see paragraph 3-3).

1-33. Planning and executing military operations will require intelligence regarding the threat (traditional, irregular, catastrophic, and disruptive) and the AO. The intelligence warfighting function generates intelligence and intelligence products that portray the enemy and aspects of the environment. These intelligence products enable the commander to identify potential COAs, plan operations, employ forces effectively, employ effective tactics and techniques, and implement protection.

1-34. The intelligence warfighting function is always engaged in supporting the commander in offensive, defensive, stability, and, when directed, civil support operations. Intelligence provides products that are timely, relevant, accurate, predictive, and tailored. Hard training, thorough planning, meticulous preparation, and aggressive execution posture the Army for success. In the current environment we must maintain intelligence readiness to support operations. This support reaches across full spectrum operations and levels of war to produce the intelligence required to successfully accomplish the mission through a combination of space, aerial, seaborne, and ground-based systems to provide the most comprehensive intelligence possible. During force projection operations, the intelligence warfighting function supports the commander with accurate and responsive intelligence from predeployment through redeployment.

1-35. The intelligence warfighting function architecture provides specific intelligence and communications structures at each echelon from the national level through the tactical level. (In recent years, brigade combat team [BCT] intelligence capabilities and access have been significantly increased.)These structures include intelligence organizations, systems, and procedures for generating intelligence knowledge, planning, preparing, collecting, and producing intelligence and other critical information in a useable form to those who need it, when they need it. Effective communications connectivity and automation are essential components of this architecture.

PURPOSE OF INTELLIGENCE

1-36. The purpose of intelligence is to provide commanders and their staffs with timely, relevant, accurate, predictive, and tailored intelligence about the enemy and the environment in a timely manner. Intelligence supports the planning, preparing, execution, and assessment of missions. The most important role of intelligence is to support the commander's decision making to drive operations. Intelligence must be timely, relevant, accurate, predictive, and tailored.

ROLE OF INTELLIGENCE

1-37. Intelligence drives the conduct of operations; therefore, the G-2/S-2 is responsible for ensuring that the intelligence warfighting function operates smoothly and efficiently so that the commander receives timely, relevant, accurate, predictive, and tailored information in a timely manner. The G-2/S-2 is not simply a manager but is the primary advisor to the commander on how to utilize ISR assets, supports the commander with analysis and production, and drives ISR collection.

1-38. The commander requires intelligence about the enemy and the environment prior to engaging in operations in order to effectively execute battles, engagements, and other missions within full spectrum operations. Intelligence assists the commander in visualizing the environment, organizing the forces, and controlling operations to achieve the desired objectives or end-state. Intelligence supports protection by alerting the commander to threats and assisting in preserving and protecting the force.

1-39. The unit may need to deal with multiple threats. The commander must understand how current and potential enemies organize, equip, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, executing, and assessing military operations. The commander must also understand the AO and area of influence and their effects on both friendly and threat operations. The commander receives mission-oriented intelligence on enemy forces and

the AO and area of influence from the G-2/S-2. The G-2/S-2 depends upon the ISR effort to collect and provide information on the threat and environment.

1-40. One of the most significant contributions that intelligence personnel can accomplish is to accurately predict possible enemy events and actions. Although intelligence is never perfect and can be extremely time consuming and difficult, providing worst case and probable COA based on verified or probable threat capability and intent during wargaming is a core intelligence function. Thus, predictive intelligence enables the commander and staff to anticipate key enemy events or reactions and develop corresponding plans or counteractions. Intelligence professionals must tailor the intelligence to the commander's requirements to support the commander's situational understanding. Commanders must receive the intelligence in a format that is clear and concise so they can understand it, believe it, and act on it. It is the G-2/S-2's primary function to deliver that intelligence to the commander in a timely manner. In order for intelligence professionals to provide the best possible support and to tailor products to the commanders' needs, the commander and the G-2/S-2 must develop a close professional relationship. Through this doctrinal concept, intelligence drives operations.

INTELLIGENCE TASKS

1-41. The personnel and organizations within the intelligence warfighting function conduct four primary intelligence tasks that facilitate the commander's visualization and understanding of the threat and the environment. These tasks are interactive and often take place simultaneously. (Refer to FM 7-15 for the complete subordinate task listing.) Table 1-1 shows these tasks tailored to the commander's needs.

SUPPORT TO FORCE GENERATION

1-42. Support to force generation is the task of generating knowledge concerning an area of possible employment or deployment, facilitating future intelligence operations, and tailoring the force. It includes establishing intelligence communication architecture and developing the intelligence staff's knowledge management—these enable intelligence reach, collaborative analysis, data storage, processing, and analysis and intelligence production between the strategic and operational intelligence communities to the tactical intelligence warfighting function. This task consists of five subtasks.

Provide Intelligence Readiness

1-43. Intelligence readiness operations support ongoing operations, contingency planning, and operational preparation by developing baseline knowledge of multiple potential threats and operational environments. These operations and related intelligence training activities enable the intelligence warfighting function to support the commander's intelligence requirements effectively. This task consists of three subtasks:

- **Perform Indications & Warnings (I&W).** This activity provides the commander with advance warning of threat actions or intentions. The intelligence officer develops I&W to alert the commander rapidly of events or activities that would change the basic nature of the operations. I&W enables the commander to quickly reorient the force to unexpected contingencies and shape the operational environment.
- **Conduct Intelligence Readiness Operations.** Intelligence readiness operations support contingency planning and preparation by developing baseline knowledge of multiple potential threats and operational environments. This information and training enables a collaborative effort and environment to provide the best possible initial threat understanding.
- **Conduct Foundry.** Foundry is a training program designed to sustain critical intelligence capabilities, perishable intelligence skills, and provide regional focus, technical training, and functional expertise for the tactical MI force through home-station training platforms, mobile training teams, and live environment training opportunities. Foundry provides a single "hub" for advanced skills training across the Active Army, ARNG, and USAR MI force, as well as train leaders who supervise MI missions and all Soldiers who perform MI activities.

Table 1-1. Intelligence tailored to the commander's needs

Intelligence Tasks ►	***Commander's Focus*** ►	***Commander's Decisions***
Support to Force Generation • Provide Intelligence Readiness. • Establish Intelligence Architecture. • Provide Intelligence Overwatch. • Generate Intelligence. • Tailor the Intelligence Force.	Orient on contingencies.	Should the unit's level of readiness be increased? Should the OPLAN 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.	Plan an operation. Prepare. Execute. Assess. Secure the force.	Which COA will I implement? Which enemy actions are expected?
Perform Intelligence, Surveillance, and Reconnaissance • Perform ISR Synchronization. • Perform ISR Integration. • Conduct Reconnaissance. • Conduct Surveillance. • Conduct Related Missions and Operations.	Plan an operation. Prepare. Execute. Assess.	Which DPs, HPTs, HVTs, are linked to the enemy's actions? Are the assets available and in position to collect on the DPs, HPTs, HVTs? Have the assets been repositioned for contingency missions?
Support to Targeting and Information Superiority • Provide Intelligence Support to Targeting. • Provide Intelligence Support to Information Superiority. • Provide Intelligence Support to Combat Assessment.	Utilize lethal or nonlethal fires against targets. Destroy/suppress/neutralize targets. Reposition intelligence or attack assets.	Is the unit's fire (lethal and nonlethal) and maneuver effective? Should the same targets be reengaged? Is the unit's information engagement effective?

Establish Intelligence Architecture

1-44. Intelligence architecture activity includes complex and technical issues like sensors, dataflow, hardware, software, communications, communications security (COMSEC) materials, network

classification, technicians, database access, liaison officers (LNOs), training, and funding. Well-defined and designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible threat, terrain, weather, and civil considerations understanding. This task consists of four subtasks:

- **Conduct Intelligence Reach.** *Intelligence reach is a process 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 deployed in theater and outside the theater unconstrained by geographic proximity, echelon, or command* (TC 2-33.5). Such intelligence helps prepare for the mission and answer the commander's critical information requirements (CCIRs) during the mission directly from the source (pull) without the need to wait for the information to come to them (push).
- **Develop and Maintain Automated Intelligence Networks.** Use existing automated information systems, such as the Distributed Common Ground System-Army (DCGS-A), or create operationally specific networks to connect unique assets, units, echelons, agencies, or multinational partners for intelligence, collaborative analysis and production, dissemination, and intelligence reach. These networks include accessibility and interoperability across the AO, to include unclassified and classified means. This task includes identifying deficiencies in systems or networks, Service procedures, system administration procedures, security procedures, alternate power plan, redundancy capability, system backups, and update procedures.
- **Establish and Maintain Access.** Establish and provide access to classified and unclassified programs, databases, networks, systems, and other web-based collaborative environments for Army, joint, interagency, and multinational organizations to facilitate intelligence reporting, production, dissemination, sustainment, intelligence reach, and a multi-level collaborative information environment.
- **Create and Maintain Intelligence Databases.** Create and maintain unclassified and classified databases to create interoperable and collaborative environments for Army, joint, interagency, and multinational organizations to facilitate intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach. This subtask also includes the requirements for format and standardization, indexing and correlation, normalization, storage, security protocols, and associated applications. The following must be addressed in database development, management, and maintenance:
  - Data sources.
  - Information redundancy.
  - Import and export standards.
  - Data management.
  - Update and backup procedures.
  - Data mining, query, and search protocols.

Provide Intelligence Overwatch

1-45. Intelligence overwatch is creating standing, fixed analytical intelligence capabilities that provide dedicated intelligence support and overwatch to committed maneuver units. The overwatch cell is connected via a shared intelligence network that can pull information from multiple sources and provide succinct answers (vice megabytes of information) directly to supported units when time is of the essence.

Generate Intelligence Knowledge

1-46. Generate intelligence knowledge is a continuous and user-defined task driven by the commander that begins prior to mission receipt and provides the relevant knowledge required concerning the operational environment for the conduct of operations. Generate intelligence knowledge uses these components as a start point to acquire and organize the information. The execution of this task must follow all applicable policies and regulations on the collection of information and operations security (OPSEC). The information

and intelligence obtained are refined for use in mission analysis through functional analysis. Knowledge is obtained through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; OSINT; or other information sources that support the conduct of operations. The execution of this task must follow all applicable policies and regulations on the collection of information and OPSEC. This task contains five subtasks:

- **Develop the Foundation to Define Threat Characteristics.** Obtain detailed information and intelligence concerning threat characteristics affecting the conduct of operations. Obtain this information through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; OSINT; or other information sources to support operations, planning, execution, and commander's decisions. This subtask requires specific and detailed information for each threat characteristic.
- **Obtain Detailed Terrain Information and Intelligence.** Obtain detailed information and intelligence on the terrain of the expected area of interest (AOI) through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; OSINT; or other information sources to support operations, planning, execution, and commander's decisions. The information, intelligence, products, and material obtained are refined for use in mission analysis, IPB, and planning through functional analysis. This subtask encompasses the military aspects of terrain.
- **Obtain Detailed Weather and Weather Effects Information and Intelligence.** Obtain detailed information and intelligence concerning the recent and historical weather trends, seasonal patterns, aspects of weather, and weather zones. Obtain information on how the weather affects friendly and enemy forces and operations in the AOI through intelligence reach; research; data mining; database access via the digital topographic support system; academic studies, products, or materials; intelligence archives; OSINT; or other information sources to support operations, planning, execution, and commander's decisions. The Integrated Meteorological System is accessed through DCGS-A and provides commanders at all echelons of command with an automated weather system. This system receives, processes, and disseminates weather observations, forecasts, and weather and environmental effects decision aids to all warfighting functions. The information, intelligence, products, and material obtained are refined for use in mission analysis, IPB, and planning through functional analysis. This subtask requires specific and detailed information for each weather factor.
- **Obtain Detailed Civil Considerations Information and Intelligence.** Obtain detailed information and intelligence concerning the civil considerations within or affecting the expected AOI through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; OSINT; or other information sources to support operations, planning, execution, and commander's decisions. The data, information, intelligence, products, and material obtained are refined for use in IPB, and planning through functional analysis. This subtask requires specific and detailed information for each factor.
- **Complete Studies.** Study and provide understanding of the local populations; cultures and caste system; societal systems or organizations; political systems and structures; religions practiced and their impacts; moral beliefs and their impacts; civil authority considerations; military organizations, structure, and equipment; and attitudes toward US, multinational, or HN forces to assist in achieving goals and objectives. Studies can also include the views and attitudes of multinational and HN forces towards these factors. The study provides detailed information, assessments, and conclusions on the AOIs of the requesting command or organization. The study could be a systems or functional analysis product and should be as detailed and in-depth as time allows. This subtask has two subtasks:
  - ***Conduct Area, Regional, or Country Study of a Foreign Country.*** Study and provide mission-focused understanding of the terrain, civil considerations, weather, and threat characteristics for a specified area or region of a foreign country, to include attitudes toward joint, multinational, or HN forces to assist in achieving goals and objectives. The studies can also include the views and attitudes of multinational and HN forces. The study

provides detailed information, assessments, and conclusions on the AOIs of the requesting command or organization and should be as detailed as time allows.

- ***Conduct Specified Study.*** Study and provide focused understanding of the terrain, civil considerations, weather, and threat characteristics for a specified topic or requirement. The study provides detailed information, assessments, and conclusions on the AOIs of the requesting command or organization and should be as detailed and in-depth as time allows.

Tailor the Intelligence Force

1-47. The generating force uses mission analysis to focus the allocation of intelligence resources for use by a joint task force (JTF) or combatant commander (CCDR) as well as to support strategic objectives, the Army's mission, and operations at each echelon. Based on the mission analysis, the staff at each echelon allocates intelligence resources obtained through the generating force to support the commander's guidance, intent, and mission objectives.

SUPPORT TO SITUATIONAL UNDERSTANDING

1-48. Support to situational understanding is 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 enemy and the environment. It supports the commander's ability to make sound decisions.

Perform Intelligence Preparation of the Battlefield

1-49. IPB is a continuous staff planning activity undertaken by the entire staff. The staff aims to understand the operational environment and the options it presents to friendly and threat forces. IPB is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain, weather, and civil considerations in a specific AOI and for a specific mission. By applying IPB, commanders gain the information necessary to selectively apply and maximize combat power at critical points in time and space.

Perform Situation Development

1-50. Situation development is a process for analyzing information and producing current intelligence concerning the portions of the mission variables of enemy, terrain, weather, and civil considerations before and during operations. The process helps the intelligence officer recognize and interpret indicators of threat intentions, objectives, combat effectiveness, and potential COAs. Situation development confirms or denies threat COAs, provides threat locations, explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness. The locations and actions of noncombatant elements and NGOs in the AO that may impact operations should also be considered. Through situation development, the intelligence officer quickly identifies information gaps, explains threat activities in relation to the unit's operations, and assists the commander in gaining and maintaining situational understanding. Situation development helps the commander make decisions and execute branches and sequels.

Provide Intelligence Support to Protection

1-51. Provide intelligence in support of protecting the Army's fighting potential so that it can be applied at the appropriate time and place. This task includes those measures the command takes to remain viable and functional by protecting itself from effects of or recovery from threat activities. This task is linked with antiterrorism and homeland security.

Provide Tactical Intelligence Overwatch

1-52. Tactical intelligence overwatch is creating standing, fixed analytical intelligence capabilities that provide dedicated intelligence support and overwatch to committed maneuver units. The tactical

intelligence overwatch cell is connected via a shared intelligence network that can pull information from multiple sources and provide succinct answers directly to supported units when time is critical.

Conduct Police Intelligence Operations

1-53. Police intelligence is a set of systems, technologies, and processes that use data and information to analyze, understand, and focus policing operations and activities to achieve social order. Police intelligence operations (PIO) is a military police (MP) integrating function that supports the intelligence and protection warfighting functions through the integration of police engagement, police information, and police investigations to enhance situational understanding, protection of the force, and homeland security. This information, whether police, criminal, or tactical in nature, is gathered while conducting policing functions and upon analysis may contribute to CCIRs, intelligence-led, time-sensitive operations, or policing strategies necessary to forecast, anticipate, and preempt crime or related activities to maintain order.

1-54. The dissemination of police and criminal information is included in ART 5.5.1.2.3 (Conduct criminal investigations). Joint, interagency, and multination coordination is included in ART 5.2.2.1 (Prepare the Command Post for Displacement) (FM 3-19.1) (US Army Military Police School).

Note. The PIO function is not an intelligence discipline; it is a law enforcement function. However, it is within the critical intelligence task, "support situational understanding" that PIO best supports the MI cycle. Police intelligence operations are essential to this task, particularly where asymmetric threats (criminal, terrorist, and insurgents) threaten the security of US forces and military operations. This function supports and enhances the commander's situational awareness and common operational picture (COP) through collection, analysis, and appropriate dissemination of relevant criminal, police information, and criminal intelligence. Police intelligence operations are a vital tool of law enforcement and criminal investigators that distributes and focuses MP and criminal investigations assets. US Codes, executive orders, Department of Defense (DOD) directives, and Army regulations contain specific guidance regarding the prohibition of intelligence personnel from collecting intelligence on US citizens, US corporations, and resident aliens. Any access by the intelligence community to information or products resulting from PIO directed against American citizens should undergo competent legal review.

Provide Intelligence Support to Civil Affairs Operations

1-55. This task enables MI organizations to collect and provide information and intelligence products concerning the factors of ASCOPE in the AO in support of civil affairs (CA) activities.

PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

1-56. ISR is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination of systems in direct support (DS) of current and future operations. This is an integrated intelligence and operations function. For Army forces, this combined arms operation focuses on priority intelligence requirements (PIRs) while answering the CCIRs. Through ISR, commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information, combat information, and intelligence to satisfy the CCIRs and other intelligence requirements. When necessary, ISR assets focus on special requirements, such as personnel recovery.

Perform ISR Synchronization

1-57. ***Intelligence, surveillance, and reconnaissance synchronization*** **is the task that accomplishes the following: analyzes information requirements and intelligence gaps; evaluates available assets**

internal and external to the organization; determines gaps in the use of those assets; recommends intelligence, surveillance, and reconnaissance assets controlled by the organization to collect on the commander's critical information requirements; and submits requests for information for adjacent and higher collection support (FM 3-0). This task ensures that ISR, intelligence reach, and requests for information (RFIs) successfully report, produce, and disseminate information, combat information, and intelligence to support decision making. The intelligence officer, in coordination with the operations officer and other staff elements as required, synchronizes the entire collection effort. This effort includes assets the commander controls and those of adjacent and higher echelon units and organizations. It also uses intelligence reach to answer the CCIRs and other requirements. This task has two subtasks:

- **Develop Information Requirements.** The intelligence staff develops a prioritized list focusing on what information it needs to collect to produce intelligence. Additionally, the intelligence staff dynamically updates and adjusts the requirements in response to mission adjustments and changes. Each requirement is assigned a latest time information is of value (LTIOV) to meet operational requirements.
- **Develop the ISR Synchronization Plan.** The entire unit staff develops their information requirements and determines how best to satisfy them. The staff uses reconnaissance and surveillance assets to collect information. The intelligence synchronization plan includes all assets that the operations officer can task or request and coordinating mechanisms to ensure adequate coverage of the AOIs.

Perform ISR Integration

1-58. ***Intelligence, surveillance, and reconnaissance integration*** **is the task of assigning and controlling a unit's intelligence, surveillance, and reconnaissance assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans and orders** (FM 3-0). ISR integration assigns and controls a unit's ISR assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans (OPLANs) and operations orders (OPORDs). The operations officer integrates the best ISR assets through a deliberate and coordinated effort of the entire staff. Specific information requirements facilitate tasking by matching requirements to assets. Intelligence requirements are identified, prioritized, and validated. ISR integration is vital in controlling limited ISR assets. During ISR integration, the staff recommends redundancy, mix, and cue as appropriate. The result of ISR synchronization and integration is an effort focused on answering the commander's requirements. This task has two subtasks:

- **Develop the ISR Plan.** The operations officer develops the ISR plan. The entire unit staff analyzes each requirement to determine how best to satisfy it. The staff receives ISR tasks and RFIs from subordinate and adjacent units and higher headquarters. The ISR plan includes all assets that the operations officer can task or request and coordinating mechanisms to ensure adequate coverage of the AOI.
- **Execute, Evaluate, and Update the ISR Plan.** The operations officer updates the ISR plan based on information received from the intelligence officer. The operations officer is the integrator and manager of the ISR effort through an integrated staff process and procedures. As PIRs are answered and new information requirements arise, the intelligence officer updates intelligence synchronization requirements and provides the new input to the operations officer who updates the ISR plan. The intelligence and operations officers work closely with all staff elements to ensure the unit's collectors receive appropriate taskings. This ISR plan reflects an integrated collection strategy and employment, production, and dissemination scheme that will effectively answer the CCIRs. This task includes updating ISR operations through dynamic retasking and periodic updates of the ISR plan.

Conduct Reconnaissance

1-59. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about activities and resources of an enemy or potential enemy. This mission also secures data

concerning the meteorological, hydrographic, or geographic characteristics and the local population of an AO. Other detection methods include signals, imagery, measurement of signature, or other technical characteristics. This task includes performing chemical, biological, radiological, and nuclear (CBRN) reconnaissance; engineer reconnaissance (to include infrastructure reconnaissance and environmental reconnaissance).

Conduct Surveillance

1-60. Surveillance is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. Other means may include but are not limited to space-based systems, and using special CBRN, artillery, engineer, special operations forces, and air defense equipment. Surveillance involves observing an area to collect information.

Conduct Related Missions and Operations

1-61. The associated tasks (mission and debriefing program, intelligence coordination, technical channels, and intelligence support to personnel recovery) that facilitate the conduct of ISR operations and the specialized missions (sensitive site exploitation [SSE]), providing intelligence and information outside the traditional ISR construct. This task has four subtasks:

- **Establish a Mission Intelligence Briefing and Debriefing Program.** The commander must establish, support, and allocate appropriate resources for a mission briefing and debriefing program. The battle updates and after-action reviews are separate tasks from the mission briefing and debriefing program. The G-2/S-2 develops a mission intelligence briefing plan and complementary debriefing plan to support the commander's program. The intelligence mission briefing plan sensitizes Soldiers to specific information and reporting requirements, information gaps, and unique mission requirements. The intelligence mission briefings and debriefings generally follow the format of a mission briefing: review the route traveled, collection objectives of the patrol, and methods employed. The debriefing program captures the SIRs the patrol was to collect and any additional information and observations the patrol made concerning the operational environment. It also collects any fliers, pamphlets, media, or pictures the patrol found or obtained. This subtask has two subtasks:
  - ***Establish a Mission Intelligence Briefing Plan.*** The G-2/S-2 section should develop a mission intelligence briefing plan. The mission intelligence briefing plan ensures that all Soldiers conducting patrols, tactical movements, and nontactical movements are sensitized to specific information and reporting requirements, information gaps, and unique mission requirements. The intelligence mission briefing and debriefing generally follow the format of a mission briefing: review the route traveled, collection objectives of the patrol, and methods employed.
  - ***Establish a Debriefing Plan.*** The G-2/S-2 section develops a complementary debriefing plan. The debriefing plan captures the SIRs the patrol was to collect and any additional information and observations the patrol made concerning the operational environment. It also collects any fliers, pamphlets, media, or pictures the patrol found or obtained. The program should include all returning patrols, leaders who have traveled to meetings, returning human intelligence (HUMINT) collection teams (HCTs), aircrews, and others who may have obtained information of intelligence value. The G-2/S-2 section debriefs personnel, writes and submits reports, or reports information verbally, as appropriate. The requirement for a debriefing by the G-2/S-2 section following each mission should be a part of the intelligence mission briefing. Leaders should not consider the mission complete and release the personnel until the reporting and debriefings are done.
- **Conduct Intelligence Coordination.** Conduct intelligence coordination is the task carried out by the intelligence section to facilitate active collaboration horizontally, laterally, and vertically. It includes providing and conducting technical channels to refine and focus the intelligence

disciplines ISR tasks. It also properly coordinates the discipline assets when operating in another unit's AO. This subtask has two subtasks:

- ***Establish and Maintain Technical Channels.*** Intelligence commanders and the intelligence staff maintain control of each intelligence discipline during operations through technical channels to ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant US law, the law of war, international law, directives, DOD Instructions, and Orders. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess portions of the unit's collection effort. Technical channels also involve translating ISR tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the ISR effort. Technical channels include but are not limited to defining, managing, or guiding the use of specific ISR assets; identifying critical technical collection criteria such as technical indicators; recommending collection techniques, procedures, or assets; coordinating operations; and directing specialized training for specific MI personnel or units.

Note. In specific cases regulatory authority is granted to specific national and DOD intelligence agencies for specific intelligence discipline collection and is passed through technical channels.

- ***Conduct Deconfliction and Coordination.*** Deconfliction and coordination consists of a series of related activities that facilitate operations in another unit's AO. These activities facilitate successful ISR collection, support of the mission, and fratricide avoidance. Military intelligence organizations may be used in general support for coverage of an AO or in DS to support a specific unit. Military intelligence organizations operating in general support should coordinate with unit commanders when operating in that unit's AO. At a minimum, the MI organizations announce their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission. An MI organization operating in DS of a specific unit coordinates with the unit for augmentation to conduct operations in accordance with FP requirements. The MI organization's leader also coordinates with the supported unit's S-2 for debriefings of returning members, convoy leaders, and others.

Support Sensitive Site Exploitation

1-62. SSE consists of a related series of activities inside a captured sensitive site to exploit personnel, documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents. A sensitive site is a designated, geographically limited area with special diplomatic, informational, military, and economic sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money laundering areas, and document storage areas for secret police forces. These activities exploit personnel, documents, electronic data, and material captured at the site while neutralizing any threat posed by the site or its contents. While the physical process of exploiting the sensitive site begins at the site itself, full exploitation may involve teams of experts located around the world.

Intelligence Support to Personnel Recovery

1-63. Support to personnel recovery consists of intelligence activities and capabilities focused on collecting information to recover and return own personnel—whether Soldier, Army civilian, selected DOD contractors, or other personnel as determined by the Secretary of Defense—who are isolated, missing, detained, or captured in an operational environment. This support also includes detailed analysis, developing detailed products, and estimates to support operations undertaken to recover isolated, missing, detained, or captured personnel.

SUPPORT TO TARGETING AND INFORMATION SUPERIORITY

1-64. Intelligence support to targeting and information superiority is the task of providing the commander information and intelligence support for targeting through lethal and nonlethal actions. It includes intelligence support to the planning and execution of direct and indirect fires, command and control engagement, information engagement, and individual capabilities of information operations as well as assessing the effects of those operations.

Provide Intelligence Support to Targeting

1-65. The intelligence officer (supported by the entire staff) provides the fire support coordinator, information engagement officer, electronic warfare (EW) officer, and the information operations officer with information and intelligence for targeting the threat's forces and systems with direct and indirect lethal and nonlethal fires. It includes identification of threat capabilities and limitations. The targeting process uses the decide, detect, deliver, and assess (D3A) methodology. The intelligence officer ensures the ISR plan supports the finalized targeting plan. This task has two subtasks:

- ***Provide Intelligence Support to Target Development.*** The systematic analysis of threat forces and operations to determine high-value targets (HVTs) (people, organizations or military units), high-payoff targets (HPTs) (people, organizations or military units), and systems and system components for potential attack through maneuver, fires, electronic means, or information engagement or operations.
- ***Provide Intelligence Support to Target Detection.*** The intelligence officer establishes procedures for dissemination of targeting information. The targeting team develops the sensor and attack guidance matrix to determine the sensor required to detect and locate targets. The intelligence officer places these requirements into the ISR synchronization plan for later incorporation into the ISR plan.

Provide Intelligence Support to Information Superiority

1-66. Intelligence support to targeting and information superiority is the task of providing the commander information and intelligence support for targeting through lethal and nonlethal actions. It includes intelligence support to the planning and execution of direct and indirect fires, command and control engagement, information engagement, and individual capabilities of information operations as well as assessing the effects of those operations. Key activities reflected in this task include communications, planning, synchronization, and integration of intelligence into OPLANs and OPORDs. This task has five subtasks:

- **Provide Intelligence Support to Information Engagement.** The intelligence warfighting function when operating outside US territories supports activities related to information engagement under some circumstances. This subtask has two subtasks:
  - ***Provide Intelligence Support to Public Affair.*** This task enables MI organizations to collect and provide information and intelligence products concerning civil considerations in the operational environment in support of public affairs (PA) activities.
  - ***Provide Intelligence Support to Psychological Operations.*** Psychological operations (PSYOP) require information and intelligence to support analysis of foreign target audiences and their environment to include the PMESII-PT factors. Continuous and timely intelligence are required to assess target audience behavioral trends. Information and intelligence are centered on target audience motivation and behavior; the analysis of collected impact indicators; and the target audience's reaction to friendly, hostile, and neutral force actions.
- **Provide Intelligence Support to Command and Control Warfare.** The intelligence warfighting function supports command and control warfare by providing information to identify threat decision making and command and control nodes, processes, and means by order of criticality. Intelligence also helps identify threat systems, activities, and procedures that may

be vulnerable to command and control warfare. Additionally, intelligence plays a key role in evaluating and assessing the effectiveness of command and control warfare.

Note. This task supports electronic attack (EA) employing jamming, electromagnetic energy, or directed energy against personnel, facilities, or equipment. It identifies critical threat information systems and command and control nodes.

- **Provide Intelligence Support to Information Protection.** The intelligence warfighting function supports information protection by providing information to identify threat offensive information operations capabilities and activities and tactics, techniques, and procedures (TTP). Intelligence provides information relating to computer network defense, physical security, OPSEC, counterdeception, and counterpropaganda.
- **Provide Intelligence Support to Operations Security.** This task identifies capabilities and limitations of the threat's intelligence system including adversary intelligence objectives and means, procedures, and facilities to collect, process, and analyze information. This task supports the identification of indicators that adversary intelligence capabilities and systems might obtain that could be interpreted or pieced together to obtain essential elements of friendly information in time to be useful to adversaries.
- **Provide Intelligence Support to Military Deception.** This task identifies capabilities and limitations of the threat's intelligence-collecting capabilities, systems, and means and identifies threat biases and perceptions.

Provide Intelligence Support to Combat Assessment

1-67. Intelligence supports the assess phase of the operations process and targeting methodology. The commander uses combat assessment to determine if targeting actions have met the attack guidance and if reattack is necessary to perform essential fires tasks and achieve the commander's intent for fires. The staff determines how combat assessment relates to specific targets by completing battle damage, physical damage, functional damage, and target system assessments. This task has two subtasks:

- **Conduct Physical Damage Assessment.** This is a staff task that estimates the extent of physical damage to a target based on observed or interpreted damage. It is a post-attack target analysis that is a coordinated effort among all units.
- **Conduct Functional Damage Assessment.** The staff conducts the functional damage assessment for the remaining functional or operational capability of the threat. The assessment focuses on measurable effects and estimates the threat's ability to reorganize or find alternative means to continue operations. The targeting cell and staff integrate analysis with external sources to determine if the commander's intent for fires has been met.

CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

1-68. The effectiveness of the intelligence warfighting function is measured against the relevant information quality criteria:

- **Accuracy.** Intelligence must give commanders an accurate, balanced, complete, and objective picture of the enemy and 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 bias-free intelligence.
- **Timeliness.** Intelligence must be provided early enough to support operations, and prevent surprise from enemy action. 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 presented in a form that is easily understood or displayed in a format that immediately conveys the meaning to the consumer.
- **Completeness.** Intelligence briefings and products must convey all the necessary components to be as complete as possible.
- **Precision.** Intelligence briefings and products must provide the required level of detail to answer the requirements, no more and no less.
- **Reliability.** Intelligence must be evaluated to determine the extent to which the information that has been collected and is being used in intelligence briefings and products is trustworthy, uncorrupted, and undistorted. If there are any concerns with these, they must be stated up front.

1-69. Intelligence requires three additional criteria in order to be effective:

- **Relevant.** Intelligence must support the commander's concept of the operation and the unit's mission. It must be relevant to the capabilities of the unit, the CCIRs, and the commander's preferences.
- **Predictive.** Intelligence should inform the commander about what the enemy can do (most dangerous COA), and is most likely expected to do (most likely enemy COA). The intelligence warfighting function should anticipate the intelligence needs of the commander.
- **Tailored.** Intelligence must be presented based on the needs of the commanders, subordinate commanders, and staff in a specific format that is clear and concise so they can understand it, believe it, and act on it. It should support and satisfy the priorities of the commander.

ACTIONABLE INTELLIGENCE

1-70. Actionable intelligence is an example of bringing the characteristics of effective intelligence together with the effective integration of intelligence into ongoing operations to support the commander. Joint doctrine discusses the concept of critical intelligence. (See JP 2-0.) Army personnel have used the concept of actionable intelligence to reflect the Joint concept of critical intelligence. In the current operational environment, the concept of actionable intelligence is used by Army personnel to describe information that answers operational requirements or specific commander's guidance in the attack guidance matrix to sufficient degree and with sufficient reliability to support the commander's targeting decisions.

1-71. Ideally, the staff thoroughly integrates intelligence into the operations process for all operations to ensure the collection and reporting of timely, relevant, accurate, predictive, and tailored information and intelligence. This is accomplished by using the characteristics of effective intelligence as well as conducting successful ISR operations through detailed ISR synchronization and integration so that commanders can fight the threat through knowledge rather than assumption.

THE INTELLIGENCE PROCESS

1-72. Intelligence operations are executed by performing five steps that constitute the intelligence process: generate intelligence knowledge, plan, prepare, collect, and produce. Additionally, there are three activities that occur across the five steps of the intelligence process: analyze, assess, and propagate. The three continuing activities plus the commander's input drive, shape, and develop the process; they can occur at any time during the process.

1-73. The intelligence process provides a common model with which to guide one's thoughts, discussions, plans, and assessments. The intelligence process generates information, products, and knowledge about the threat, terrain and weather, and civil considerations, which supports the commander and staff in the conduct of operations. Figure 1-1 shows the intelligence process.

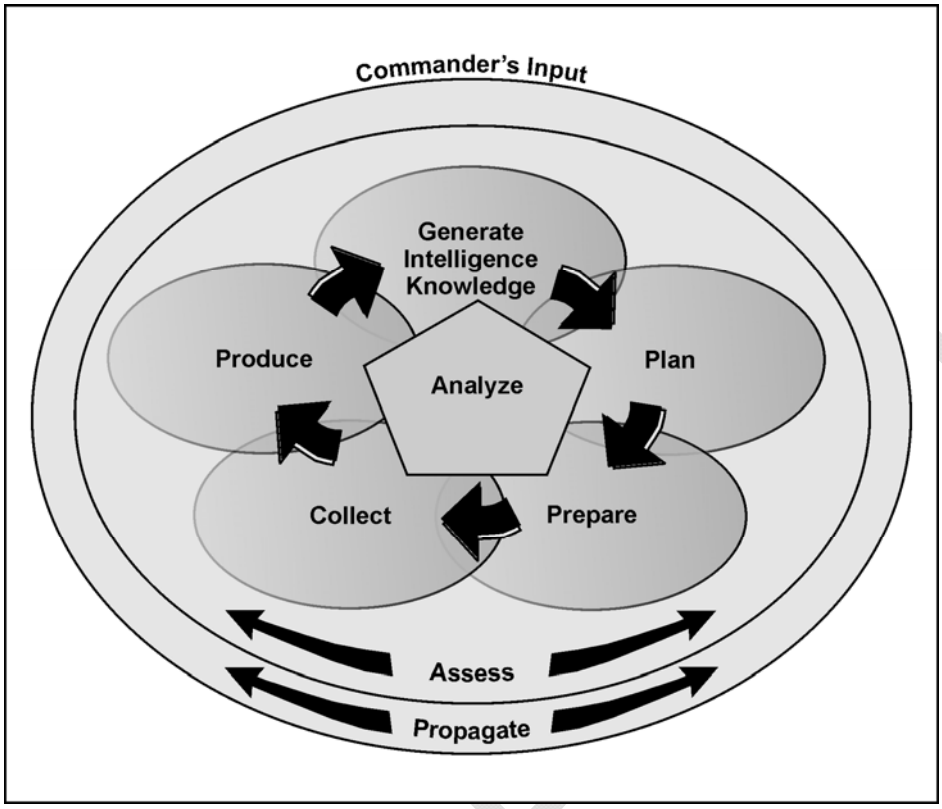


Figure 1-1. The intelligence process

GENERATE INTELLIGENCE KNOWLEDGE

1-74. Generate intelligence knowledge is a continuous and user-defined step driven by the commander that begins prior to mission receipt and provides the relevant knowledge required concerning the operational environment for the conduct operations. Generate intelligence knowledge begins as early as possible, in some cases when the commander knows only the general location or category of mission for a projected operation, and continues throughout the operations process. The unit determines what information it will need (based on the commander's guidance), what information it already has, and what information it needs to collect. For Army units, the initial step in locating the information they need to collect will be establishing an intelligence architecture that provides access to relevant intelligence community and other DOD databases and data files. When conducting the generate intelligence knowledge step, units and personnel must follow all applicable policies and regulations on the collection of information and OPSEC. Generate intelligence knowledge is an integral part of the intelligence process. (When published, refer to TC 2-33.401.)

Initial Database Development

1-75. The initial result of the generate intelligence knowledge step is the creation and population of data files as directed by the commander that are compatible with the unit's battle command systems. When generating intelligence knowledge, unit intelligence personnel should begin by determining what information they need to collect based on the primary components of the operational environment for which the intelligence staff is responsible in order to support the command, IPB, and answer the CCIRs.

1-76. As units begin to collect data on the projected AO, the data should be organized into baseline data files per the commander's guidance. Generally, the tactical echelons create primary data files, based on the threat, terrain, weather, and civil considerations. Strategic and operational echelons create data files based on the commander's operational requirements. Information can be based on the joint system's perspective (PMESII), as well as the operational variables (PMESII-PT) to populate the baseline data files.

1-77. All-source analysts ensure that relevant information is incorporated into the common database and the unit webpage. This information becomes the basis for providing intelligence support for developing predeployment readiness training on the operational environment. This information is used to develop Soldier predeployment packages; it helps to identify the specific types of threats, threat equipment, and threat TTP and civil considerations that Soldiers can expect to encounter when deployed. This information can be used to incorporate simulations or replications of items such as threat vehicles, weapons, and uniforms as well as threat TTP—along with civil considerations in the AO—into predeployment training exercises or mission rehearsal exercises to provide the most realistic and relevant training possible.

1-78. As with IPB, generate intelligence knowledge is a continuous process. Many factors can drive the requirement to update the baseline knowledge. This can include current operations, higher operations, intelligence analysis or assessments, and additional considerations. Additional considerations include such factors as updates based on local elections or key local leadership personnel changes, changes to local infrastructure, and events outside the unit's projected AO that may impact operations within the projected AO.

1-79. After creating the data files the data, information, intelligence, products, and material obtained are organized and refined to support planning. Generate intelligence knowledge is the precursor for conducting IPB and mission analysis. Generate intelligence knowledge is also the basis for developing a unit's initial intelligence survey. (When published, see TC 2-33.401 and FM 3-0.2) The generate intelligence knowledge process continues to gather, categorize, and analyze information on relevant aspects of the projected AO, continually adding new information and updating and refining the understanding of the projected AO throughout the operations process.

1-80. During a deployment, a unit's information databases become a source of information for the generate intelligence knowledge step of follow-on units (in support of Army Force Generation [ARFORGEN]) that may replace them. During and after deployment, the generate intelligence knowledge step also supports tactical overwatch and the collection of lessons learned.

Intelligence Survey

1-81. The intelligence survey is a process that assists the G-2/S-2 in identifying ISR asset collection capabilities and limitations within the projected AO for potential employment. The intelligence survey consists of five steps:

- Develop a comprehensive information baseline, collection capability baseline, and analytical baseline for the projected AO.
- Determine key intelligence gaps.
- Determine key gaps in analytical ability.
- Develop an understanding of the information and intelligence that can be collected with unit intelligence assets and, when appropriate, ISR assets in the projected AO and how and where it may best be collected.
- Determine a method of understanding when changes to the information baseline, collection capability baseline, or analytical baseline occur that are of intelligence interest.

1-82. The intelligence survey, which is developed over time and is continuously updated, provides the unit intelligence officer with an initial assessment for recommending intelligence asset apportionment within the projected AO and how best to use the unit's intelligence assets within the projected AO, taking into account technical and tactical considerations across all disciplines. For example, one portion of the projected AO may be unsuited for unit SIGINT asset collection due to terrain or lack of threat transmitters,

but it may be well-suited for HUMINT collection teams (HCTs). The intelligence officer may recommend to the commander that unit SIGINT collection assets not be deployed to that area, but that additional HCTs would be a valuable source of intelligence collection in that same area.

1-83. This assessment includes determining what nonstandard ISR assets, to include quick reaction capabilities and off-the-shelf capabilities and systems, are available to support the commander. Additionally, when reviewing contingency plans (CONPLANs) and operations plans (OPLANs), the G-2/S-2 should use the intelligence survey to update the CONPLAN or OPLAN based on new technologies, capabilities, or sources of information and intelligence.

1-84. The intelligence survey also assists in determining what communications will be required for deployed intelligence operations and addresses any apparent gaps in intelligence standing operating procedures (SOPs). Additionally, the intelligence survey is the basis for determining what additional or specialized intelligence assets the unit may require for mission accomplishment.

PLAN

1-85. The plan task consists of the activities that identify pertinent information requirements and develop the means for satisfying those requirements. The CCIRs (PIRs and FFIRs) drive the ISR effort. The intelligence officer synchronizes ISR operations and supports the G-3/S-3 in ISR integration. Planning activities include, but are not limited to—

- Conducting IPB and preparing IPB products and overlays.
- Developing initial PIRs.
- Developing the ISR synchronization plan, overlays, and matrices.
- Developing the initial running intelligence estimates or briefings (usually as part of the Mission Analysis Briefing), which should include initial PIRs as well as threat strengths and vulnerabilities that friendly forces should avoid or exploit.
- Managing requirements.
- Submitting RFIs and using intelligence reach to fill information gaps.
- Evaluating reported information.
- Establishing the intelligence communications and dissemination architecture.
- Developing, managing, and revising the ISR synchronization plan and the ISR plan as mission requirements change.
- Supporting the preparation of annex B (Intelligence), and assisting the S-3 in completing annex L (ISR).

PREPARE

1-86. Preparation is the key to successful intelligence analysis and collection. Intelligence analysts must use the previous steps to prepare products for the commander and staff for orders production and the conduct of operations. Failure to properly prepare for intelligence collection and the publication of finished intelligence products can cause an operation to be focused on an entirely wrong location, force, or objective. Thorough preparation by the staff allows the commander to focus the unit's power to achieve mission success. The prepare step includes those staff and leader activities which take place upon receiving the operations order (OPORD), OPLAN, warning order (WARNO), or commander's intent in order to improve the unit's ability to execute tasks or missions.

COLLECT

1-87. The collect task involves collecting, processing, and reporting information in response to ISR tasks. ISR assets collect information and data about the threat, terrain and weather, and civil considerations for a particular AO and AOI. A successful ISR effort results in the timely collection and reporting of relevant and accurate information which supports the commander's situational understanding.

1-88. This collected information forms the foundation of intelligence databases, intelligence production, and the situational awareness of the G-2/S-2. The requirements manager evaluates the reported information for its responsiveness to the CCIRs (PIRs and FFIRs).

Process

1-89. Once information has been collected, it is processed. Processing involves converting, evaluating, analyzing, interpreting, and synthesizing raw collected data and information into a format which enables the analysts to extract essential information to produce intelligence and targeting data. Examples of processing include preparing imagery for exploitation, enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized reporting format (to include a database format) that can be analyzed by a system operator, and correlating information.

1-90. Processing data and information is performed unilaterally and cooperatively by both humans (cognitive) and automated systems. Information or intelligence that is relevant to the current situation is converted into the appropriate format for inclusion in the common operational picture (COP).

Reporting

1-91. The timely and accurate reporting of combat information and intelligence is critical to successful operations. Information and intelligence is delivered as voice, text, graphic, or digital media. Voice data is reported over tactical radios on the command net or operations and intelligence net. Text, graphic, and other digital media are reported over the battle command network by system to include DCGS-A and deposited in the common database, email accounts, and on the unit's webpage.

PRODUCE

1-92. The produce task involves combining analyzed information and intelligence from single or multiple sources into intelligence or intelligence products in support of known or anticipated requirements. Production also involves combining new information and intelligence with existing intelligence in order to produce intelligence in a form that the commander and staff can apply to the military decision-making process (MDMP) and that supports and helps facilitate situational understanding. During the produce task, the intelligence staff exploits information by—

- Analyzing the information to isolate significant elements.
- Evaluating the information to determine accuracy, timeliness, usability, completeness, precision, and reliability. It must also be evaluated to determine if it is relevant, predictive, and properly tailored.
- Combining the information with other relevant information and previously developed intelligence.
- Applying the information to estimate possible outcomes.
- Presenting the information in a format that will be most useful to its user.

1-93. The intelligence staff deals with numerous and varied production requirements based on PIRs and intelligence requirements; diverse missions, environments, and situations; and user format requirements. Through analysis, collaboration, and intelligence reach, the G-2/S-2 and the staff use the collective intelligence production capability of higher, lateral, and subordinate echelons to meet the production requirements. Proficiency in these techniques and procedures facilitates the intelligence staff's ability to answer command and staff requirements regardless of the factors of METT-TC.

CONTINUING ACTIVITIES

1-94. The three continuing activities discussed below drive, shape, and develop the process; they can occur at any time during the process.

ANALYZE

1-95. *Analysis is the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat, terrain and weather, and civil considerations on operations* (FM 2-33.4). The intelligence staff analyzes intelligence and information about the threat's capabilities, friendly vulnerabilities, and the AO to determine how they will impact operations. The intelligence staff must also analyze and identify issues and problems that occur while conducting the unit's intelligence process. One example of this could be focusing on the wrong priority or assets that are inadequately placed to collect required information.

1-96. This analysis enables the commander and staff to determine the appropriate action or reaction and to focus or redirect assets and resources to fill information gaps, mitigate collection limitations, or alleviate pitfalls.

Critical Thinking

1-97. Critical thinking is an essential element of the analytical thought process and is necessary for adaptation to new developments in the ever-changing combat environment. Rapid and constant changes in society and the uncertainties of future operations cause the military to realize the importance of critical thinking skills training

1-98. *Critical thinking is the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information obtained from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action* (FM 2-33.4). In its exemplary form, it is based on universal intellectual values that transcend subject matter divisions: clarity, accuracy, precision, consistency, relevance, sound evidence, good reasons, depth, breadth, and fairness.

1-99. Critical thinking involves improving the quality of thinking by applying the scientific elements of reasoning to gather, evaluate, and use information effectively. It consists of mental processes of discernment, analysis, and evaluation. It includes possible processes of reflecting upon a tangible or intangible item in order to form a solid judgment that reconciles scientific evidence with common sense. Hence, critical thinking is self-directed, self-disciplined, self-monitored, and self-corrective thinking. It requires effective communication, problem-solving abilities, and continuous evaluation.

1-100. Critical thinking entails the examination of those structures or elements of thought implicit in all reasoning: purpose problem or question-at-issue, assumptions, concepts, empirical grounding, reasoning leading to conclusions, implications and consequences, objections from alternative viewpoints, and frame of reference. Critical thinking—in being responsible to variable subject matter, issues, and purposes—is incorporated in a family of interwoven modes of thinking, among them: scientific thinking, mathematical thinking, historical thinking, anthropological thinking, economic thinking, moral thinking, and philosophical thinking.

1-101. The following are characteristics of a Critical Thinker:

- **Fair-minded.** Neutral in appraising or applying counter-theories to opinions of others.
- **Honest.** Must know and acknowledge personal biases and opinions.
- **Reasonable.** Applies checks and balances to a hypothesis to ensure it is possible.
- **Systematic.** Applies a methodical process to present ideas or concepts in a logical manner.
- **Precise.** Possesses the highest standard of accuracy.
- **Persistent.** Stays the course; does not stop at the obvious; digs deeper to overcome initial conclusions, satisfied only when the hypothesis is fully developed.
- **Focused.** Not easily swayed or distracted by emotions; maintains a point of concentration.
- **Questioning.** Not satisfied with the obvious; eager to seek out additional information and data when none is immediately apparent.

- **Open-minded.** Willing to consider new or different ideas and modify the conclusions based upon new data or ideas even when they disagree with others.

CIVIL CONSIDERATIONS AND CULTURAL AWARENESS

1-102. Civil considerations comprise six characteristics expressed in the memory aid ASCOPE. Depending on the echelon conducting operations, these factors may be expressed using the joint systems perspective, the operational variables, and the mission variables. Additionally, the human terrain analysis team can provide detailed information and analysis pertaining to the socio-cultural factors involved in the operation.

Note. For additional information on ASCOPE and the IPB process, see FM 2-01.3. Also refer to the operational variables (PMESII-PT) discussed in paragraph 1-2.

1-103. A key component that describes the people is cultural awareness. 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. Each group to which individuals belong influences their beliefs, values, attitudes, and perceptions. As such, culture is internalized in the sense that it is habitual, taken for granted, and perceived as natural by people in the society.

1-104. Culture conditions an individual'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. Culture also includes the circumstances under which rules shift and change. Culture influences how people make judgments about what is right and wrong, assess what is important and unimportant, categorize things, and deal with things that do not fit into existing categories. Culture provides the framework for rational thought and decisions. What one culture considers rational may not be rational in another culture.

1-105. Understanding other cultures applies to full spectrum operations, not just those dominated by stability. For example, different tactics may be used against an adversary who considers surrender a dishonor worse than death, as compared to those for whom surrender remains an honorable option. Cultural understanding is 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 that of the HN. To operate successfully in multinational settings, Army leaders must recognize any differences in doctrinal terminology as well as the interpretation of orders and instructions. They must learn how and why others think and act as they do.

ASSESS

1-106. Assess plays a critical role in evaluating the information collected during the intelligence process. The continual assessment of ISR operations, available information and intelligence, and various aspects of the factors of METT-TC are critical to ensure that the intelligence staff:

- Answers the CCIRs.
- Provides the operations staff with input to redirect ISR assets in support of changing requirements.
- The effective use of information and intelligence.

PROPAGATE

1-107. Propagate includes direct dissemination; granting access to databases, information, or intelligence; and sharing. It also encompasses posting information to the web, intelligence reach, and updating the COP.

Dissemination

1-108. Dissemination is the act of getting relevant information to the right person at the right time. Dissemination entails delivering timely, relevant, accurate, predictive, and tailored intelligence to the commander. Determining the product format and selecting the means to deliver it are key aspects of dissemination.

1-109. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, the time allocated, and the individual preference of the commander all influence the information format. The DCGS-A enterprise provides a common backbone for the dissemination of intelligence. Answers to CCIRs for the commander, subordinate commanders, and staff require direct dissemination.

Granting Access

1-110. Granting access to databases, information, or intelligence ensures that personnel, units, or organizations that need all or part of the information in established classified and unclassified databases, programs, networks, systems, and other web-based collaborative environments for National Agency, Multinational, Joint, and Army organizations or echelons receive the appropriate access. This is accomplished through applicable National Agencies, Multinational, Joint, and Army regulations, policies, and procedures for personnel accesses and clearances; individual system accreditation; specialized training for clearances and systems or database usage; and special security procedures and enforcement.

Sharing

1-111. Sharing is primarily the result of establishing a web-based collaborative environment. Collaboration is the sharing of knowledge, expertise, and information normally online. Collaboration may take numerous forms. Collaborative tools are computer-based tools (groupware) that help individuals work together and share information. They allow for virtual online meetings and data sharing. Sharing allows analysts, other intelligence personnel, and other subject matter experts to freely exchange information and intelligence in support of answering their commander's requirements.

Posting

1-112. Information may be posted to the web for the widest possible dissemination. This makes the information available to personnel and units interested in the information or intelligence which is not part of the normal dissemination group for a specific unit or organization. When posting information to the web or updating information on their website, it is critical that units or organizations inform higher, subordinate, and lateral units or organizations that may require this information since units rarely have enough personnel to dedicate a Soldier to continuously search websites for new or updated information that may be of use to that unit or organization.

Intelligence Reach

1-113. Intelligence reach is an important part of the intelligence effort. Intelligence reach allows intelligence analysts to retrieve existing information, intelligence products, and data which can support answering the CCIRs from outside the unit in a timely manner without having to wait for an answer to an RFI or an ISR task. The information, intelligence products, or data retrieved can then be evaluated for use in the unit's intelligence products or analysis.

Updating the COP

1-114. As required by unit SOPs, new or updated intelligence information must be regularly inputted in the COP to provide the most current picture. The COP is a single display of all relevant information conveyed through reports, automatic updates, and overlays common to all echelons and digitally stored in a

common database. It facilitates battle command through collaborative interaction and real-time sharing of information between commanders and staffs. The intelligence portions of the COP are those messages and overlays relating to threat, terrain and weather, and civil considerations sent to the common database from intelligence organizations at various echelons and combat information transmitted from individual Soldiers and platforms. The G-2/S-2 monitors the common database to ensure it reflects the most current information and intelligence available.

COMMANDER'S INPUT

1-115. While commander's input is a commander's responsibility to drive the intelligence process, it is not a part of the intelligence process itself. Commander's input provides the primary mechanism for the commander to focus the intelligence warfighting function and is provided at the commander's discretion. Through the assess continuing activity, the intelligence staff is triggered to consult the commander to gain the commander's input The commander's input directly influences the unit's ISR effort. Each commander determines which intelligence products are developed as well as the format of the products. The commander may provide input at any point during the intelligence process, and the intelligence effort will have to be adjusted accordingly.

ARMY INTELLIGENCE ENTERPRISE

1-116. Within the framework of the intelligence warfighting function, the intelligence tasks and the intelligence process, intelligence personnel further focus on conducting intelligence from a fundamental enterprise perspective.

1-117. The Army intelligence enterprise is the sum total of the networked and federated systems, and efforts of the military intelligence personnel (to include collectors and analysts), sensors, organizations, information, and processes that allow the focus necessary to use the power of the entire intelligence community.

1-118. The purpose of the Army intelligence enterprise is to provide technical support and guidance as well as an information and intelligence architecture that efficiently and effectively synchronize ISR operations and intelligence analysis and production to drive intelligence production in support of the commander's situational awareness. Figure 1-2 shows an example of the tactical portion of the Army intelligence enterprise.

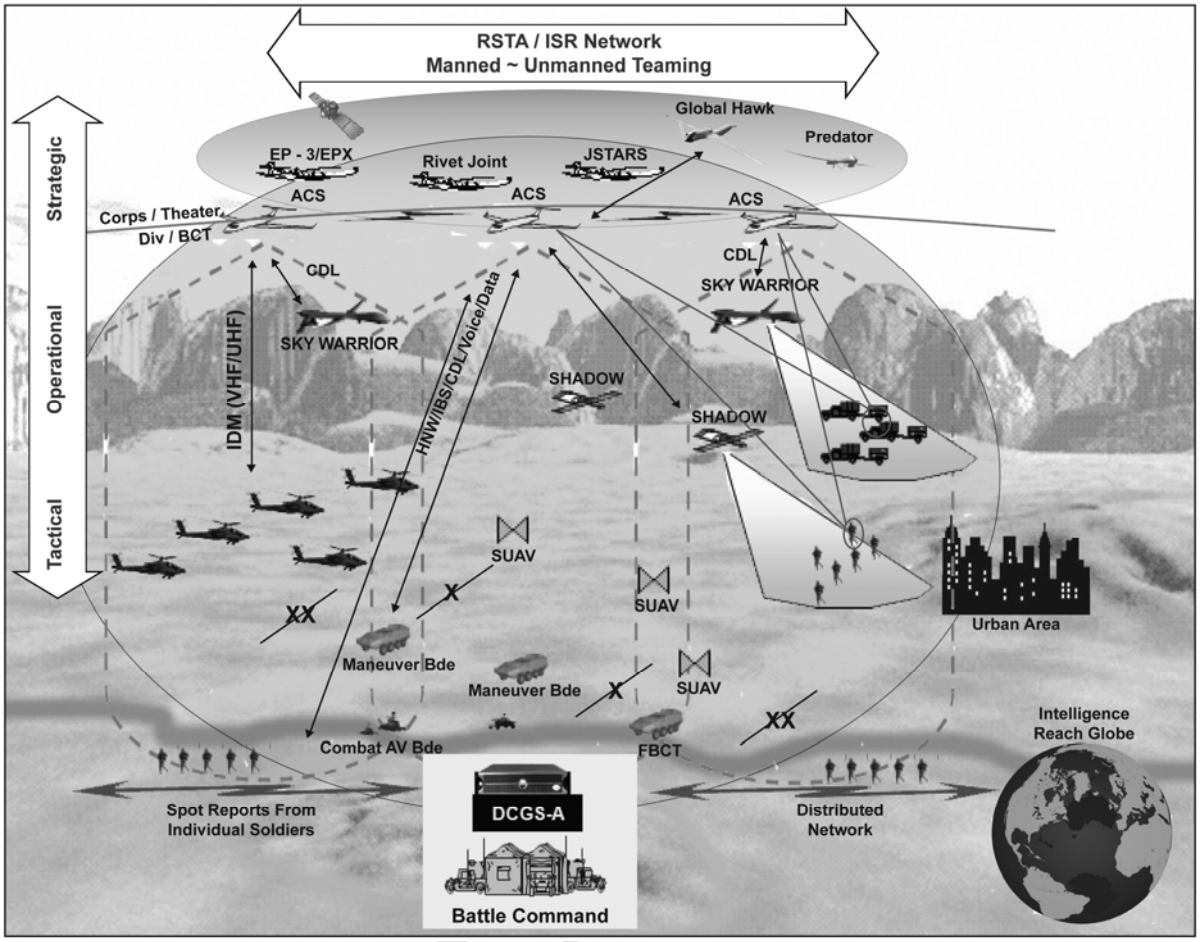


Figure 1-2. Example of the tactical portion of the Army intelligence enterprise

INTELLIGENCE DISCIPLINES

1-119. Intelligence is further broken down into disciplines. Each discipline applies unique aspects of support and guidance called technical channels.

1-120. The Army's intelligence disciplines are all-source intelligence, counterintelligence (CI), HUMINT, geospatial intelligence (GEOINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT) , OSINT, SIGINT, and technical intelligence (TECHINT). For more information regarding the intelligence disciplines, see Part Three of this manual, as well as the respective manuals, which covers each intelligence discipline.

ALL-SOURCE INTELLIGENCE

1-121. All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including OSINT, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the step used to produce intelligence from multiple intelligence or information sources. See chapter 5 for more information on all-source intelligence.

COUNTERINTELLIGENCE

1-122. CI counters or neutralizes adversarial, foreign intelligence services, and terrorists (AFIST) intelligence collection efforts through collection, CI investigations, operations, analysis, production, and functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; it is the key intelligence community contributor to protect US interests and equities. CI assists in identifying essential elements of friendly information, identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against US forces. See chapter 6 for more information on CI.

HUMAN INTELLIGENCE

1-123. HUMINT is the collection of foreign information—by a trained HUMINT collector—from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both passively and actively, to collect information. See chapter 7 for more information on HUMINT.

GEOSPATIAL INTELLIGENCE

1-124. Title 10 US Code § 467 establishes GEOINT. National Geospatial-Intelligence Agency (NGA) defines GEOINT as "the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, imagery intelligence, and geospatial information."

1-125. The Army implementation of GEOINT is a result of the Army's organization, manning, and training. There are multiple types of data and information that various Army units and organizations collect, provide, and analyze in order to support the GEOINT enterprise. The two primary GEOINT service providers in the Army are MI units and organizations and Engineer (topographic) units and organizations:

- MI units and organizations provide imagery and IMINT to the enterprise.
- Engineer (topographic) units and organizations provide geospatial data and information to the enterprise.
- Therefore, while some of the collection, analysis, and exploitation of imagery and geospatial information occur within the intelligence warfighting function; some of the collection, analysis, and exploitation of imagery and geospatial information occur outside the realm of intelligence. See chapter 8 for more information on GEOINT.

1-126. The Army does not conduct GEOINT operations in isolation. GEOINT is comprised of many ongoing operations and activities across the DOD. The National System for Geospatial-Intelligence (NSG) manages operations through guidance, policy, programs, and organizations. The NSG is the combination of technology, policies, capabilities, doctrine, activities, people, data, and communities necessary to produce GEOINT in the form of integrated intelligence across multiple environments. The NSG community consists of members and partners:

- Members include the intelligence community, joint staff, military departments (to include the Services), and combatant commands.
- Partners include Civil Applications Committee members, international partners, industry, academia, Defense Service providers, and civil community service providers.

IMAGERY INTELLIGENCE

1-127. IMINT is intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multi-spectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. See chapter 9 for more information on IMINT.

MEASUREMENT AND SIGNATURE INTELLIGENCE

1-128. MASINT is technically derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from IMINT and SIGINT collection. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, radio frequency (RF), nuclear detection, and seismic sensors, as well as techniques for collecting CBRN, and other material samples. See chapter 10 for more information on MASINT.

OPEN -SOURCE INTELLIGENCE

1-129. The National Defense Authorization Act for Fiscal Year 2006 states:

> *Open source intelligence is 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.*

1-130. Expressed in terms of the Army intelligence process, OSINT is relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements.

1-131. The Army does not have a specific military occupational specialty (MOS), additional skill identifier (ASI), or special qualification identifier (SQI) for OSINT. With the exception of the Asian Studies Detachment, the Army does not have base tables of organization and equipment (TOE) for OSINT units or staff elements. OSINT missions and tasks are imbedded within existing missions and force structure or accomplished through task organization. See chapter 11 for more information on OSINT.

SIGNALS INTELLIGENCE

1-132. SIGINT is intelligence produced by exploiting foreign communication systems and noncommunications emitters. SIGINT provides unique intelligence and analysis information in a timely manner. The discipline is comprised of communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). See chapter 12 for more information on SIGINT.

TECHNICAL INTELLIGENCE

1-133. TECHINT is intelligence derived from the collection and analysis of threat and foreign military equipment and associated 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. See chapter 13 for more information on TECHINT.

EMERGING CAPABILITIES

1-134. Four emerging capabilities which are not intelligence-specific capabilities, but which will impact intelligence operations, are biometrics, DCGS-A, human terrain analysis teams, and document and media exploitation (DOMEX).

BIOMETRICS

1-135. A biometric is defined by JP 2-0 as a measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual. **Biometrics-enabled intelligence is defined as the intelligence information associated with biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist or insurgent networks and related pattern analysis; facilitates high-value individual targeting; reveals movement patterns; and confirm identities** (DOD Directive 8521).

1-136. Typical automated biometric systems are comprised of five integrated components:

- **Collection Device.** Hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.
- **Algorithms.** A sequence of instructions that tells a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a match exists between a biometric sample and a biometric template.
- **Database.** Used to store the information collected that will be used later to do matching against.
- **Decision Process.** Automated or human-assisted process or analysis that results in a decision by matching components and specific search criteria.
- **Dissemination Process.** Gets the data collected to whomever and wherever it needs to be in a timely manner.

1-137. The implementation of these five components leads to personal identification (PI) or the identification of an individual with certitude. This can be summarized into three stages:

- The sensor collects a biometric feature to include fingerprints, iris, or photographic image of face, or DNA.
- The system stores that feature in a mathematical template in a database.
- The processing device runs search on the template against a matching algorithm that compares it to templates already stored in the database.

1-138. Military commanders require the ability to link identity information to a given individual. Biometric systems are employed to deny threat forces freedom of movement within the populace and positively identify known threats. These systems gather biometric data such as iris scans, fingerprints, and photographic images and combine them with contextual data to produce an electronic dossier on the individual.

1-139. PI includes positively indentifying friendly, adversarial, non-adversarial forces. Intelligence-related functions that biometrics can support or enhance are—

- Intelligence analysis.
- Foreign national and local employee hires screening.
- Counterintelligence and force protection (FP).
- Interrogation and detention operations.
- HVT confirmation (including high-value individuals [HVIs] and killed in action).
- Base access and local security.
- Population control or census (screening, enrolling, and badging operations).

1-140. The capability to positively indentify an individual and to place that individual within a relevant context adds a level of certitude that significantly enhances the overall effectiveness of the mission. PI enabled by biometric technology can help to identify and locate specific individuals in support of targeting. This capability is necessary not only for FP and security missions but also when an operational capability is required to achieve an advantage over an enemy in conventional warfare, combating terrorism, forcible entry, strikes, raids, and operations with multinational partners.

1-141. Affixing an individual's identification using the person's unique physical features and linking this identity to the individual's past activities and previously used identities such as friendly forces' accesses, permissions, clearance status, medical information, and unique biometrically based identifiers, in addition to adversary or unknown persons. Ensuring access to all available information on an individual is critical to such functions as screening persons for access to vessels, position of trust, and the prosecution of criminals and terrorists. As biometric capabilities continue to develop and current operations change in nature, it is necessary to integrate the operational, intelligence, and communications aspects of biometrics systems into a cohesive concept of employment.

1-142. For more information on biometrics enabled intelligence, see TC 2-22,101 when published.

DISTRIBUTED COMMON GROUND SYSTEM-ARMY

1-143. DCGS-A provides a net-centric, enterprised ISR, weather, geospatial engineering, and space operations capability to maneuver, maneuver support, and maneuver sustainment support organizations at all echelons from the battalion to JTFs. DCGS-A will be the ISR component of the modular and future force Battle Command System and the Army's primary system for ISR tasking, posting, processing, and using information about the threat, terrain, weather, and civil considerations at all echelons.

1-144. DCGS-A provides the capabilities necessary for commanders to access information from all data sources and to synchronize sensors. DCGS-A provides continuous acquisition and synthesis of data and information from joint and interagency capabilities, multinational partners, and non-traditional sources that will permit forces to maintain an updated and accurate understanding of the operational environment. DCGS-A contributes to visualization and situational awareness, thereby enhancing tactical maneuver, maximizing combat power, and enhancing the ability to operate in an unpredictable and changing operational environment throughout full spectrum operations.

1-145. DCGS-A will facilitate the rapid conduct of operations and synchronization of all warfighting functions resulting in the ability to operate within the threat's decision cycle, as well as to shape the environment for successful operations. The core functions of DCGS-A are—

- Receipt and processing of select ISR sensor data.
- Control of select Army sensor systems.
- Facilitation of ISR synchronization.
- Facilitation of ISR integration.
- Fusion of sensor information.
- Direction and distribution of relevant threat.
- Facilitation of friendly and environmental (weather and terrain) information.

HUMAN TERRAIN ANALYSIS TEAMS

1-146. A headquarters may request a human terrain analysis team to assist with socio-cultural research and analysis. As part of building their situational understanding, commanders consider how culture (both their own and others within the AO) affects operations. Culture is examined as part of the mission variable civil considerations. Understanding the culture of a particular society or group within a society significantly improves the force's ability to accomplish the mission. Army leaders are mindful of cultural factors in three contexts:

- Sensitivity to the different backgrounds of team members to best leverage their talents.
- Awareness of the culture of the country in which the organization operates.
- Consideration of the possible implication of partners' customs, traditions, doctrinal principles, and operational methods when working with their forces.

1-147. Effective Army leaders understand and appreciate their own culture (individual, military, and national) in relationship to the various cultures of others in the AO. Just as culture shapes how other groups view themselves and the world around them, culture shapes how commanders, leaders, and Soldiers perceive the world. Effective commanders are aware that their individual perceptions greatly influence how they understand the situation and make decisions. Through reflection, dialog, engagement, and analysis of differences between their culture and that of the indigenous population, commanders expose and question their assumptions about situation. They seek to understand how enemies, partners, and the population view the situation.

DOCUMENT AND MEDIA EXPLOITATION IN MODERN MILITARY OPERATIONS

1-148. Modern military operations are conducted in volatile, complex, and ever-changing operational environments. It is essential for tactical military leaders to have access to accurate and timely information

when planning and conducting operations. Tactical, operational, and strategic leaders are enabled with accurate information about enemy forces through the rapid and accurate extraction, exploitation, and analysis of captured enemy documents (CEDs), media, and materiel.

1-149. DOMEX is the systematic extraction of information from all media in response to the commander's collection requirements. When conducted properly, DOMEX operations are intended to—

- Maximize the value of intelligence gained from captured enemy documents and media.
- Provide the commander with timely and relevant intelligence to effectively enhance awareness of the enemy's capabilities, operational structures, and intent.
- Provide timely and accurate intelligence support to the warfighter throughout the entire range of military operations.
- Assist in criminal prosecution or legal processes by maintaining chain of custody procedures and preserving the evidentiary value of captured materials.

1-150. As an integral part of today's operational environment, DOMEX is an increasingly specialized full-time mission requiring advanced automation and communications support, analytical support, and expert linguists. DOMEX and translation operations were once considered purely HUMINT processing activities directly associated with language capabilities and extensive background knowledge in area studies.

1-151. Current doctrinal thought acknowledges that HUMINT is no longer the sole asset capable of conducting DOMEX operations. Personnel involved in DOMEX do not require HUMINT training in order to screen or translate a document, particularly since the unit may better utilize its sparse HUMINT assets to conduct the HUMINT mission. DOMEX is an Armywide responsibility and while HUMINT assets may be utilized to perform the DOMEX mission when available, HUMINT is a consumer of DOMEX information, rather than the major provider.

1-152. For DOMEX products to be a force multiplier, the rapid exploitation of captured materials must occur at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and accurate intelligence support to the warfighter; not only does this enable the rapid exploitation and evacuation of captured materials, it also hastens the feedback commanders receive from the higher-echelon analysis of captured materials affecting operations.

1-153. The current methodology for intelligence dissemination sends reporting through an echeloned structure from national, to theater, to corps, to division, and so on, then back down through the same rigid structure. Recent military operations have shown that this methodology is not timely and seldom results in lower tactical echelons receiving intelligence critical to their AO. The intelligence staff must be prepared to use any form of communication to pass vital information.

1-154. Depending upon the tactical situation, available resources, and the CCIRs, PIRs, SIRs, critical pieces of information must be passed quickly to those who can use them; specifically, tactical commanders. Intelligence staffs are responsible for reporting and disseminating DOMEX-derived information in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

1-155. In today's operational environment, commanders and staff must determine how to task-organize their ISR units to best satisfy their information requirements. Additionally, commanders anticipating requirements their unit cannot satisfy must consider requesting specialized or uniquely trained units. Assigning these units to the requesting organization may be the best solution, but often specialized units are allocated to higher headquarters and are attached to requesting units based on availability and priority.

1-156. In addition to identifying information requirements and capable ISR units, planning to conduct DOMEX operations efficiently requires a synchronized concept of operations. Other than intelligence units, assigned intelligence personnel representation generally ends at the battalion echelon with the battalion intelligence staff. Battalion staffs must plan for DOMEX operations from their subordinate units. Two techniques to provide better intelligence below the battalion echelon are to task-organize intelligence

personnel as intelligence support teams to company or platoon echelon, or to train company or platoon personnel in specific handling, screening, and inventorying techniques.

1-157. Where tactical assets are insufficient, operational and strategic assets can be relied upon to support a unit's organic assets, either via personnel augmentation or via virtual or long-distance support to tactical operations from continental United States and outside continental United States DOMEX support elements worldwide.

1-158. The skills, knowledge, and equipment for specialized processing are available at intelligence community organizations through the communications architecture. Units can request the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Media Exploitation Center (NMEC), the National Ground Intelligence Center (NGIC), the Joint Document Exploitation Center (JDEC), and other US or multinational intelligence community organizations to 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.

Chapter 2

Intelligence Communities and Joint Considerations

2-1. *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 integrate joint, single-service, special, and supporting intelligence operations with interagency, nongovernmental, and multinational operations. Army Forces (ARFOR) often bring unique ISR capabilities to unified action.

2-2. This chapter discusses the synchronization of Army intelligence efforts with joint and other national and international partners to achieve unity of effort and to accomplish the commander's intent.

INTELLIGENCE COMMUNITY

2-3. There are many organizations in the intelligence community that support military operations by providing specific intelligence products and services. The J-2/G-2/S-2 and the staff must be familiar with these organizations and the methods of obtaining information from them as necessary. Figure 2-1 shows organizations that compose the intelligence community.

DOD AGENCIES

2-4. The DOD agencies are discussed below.

Defense Intelligence Agency

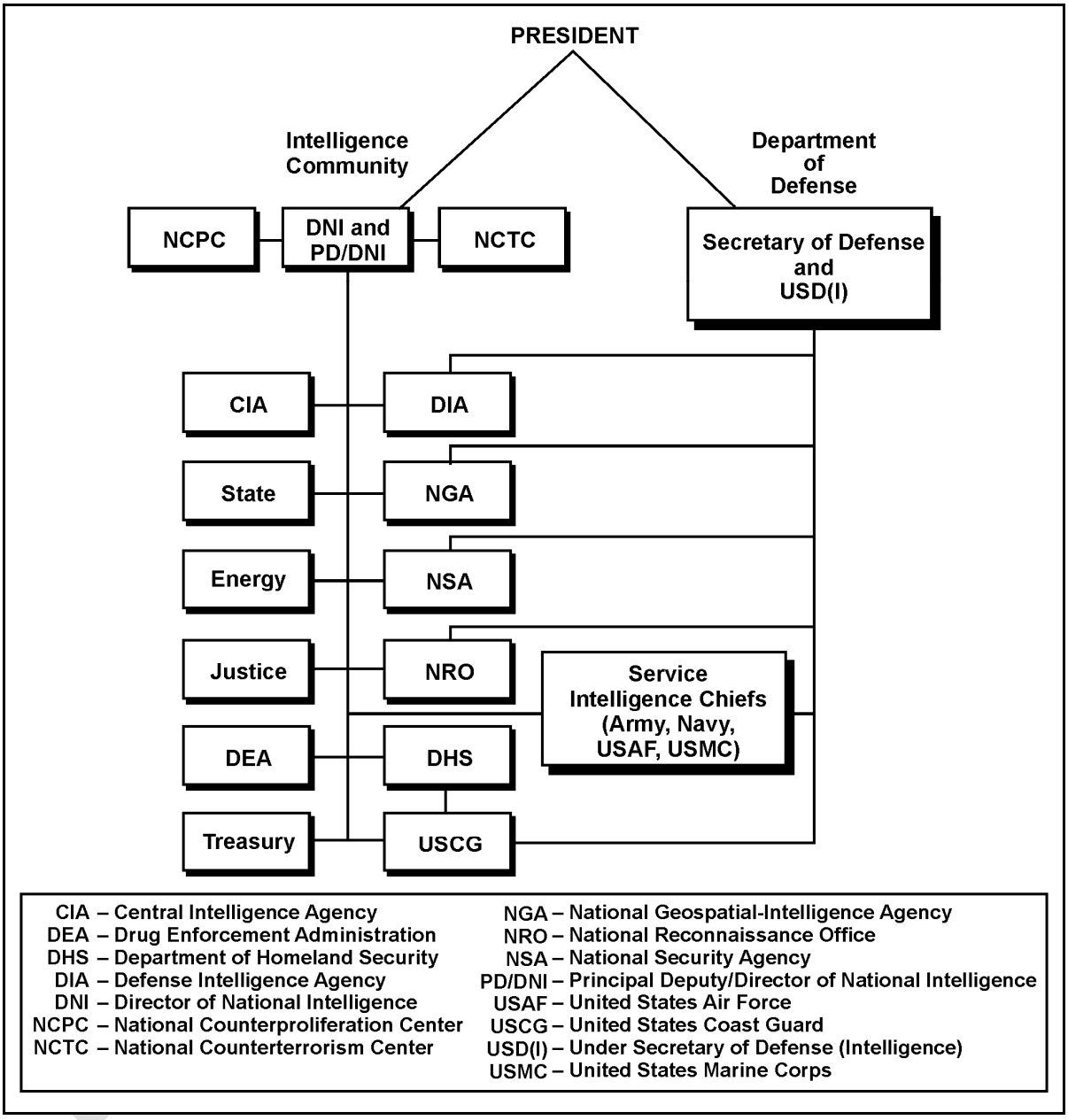
2-5. The Defense Intelligence Agency (DIA) has oversight of the Defense Intelligence Analysis Program and provides intelligence support in areas, such as all-source military analysis, human factors analysis, HUMINT, MASINT, Medical Intelligence, CI, counterterrorism, chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) counterproliferation, counterdrug operations, information operations, personnel recovery, peacekeeping and multinational support, noncombatant evacuation operations, I&W, targeting, battle damage assessment (BDA), current intelligence, systems analysis of the adversary, collection management, intelligence architecture and systems support, intelligence support to operation planning, defense critical infrastructure protection, and document and media exploitation (DOMEX).

National Security Agency/Central Security Service

2-6. The National Security Agency/Central Security Service is a unified organization structured to provide for the SIGINT mission of the US and to ensure the protection of national security systems for all departments and agencies of the US Government.

National Geospatial-Intelligence Agency

2-7. NGA provides timely, relevant, and accurate GEOINT support to include IMINT, GEOINT, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic data and information.



1631 **Figure 2-1. Intelligence community membership**

1632 **National Reconnaissance Office**

1633 2-8. The National Reconnaissance Office (NRO) is responsible for integrating unique and innovative
1634 space-based reconnaissance technologies, and the engineering, development, acquisition, and operation of
1635 space reconnaissance systems and related intelligence activities.

Joint Reserve Intelligence Centers

2-9. A Joint Reserve Intelligence Center (JRIC) is a joint intelligence production and training activity that uses information networks to link reservist intelligence personnel with the combatant commands and Services. A JRIC is located within a Service-owned and managed sensitive compartmented information facility (SCIF) and may also include surrounding collateral and unclassified areas involved in the performance and direct management of intelligence production work that uses Joint Reserve Intelligence Program infrastructure and connectivity. The more than 20 JRICs located around the country are equipped to effectively serve as satellite elements to combatant command JIOCs. JRICs are shared facilities that serve multiple customers and missions (JP 2-0).

US Army Intelligence

2-10. The Army Deputy Chief of Staff (DCS) for Intelligence exercises staff supervision over the US Army Intelligence and Security Command (INSCOM).

US Army Intelligence and Security Command

2-11. INSCOM, which includes the National Ground Intelligence Center, provides intelligence support to strategic and operational level commanders in the areas of IMINT, MASINT, SIGINT, operational and tactical HUMINT, CI, TECHINT, information operations, general military intelligence (GMI), and scientific and technical intelligence (S&TI). Other organizations include the Army Reserve Military Intelligence Readiness Command.

2-12. The US Army has vested its intelligence at the operational level with INSCOM, a direct reporting unit responsible for the Army's intelligence forces above corps. INSCOM's mission is to conduct and support intelligence, security, and information operations for military commanders and national decision makers. INSCOM goal is to provide superior information and information capabilities to Army commanders, while denying the same to adversaries. Headquarters, INSCOM, in coordination with its major subordinate commands (MSCs), provides a myriad of general intelligence support operations. INSCOM serves as the national to tactical intelligence conduit.

Army Space Program Office

2-13. The Army Space Program Office (ASPO) executes the Army's Tactical Exploitation of National Capabilities Program (TENCAP). The program focuses on exploiting current and future tactical potential of national systems and integrating the capabilities into the Army's tactical decision-making process. Army TENCAP systems enable the tactical commander maximum flexibility to satisfy intelligence needs under a wide range of operational scenarios. ASPO is the point of contact (POC) for all tactical activities between direct reporting units or users and the NRO.

US Navy Intelligence

2-14. The Director of Naval Intelligence exercises staff supervision over the Office of Naval Intelligence, which provides the intelligence necessary to plan, build, train, equip, and maintain US naval forces. The National Maritime Intelligence Center consists of Office of Naval Intelligence, the US Coast Guard Intelligence Coordination Center, the Navy Information Operations Command, and detachments of the Marine Corps Intelligence Activity and Naval Criminal Investigative Service.

US Air Force Intelligence

2-15. The Air Force DCS for Intelligence, Surveillance, and Reconnaissance is responsible for intelligence policy, planning, programming, evaluation, and resource allocation. The Air Force's main production facility is the National Air and Space Intelligence Center. Primary collection, analysis, and production units are organized under the Air Combat Command, the Air Force Warfare Center, and the Air Force Intelligence, Surveillance, and Reconnaissance Agency. Additionally, the Air Force Office of Special

Investigations is the Service's main focal point for CI activities. Additional information describing the Air Force approach to operational ISR employment is found in AFDD 2-9.

US Marine Corps Intelligence

2-16. The Director of Intelligence is the Commandant's principal intelligence staff officer and the functional manager for intelligence, CI, and cryptologic material. The Director exercises staff supervision of the Marine Corps Intelligence Activity, which provides tailored intelligence products to support Marine Corps operating forces, and serves as the fixed site of the Marine Corps Intelligence Surveillance and Reconnaissance Enterprise.

NONMILITARY MEMBERS OF THE INTELLIGENCE COMMUNITY

2-17. Joint operations require knowledge of both military and nonmilitary aspects of the operational environment. Much of this expertise falls outside the purview of the DOD members of the intelligence community. JFCs and their J-2's should be familiar with the roles and responsibilities of the following non-DOD members of the intelligence community.

Director of National Intelligence

2-18. The office of the Director of National Intelligence oversees the Intelligence Community organizations; leads the national intelligence effort.

Central Intelligence Agency

2-19. The Central Intelligence Agency's (CIA) primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political, economic, and biographic intelligence.

Department of State

2-20. The Department of State's Bureau of Intelligence and Research performs intelligence analysis and production on a wide range of political and economic topics essential to foreign policy determination and execution.

Department of Energy

2-21. The Department of Energy analyzes foreign information relevant to US energy policies and nonproliferation issues.

Federal Bureau of Investigation

2-22. The Federal Bureau of Investigation has primary responsibility for CI and CT operations conducted in the US. The Federal Bureau of Investigation shares law enforcement and CI information with appropriate DOD entities and combatant commands.

Department of the Treasury

2-23. The Department of the Treasury analyzes foreign intelligence related to economic policy and participates with the Department of State in the overt collection of general foreign economic information.

United States Coast Guard

2-24. The US Coast Guard operates as both a military service and a law enforcement organization and provides general maritime intelligence support to commanders from the strategic to tactical level in the areas of HUMINT, SIGINT, GEOINT, MASINT, OSINT, and CI.

Department of Homeland Security

2-25. The Directorate for Information Analysis and Infrastructure Protection analyzes the vulnerabilities of US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to the Homeland Security Advisory System.

Drug Enforcement Administration

2-26. The Office of National Security Intelligence collects and analyzes information related to illegal drug production, smuggling, and trafficking.

OTHER AGENCIES

2-27. There are a number of US Government agencies and organizations, not members of the intelligence community, that are responsible for collecting and maintaining information and statistics related to foreign governments and international affairs. Organizations such as the Library of Congress, the Departments of Agriculture and Commerce, the National Technical Information Center, and the US Patent Office are potential sources of specialized information on political, economic, and military-related topics. The intelligence community may draw on these organizations to support and enhance research and analysis and to provide relevant information and intelligence for commanders and planners.

2-28. Many other US Government agencies may become directly involved in supporting DOD especially during stability operations. (See JP 2-02 for a description of agency support to joint operations and intelligence.) These organizations include—

- Department of Transportation.
- Disaster Assistance Response Team within the Office of Foreign Disaster.
- US Agency for International Development.

THE LEVELS OF WAR

2-29. The levels of war are doctrinal perspectives that define and clarify the relationship between strategy, operational approach, and tactical actions. Although there are no finite limits or boundaries between them, the three levels of war are strategic, operational, and tactical (see figure 2-2).

- The strategic level is that level at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, and develops and uses national resources to achieve these objectives.
- The operational level links employing tactical forces to achieving the strategic end-state. At the operational level, commanders conduct campaigns and major operations to establish conditions that define that end-state.
- The tactical level is the employment and ordered arrangement of forces in relation to each other (CJCS Instruction 5120.02A). Through tactics, commanders use combat power to accomplish missions. The tactical level commander uses combat power in battles, engagements, and small-unit actions.

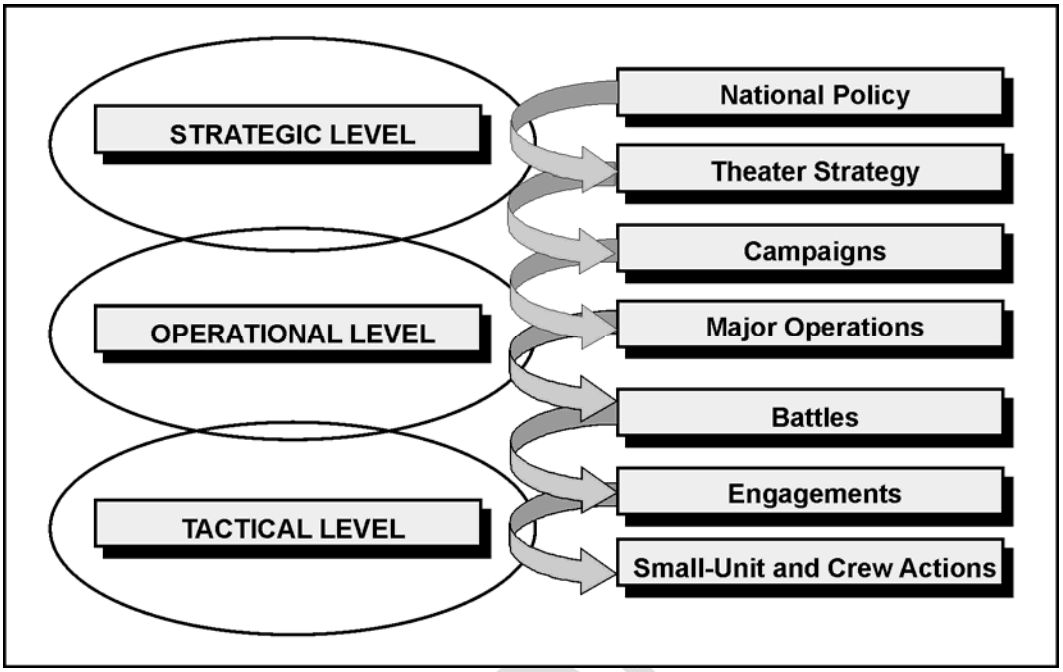


Figure 2-2. Levels of war

2-30. Understanding the interdependent relationship of all three levels of war helps commanders visualize a logical flow of operations, allocate resources, and assign tasks. Actions within the three levels are not associated with a particular command level, unit size, equipment type, or force or component type. The concept of strategic, operational, and tactical intelligence operations commanders and their intelligence officers in visualizing the flow of intelligence from one level to the next. The concept facilitates allocating required collection, analysis, production, and dissemination resources; and facilitates the assignment of appropriate intelligence tasks to national, combatant command, component, and supporting intelligence elements.

STRATEGIC

2-31. The President and the Secretary of Defense use strategic intelligence to develop national strategy and policy, monitor the international situation, prepare military plans, determine major weapon systems and force structure requirements, and conduct strategic operations

2-32. Intelligence supports joint operations across the full spectrum of military operations. It determines the current capabilities, and forecasts future developments, threats that could affect the national security and interests. During strategic operations, intelligence personnel also produce the intelligence required by CCDRs to prepare strategic estimates, strategies, and plans to accomplish missions assigned by higher authorities.

2-33. Combatant command intelligence includes determining when, where, and in what strength the threat will stage and conduct combatant command level campaigns and strategic unified operations. The intelligence staff should also focus predictive analysis efforts on identifying strategic threat events and how these events will impact US actions at the strategic, operational, and tactical levels. Intelligence operations support information operations as well. Intelligence operations support strategic planning by—

- Developing strategic intelligence policy.
- Preparing the strategic collection plan.

- Allocating national intelligence resources.

2-34. Collection on intelligence requirements can provide information which identifies indicators of threat actions or intent, thus reducing the uncertainties associated with an operation. Significant changes (that is, branches and sequels) during or to an operation usually lead to changes in intelligence requirements. Of particular importance is information relating to threat strategic vulnerabilities, strategic forces, strategic centers of gravity (COGs), and any capabilities relating to the development and employment of CBRNE weapons.

2-35. Global and regional issues and threats are identified and reported to the President and the Secretary of Defense, as well as to the senior military leadership and the CCDR. Intelligence requirements include any foreign developments that could threaten the US, its citizens abroad, or multinational military, political, or economic interests. Intelligence also includes identifying hostile reactions to US reconnaissance activities and indications and warnings (I&W) of impending terrorist attacks.

OPERATIONAL

2-36. CCDRs and subordinate JFCs and their component commanders are the primary users of operational intelligence. At the operational echelons, intelligence—

- Focuses on the military capabilities and intentions of threats.
- Provides analysis of events within the AOI and helps commanders determine when, where, and in what strength the adversary might stage and conduct campaigns and major operations.
- Supports all phases of military operations, from mobilization through general war to stable peace and all the way through redeployment of US forces. It continues during sustainment.
- Supports all aspects of the joint campaign.
- Identifies adversary COGs and HVTs.
- Provides critical support to friendly information tasks.

2-37. The JFC and staff allocate intelligence resources and request support from national agencies, other combatant commands, and multinational partners. During stability operations, operational intelligence includes training and assisting multinational partners in conducting intelligence operations.

2-38. CCDRs use intelligence concerning the factors of the operational environment to determine the type and scale of operations.

2-39. Intelligence also aids in determining the impact of significant regional features and hazards on the conduct of both friendly and threat operations. Significant regional factors include the civil considerations applied to the AOI. Intelligence analysis also assists in recommending the rules of engagement (ROE) and other restrictions which will affect operations in the JFC's JOA.

2-40. Intelligence relating to the threat's military and nonmilitary capabilities assists in determining the threat's ability to conduct military operations. Factors that operational intelligence addresses include mobilization potential, force structure (including alliance forces), force dispositions, equipment, doctrine, C2 structure, goals, and their decision-making process. Intelligence includes the continuous refinement of the threat characteristics for the entire array of the enemy's forces in the AOI.

TACTICAL

2-41. Timely, relevant, accurate, predictive, and tailored intelligence allows tactical units to achieve an advantage over the threat and is essential for mission success. Predictive intelligence also enables the staff to better develop COAs. Tactical intelligence—

- Identifies and assesses the threat's tactical capabilities, COAs, and vulnerabilities, as well as describes AO.
- Seeks to identify when, where, and in what strength the enemy will conduct operations.

- Provides the commander with information on imminent threats to the force including those from terrorists, saboteurs, insurgents, and foreign intelligence collection.
- Provides critical support to friendly information tasks.
- Develops and disseminates targeting information and intelligence.

2-42. Intelligence provides the tactical commander with the information and intelligence required to conduct missions against threat forces. At the tactical level, the intelligence tasks support the execution of battles and engagements. These intelligence tasks have a different focus than those at other levels due to their ability to immediately influence the outcome of the tactical commander's mission. They include information gathered from tactical sources, such as combat information, interrogations, debriefings, and eliciting information from captured or misplaced personnel. For a complete listing of tactical collective tasks, refer to FM 7-15.

INTELLIGENCE REACH

2-43. The G-2/S-2 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 in support of the CCIR. Table 2-1 shows examples of partners and sources for intelligence reach. The following are steps that the staff can take to ensure optimal use, operability, and effectiveness of intelligence reach:

- Establish data exchange methods and procedures.
- Establish electronic message transfer procedures.
- Establish homepages for identified forces.
- Establish POCs for I&W centers, production centers, combatant command Joint Intelligence Operations Centers (JIOCs), DIA, INSCOM, and their MSCs, such as National Ground Intelligence Center (NGIC) and the higher MI organizations.
- Ensure the intelligence staff has the necessary personnel, training, automated systems, bandwidth, and resources to conduct intelligence reach.
- Determine IRs through staff planning. Develop production requirements for identified intelligence gaps.
- Order geospatial products for the projected AOI.
- Establish and maintain a comprehensive directory of intelligence reach resources before deployment and throughout operations. The value of intelligence reach will greatly increase as the staff develops and maintains ready access to rich information resources. These resources are numerous and may include, for example, Army, Joint, DOD, non-DOD, national, commercial, foreign, and university research programs.
- Know what types of information the resources can provide. Continuously expand the resource directory through identification of new resources.
- Use intelligence reach first to fill intelligence gaps and requirements and answer RFIs. This technique can preclude unnecessary tasking or risk to limited ISR assets.
- Maintain continuous situational understanding and anticipate intelligence requirements. Use intelligence reach to fulfill these requirements and provide the results to the commander and staff for the conduct of operations.
- Exchange intelligence reach strategies with other units.
- Present the information retrieved through intelligence reach in a usable form. Share the information derived from intelligence reach with subordinate, lateral, and higher echelons. Ensure follow-on forces have all information as well.

CATEGORIES OF INTELLIGENCE PRODUCTS

2-44. Intelligence products are generally placed in one of seven production categories:

- I&W.
- Current intelligence.
- GMI.
- Target intelligence.
- S&TI.
- CI.
- Estimative.

2-45. The categories of intelligence are distinguishable from each other primarily by the purpose of the intelligence product. The categories can overlap and some of the same intelligence is useful in more than one category. Depending upon the echelon, intelligence organizations use specialized procedures to develop each category of intelligence. The following information describes each category.

Table 2-1. Examples of partners and sources for intelligence reach

ARMY	SERVICES	JOINT	DOD
ACE ISE MIB 902d NGIC ATCAE ARISCs USAIC Cultural Center USACHCS World Religion Center	ONI NMIC AF ISR Agency NASIC MCIA	USEUCOM JAC USSOUTHCOM JIOC USSOCOM JIOC USSPACECOM CIC USJFCOM AIC USCENTCOM JIOC USTRANSCOM JIOC USSTRATCOM USPACOM JOIC USNORTHCOM JIOC USAFRICOM JIOC	DIA CMO MSIC NCMI DAO DH NGA NSA RSOCs
NON-DOD	**NATIONAL**	**COMMERCIAL**	**FOREIGN**
DOE FBI DOS DEA FEMA ICE	DNI NIC CIA NRO INR DOT, Office of Intel Support DHS	RAND Jane's Defense Weekly Economic Intelligence Unit CNN Reuters Associated Press United Press International	DIS NDHQ DIO

INDICATIONS AND WARNINGS

2-46. I&W are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could pose a threat to the US or multinational military, political, or economic interests or to US citizens abroad. I&W includes forewarning of threat actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the US, US overseas forces, or multinational forces; hostile reactions to US reconnaissance activities; terrorist attacks; and other similar events. (See JP 2-0 for more information on I&W.)

2-47. While the G-2/S-2 is primarily responsible for producing I&W intelligence, each element, such as the MP conducting PIO, within every unit contributes to I&W through awareness of the CCIRs and reporting related information.

CURRENT INTELLIGENCE

2-48. Current intelligence involves the integration of time-sensitive, all-source intelligence and information into concise, accurate, and objective reporting on the AO and current threat situation. One of

the most important forms of current intelligence is the threat situation portion of the COP. The G-2/S-2 is responsible for producing current intelligence for the unit. Current intelligence supports ongoing operations during the full spectrum of operations. In addition to the current situation, current intelligence should provide projections of the threat's anticipated situations (estimates) and their implications on the friendly operation. (See JP 2-0.)

GENERAL MILITARY INTELLIGENCE

2-49. GMI is intelligence concerning military capabilities of foreign countries or organizations or topics affecting potential US or multinational military operations relating to armed forces capabilities, including threat characteristics, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness and area and terrain intelligence. This broad category of intelligence is normally associated with long-term planning at the national level. However, GMI is also an essential tool for the intelligence staff and should be in place long before the start of preparations for a particular military operation.

2-50. An up-to-date, comprehensive intelligence database is critical to the unit's ability to plan and prepare rapidly for the range of operations and global environments in which it may operate. GMI supports the requirement to quickly respond to differing crisis situations with corresponding intelligence spanning the globe. One of the many places to get information for GMI is the medical intelligence database. The G-2/S-2 planner develops his initial IPB from GMI products. Additional information on medical intelligence is found in FM 4-02, FM 4-02.7, FM 4-02.17, FM 4-02.18, and FM 8-42.

2-51. The G-2/S-2 develops and maintains the unit's GMI database on potential threat forces and environments based on the commander's guidance. As an essential component of intelligence readiness, this database supports the unit's planning, preparation, execution, and assessment of operations. The G-2/S-2 applies and updates the database as it executes its intelligence production tasks.

TARGET INTELLIGENCE

2-52. Target intelligence is the analysis of enemy units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, re-attack, or exploitation (for intelligence). It consists of two mutually supporting production tasks: target development and combat assessment.

- Target development is the systematic evaluation and analysis of target systems, system components, and component elements to determine HVTs for potential attack through maneuver, fires, or nonlethal means.
- Once attacked, combat assessment provides a timely and accurate estimate of the affects of the application of military force (lethal or nonlethal) and information operations on targets and target systems based on predetermined objectives.

SCIENTIFIC & TECHNICAL INTELLIGENCE

2-53. S&TI is the product resulting from the collection, evaluation, analysis, and interpretation of foreign S&T information. S&TI covers foreign developments in basic and applied research and in applied engineering techniques and S&T characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the related research and development (R&D), and the production methods employed for their manufacture.

2-54. S&TI concerns foreign developments in basic and applied sciences and technologies with warfare potential. It includes characteristics, capabilities, vulnerabilities, and limitations of all weapon systems, subsystems, and associated materiel, as well as related R&D. S&TI also addresses overall weapon systems and equipment effectiveness. Specialized organizations—such as the DIA Missile and Space Intelligence Center (MSIC), INSCOM, Air Missile Defense, Army Area Air and Missile Defense Command, and NGIC—produce this category of intelligence. The G-2/S-2 establishes instructions within SOPs, OPORDs, and OPLANs for handling and evacuating captured enemy materiel (CEM) for S&TI exploitation.

COUNTERINTELLIGENCE

2-55. As previously defined at the end of chapter 1, CI analyzes the threats posed by foreign intelligence and security services and the intelligence activities of non-state actors, such as organized crime, terrorist groups, and drug traffickers. CI analysis incorporates all-source information and the results of CI investigations and operations to support a multidiscipline analysis of the FP threat.

ESTIMATIVE

2-56. Estimates provide forecasts on how a situation may develop and the implications for planning and executing military operations. Estimative intelligence goes beyond descriptions of adversary capabilities or reporting of enemy activity. It tries to forecast the unknown based on an analysis of known facts using techniques such as pattern analysis, inference, and statistical probability.

UNIFIED ACTION INTELLIGENCE OPERATIONS

2-57. Joint operations focus and maximize the complementary and reinforcing effects and capabilities of each service. JFCs synchronize the complementary capabilities of the Service components that comprise the joint force.

2-58. The employment of MI in campaigns and major operations must be viewed from a joint perspective, and the intelligence construct must establish a fully interoperable and integrated joint intelligence capability. ARFOR intelligence assets work with multinational and interagency partners to accomplish their missions. Ideally, multinational and interagency intelligence partners provide cultures, perspectives, and capabilities that reinforce and complement Army MI strengths and capabilities. Close intelligence coordination is the foundation of successful unified action.

PERSISTENT SURVEILLANCE AND RELATED ARMY CONSTRUCTS (TACTICAL PERSISTENT SURVEILLANCE)

2-59. A critical part of current operations is the execution of the joint doctrinal concept of persistent surveillance. Joint doctrine defines persistent surveillance as:

> *A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near-real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action.*

2-60. In its simplest form, the goal of the Army construct of joint persistent surveillance is to provide the right intelligence to the right person at the right time and in the right format focused to their requirements. It is based on the fundamental Army ISR construct and recognizes ISR as a combined arms mission. However, these constructs (specifically tactical persistent surveillance) focus on balancing future requirements for providing or accessing combat information and intelligence in a networked environment to support ongoing operations while also supporting longer-term intelligence analysis and planning and other staff functions. Most of the constructs focus on—

- Embedded ISR synchronization capabilities.
- Improved ISR sensor capabilities.
- Assured network communications capability.
- An enterprise approach to analysis, processing, and data and information access across units and organizations and echelons.
- Enhanced automated analytical tools to include planning and control and analytical change detection capabilities.

2-61. Within the latest Army intelligence constructs there is recognition that while vast improvements in ISR capabilities are possible, these new characteristics are not likely to fully develop in the near future. ISR will—

- Not provide guaranteed and uninterrupted collection on all requirements for all operations.
- Not change from inherently using a combined arms operational construct.
- Not eliminate all operational risk and uncertainty.
- Not obviate the need for operational planning.
- Not exclusively focus on sensor capability issues.

2-62. However, we can expect gradual incremental improvements in—

- Phasing and overlapping of ISR capabilities.
- Integrating and networking ISR assets and collection efforts.
- Executing intelligence handover.

THE NATURE OF LAND OPERATIONS

2-63. Landpower is the ability—by threat, force, or occupation—to gain, sustain, and exploit control over land, resources, and people. Army operations reflect expeditionary and campaign capabilities that constantly adapt to each campaign's unique circumstances. Expeditionary capabilities require forces organized to be modular, versatile, and rapidly deployable. Rapidly deployed expeditionary force packages provide immediate options for seizing or retaining the operational initiative and also allow the conduct of sustained operations for as long as necessary. Army forces are organized, trained, and equipped for endurance. The Army's preeminent challenge is to balance expeditionary agility and responsiveness with the endurance and adaptability needed to complete a campaign successfully.

2-64. The capability to prevail in close combat is indispensable and unique to land operations. The outcome of battles and engagements depends on Army forces' ability to prevail in close combat. Many factors inherent in land combat combine to complicate the situation. These factors include chaos, complexity, insufficient intelligence, errors in understanding or planning, difficult terrain, the civilian population, and an adaptive and lethal enemy. The axiom "intelligence drives operations" continues to be true especially for land operations. Operations and intelligence are inextricably linked.

2-65. Four considerations are preeminent in generating expeditionary capabilities and Army force packages.

- **Scope.** Considers and strives to understand the threat throughout the depth of an operational area. Commanders rely on intelligence in order to use maneuver, fires, and other elements of combat power to defeat or destroy enemy forces.
- **Duration.** Forces routinely conduct missions prior to, during, and after the commitment of land combat forces. Intelligence is always engaged.
- **Terrain.** Missions occur among a complex variety of natural and manmade features. Employing forces in the complexity of the ground environment requires thorough planning.
- **Permanence.** Forces are integrated with, or assigned to, land combat forces as they seize or secure ground.

2-66. Several attributes of the land environment affect the application of landpower. These attributes include the requirement to deploy and employ Army forces rapidly; the requirement for Army forces to operate for protracted periods; the nature of close combat; and uncertainty, chance, friction, and complexity. Reconnaissance, surveillance, and target acquisition (RSTA)/ISR is the means the Army uses to implement the joint doctrinal concept of persistent surveillance in support of tactical operations. Dependable technology and responsive intelligence lessen the effects of uncertainty, chance, friction, and complexity. Complex and dynamic Army tactical operations require extensive ISR capabilities to satisfy the commander's information requirements to detect, locate, characterize, identify, track, and target HPTs and to provide combat assessment in real time within a very fluid operational environment.

2-67. RSTA/ISR is a full spectrum combined arms mission that integrates ground and air capabilities to provide effective, dynamic, timely, accurate, and assured combat information and multidiscipline actionable intelligence for lethal and nonlethal effects and decisions in DS of the ground tactical commander.

JOINT INTELLIGENCE OPERATIONS

2-68. The JTF commanders and their intelligence staffs must—

- Understand the intelligence requirements of superior, subordinate, and component commands.
- Identify organic intelligence capabilities and shortfalls.
- Access combatant command and national systems to ensure appropriate intelligence and CI products are available to the JTF.

2-69. The JTF's intelligence effort focuses on integrating multi-source information and multi-echelon intelligence into all-source intelligence products that provide relevant, accurate, and timely knowledge of the adversary and joint operational area. These products must neither overload the user nor the communications architecture.

2-70. The J-2 directly supports the JFC's responsibilities for determining objectives, directing operations, and evaluating the effects of those operations. The J-2 supports the execution of the plan with the intelligence needed to sustain the operation, attain joint force objectives, provide support to subordinate commands, and continually support protection. The J-2 analyzes the potential threat situation and provides assessments to support friendly opportunities. To maintain the initiative, the JFC will seek to get inside the adversary's decision-making cycle. The J-2 also ensures the provision of the required ISR support to the JTF and its subordinate functional and service components.

2-71. Figure 2-3 shows a notional JTF J-2 organization. The overall organization of the JTF and operations will dictate actual composition of the J-2. At a minimum, a core element of analytical, ISR management, and administrative capabilities is required.

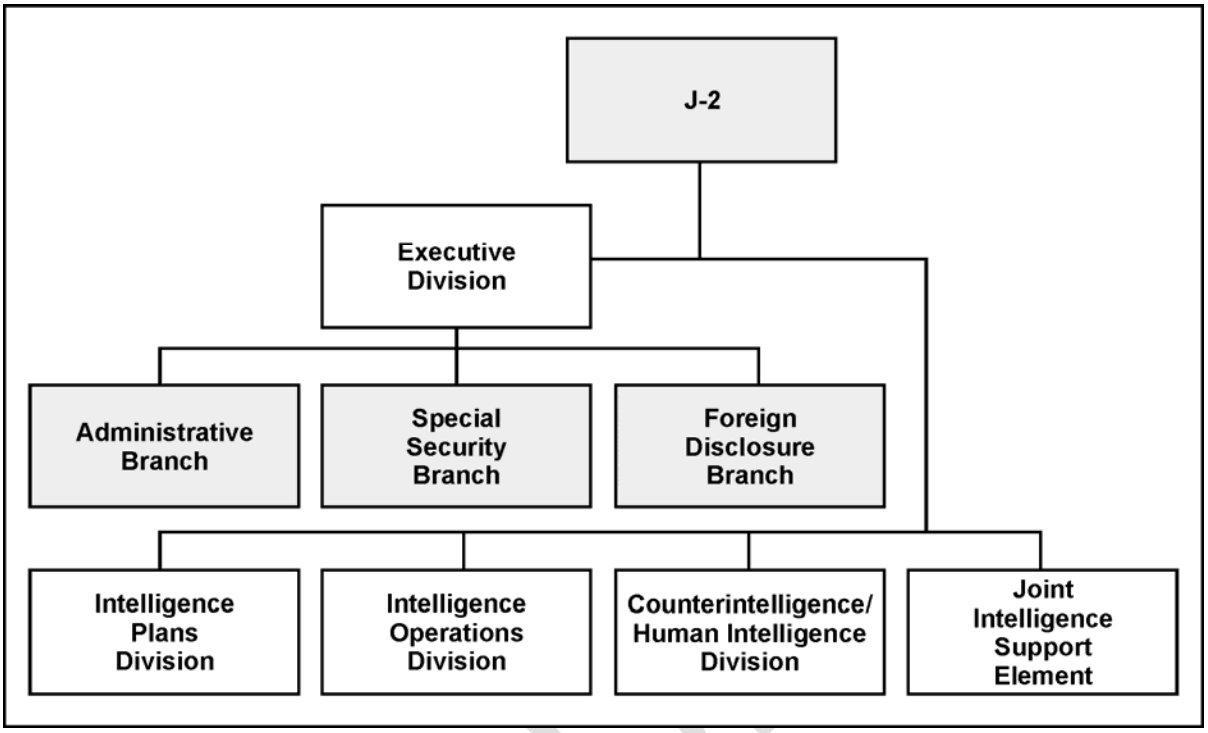


Figure 2-3. Notional joint task force J-2 organization

Considerations in Joint Intelligence Operations

2-72. When conducting joint intelligence operations, there are a number of unique problems that can arise due to the complexity of integrating the efforts of the different services and commands. Elements affecting joint intelligence operations among the different services include the following:

- Intelligence liaison is critical to the success of intelligence operations and requires early establishment, particularly between units that have not routinely trained together and possess differing capabilities. As a minimum, organizations exchange liaison teams with the higher echelon organization. Additional liaison may be necessary to facilitate joint force collection, production, or dissemination requirements. Liaison teams—
  - Support planning and C2 of intelligence operations.
  - Ensure timely two-way flow of intelligence between commands.
  - Manage intelligence and resource requirements of the subordinate command.
  - Advise the commander on service ISR capabilities, limitations, and employment.
- Commanders and staffs use IPB to understand the battlefield and develop or refine plans and orders. IPB products exchanged between echelons ensure a common picture of the battlefield and estimate of the situation.
- Communications considerations for joint operations include—
  - Planning for intelligence communications transition to facilitate execution of branches or sequels to the plan or to accommodate shifting of the main effort from one force to another.
  - Identifying the initial communications architecture to include establishing procedures and protocols for information exchanges (databases, text, imagery, voice, and video).

  - Balancing the availability of service-unique intelligence systems between echelons or services. This may require each service providing additional resources. The senior commander is responsible for allocating resources.
  - Disseminating intelligence between commands and services. Additional communications equipment, intelligence terminals, and personnel may be required to balance capabilities between services.
- Identifying the databases each service possesses or has access to; determining which databases will support the operation and, if necessary, merge them into a single database; and ensure access by the entire force prior to deployment and/or commencement of operations.
- Providing a focal point for subordinate command access to national or joint intelligence is essential. The senior commander will request and allocate resources required to support this access.
- The JFC's intelligence requirements, concept of the operation, and intent drive the ISR effort. The different organizations and services participating in joint intelligence operations must continuously share information, intelligence, and products to satisfy requirements. See FM 2-01 for details on intelligence requirements and requirements management. See JP 2-01 for more information on joint support to military operations.

Joint Reserve Intelligence Centers

2-73. A Joint Reserve Intelligence Center (JRIC) is a joint intelligence production and training activity that uses information networks to link reservist intelligence personnel with the combatant commands, Services, and/or combat support agencies. A JRIC is located within a Service-owned and managed sensitive compartmented information (SCI) facility and may also include surrounding collateral and unclassified areas involved in the performance and direct management of intelligence production work that uses Joint Reserve Intelligence Program infrastructure and connectivity. The more than 20 JRICs located around the country are equipped to effectively serve as satellite elements to combatant command JIOCs; however, they are shared facilities that serve multiple customers and missions (JP 2-0).

Joint Intelligence Architecture

2-74. In addition to the J-2 staffs at every joint level of command, the key organizations in the joint intelligence architecture are the Defense Joint Intelligence Operations Center (DJIOCs), the combatant command JIOCs, and, when formed, the JTF's joint intelligence support element (JISE). Working together, these organizations play the primary role in managing and controlling joint intelligence operations. The formal relationships which link these organizations facilitate information management and optimize complementary intelligence functions by echelon without obstructing the timely flow of intelligence up, down, or laterally.

2-75. The DJIOC is the lead DOD intelligence organization responsible for integrating and synchronizing MI and national intelligence capabilities in support of the combatant commands. The DJIOC collaborates with the United States Strategic Command's Joint Functional Component Command-Intelligence Surveillance, and Reconnaissance and Director of National Intelligence (DNI) representatives to formulate and recommend to the Chairman of the Joint Chiefs of Staff (CJCS), for Secretary of Defense action, solutions for deconflicting combatant command requirements for national intelligence resources, and ensures an integrated response to their needs.

2-76. The DJIOC ensures that joint force crisis-related and time-sensitive intelligence requirements are tasked to the appropriate Service, combatant command, or national agency when the requirements cannot be satisfied by assigned or attached assets.

Joint Task Force Joint Intelligence Operations Center

2-77. Combatant command JIOCs are the primary intelligence organizations providing support to joint forces at the operational and tactical levels. The JIOC integrates the capabilities of DNI, Service, combat support agency, and combatant command intelligence assets to coordinate intelligence planning, collection management, analysis, and support.

2-78. The combatant command JIOC is organized in accordance with the CCDR's guidance, but normally performs the general functions described in JP 2-0 and specific combatant command intelligence TTP.

Joint Task Force Joint Intelligence Support Element

2-79. At the discretion of a subordinate JFC, a JTF JISE may be established during the initial phases of an operation to augment the subordinate joint force J-2 element. Under the direction of the J-2, the JISE normally manages the intelligence collection, production, and dissemination for the JTF. The JISE provides intelligence to JTF operational forces and performs common intelligence functions.

2-80. By design, the JISE is scaleable and can expand to meet the needs of the JTF and the operating environment. It is composed of analytical experts, analysis teams, and ISR managers that provide services and products, which the JTF, JTF staff, and subordinate components require. These experts focus on solving the JTF commander's operational intelligence problems. The JISE's capability to perform all-source analysis and ISR synchronization is key to producing operational intelligence that is timely, relevant, accurate, predictive, and targeted. Figure 2-4 illustrates the features of a typical JISE.

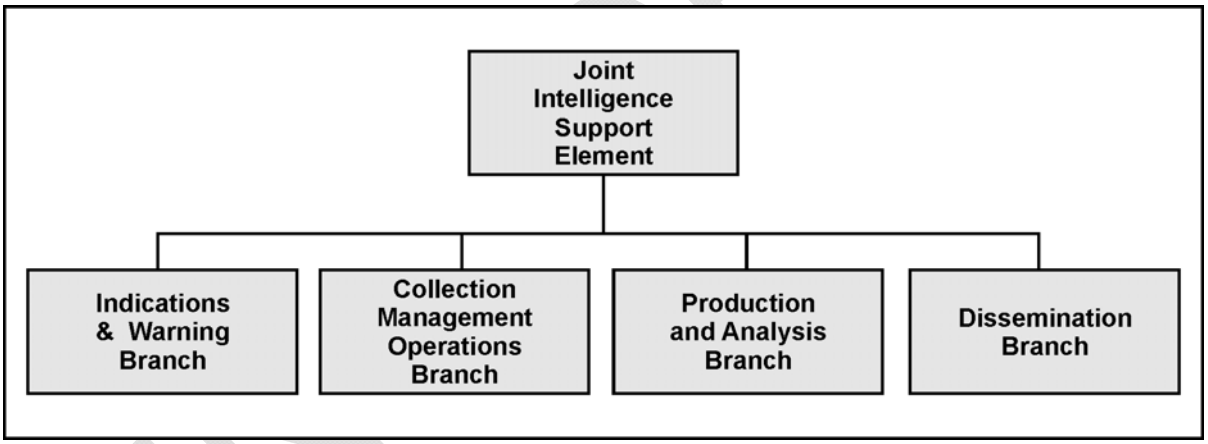


Figure 2-4. Typical joint intelligence support element

Joint Task Force Intelligence Organizations

2-81. In addition to the JISE, the JTF commander and J-2 may require other supporting JIOCs or teams based on projected operations. The JTF commander may make a request to the DJIOC for specific national intelligence agency capabilities. The DJIOC evaluates and coordinates the JTF commander's requirements with the J-3, J-5, and national intelligence agencies and tailors the composition of the deployment packages to meet those needs.

2-82. The deployment packages, such as the National Intelligence Support Team (NIST), provide access to the entire range of capabilities resident in the national intelligence agencies and can focus those capabilities on the JTF commander's intelligence requirements. The J-2X manages and coordinates the HUMINT and CI activities of national, combatant command, and service components operating within the JTF's joint operational area. The Joint Captured Materiel Exploitation Center (JCMEC) assists in management of recovery, exploitation, and disposal of captured enemy equipment (CEE). The JTF commander's

requirements dictate the composition and tailoring of such deployment packages. See JP 3-33 for more information on JTF intelligence organizations.

Augmentation Considerations

2-83. Depending on the scale of the operations, the intelligence organizations described above and those of the JTF's subordinate command may require personnel augmentation. Optimum use of available intelligence assets is essential to ensure quality support in meeting the JTF commander's requirements. The JTF J-2 should identify intelligence personnel augmentation requirements in accordance with the CJCS Instruction 1301.01. The CCDR and the JTF refine personnel requirements and initiate requests when they anticipate or start an operation.

2-84. A consideration for the JTF when requesting support or augmentation is that these national level teams and individual augmentees are not totally self-contained elements; rather they require logistic, information, and other support from the supported command. Each deployment is unique based on mission, duration, team composition, and capabilities required. A full NIST, for example, requires a private, access-controlled area within a sensitive compartmented SCI facility work environment and dedicated secure communications.

2-85. For more information on intelligence operations as they apply to other armed services, see the individual service intelligence doctrine. See also JP 2-0 series, JP 3-0, and JP 5-0 for details on joint intelligence operations and considerations.

Multinational Intelligence

2-86. Multinational intelligence operations take place within the structure of an alliance or coalition. Some multinational military organizations, such as the North Atlantic Treaty Organization and the UN Command in the Republic of Korea, are highly structured and enduring. Others, such as the coalition formed during the Gulf War, are less formal and temporary.

2-87. In multinational operations, the multinational force commander exercises command authority over a military force composed of elements from two or more nations. Therefore, in most multinational operations, the JTF must share intelligence, as necessary, for mission accomplishment with foreign military forces and coordinate exchange of intelligence with those forces.

2-88. In some circumstances, the JTF may need to seek authority to go outside the usual political-military channels to provide information to NGOs. The JTF must tailor intelligence policy and dissemination criteria to each multinational operation.

2-89. The minimum requirements for sharing intelligence, how intelligence is cleared for sharing, and the specific means for intelligence sharing will be situationally dependent. See FM 3-16 and the ABCA Coalition Operations Handbook for more information about intelligence considerations in multinational operations.

FORCE PROJECTION OPERATIONS

2-90. 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 ARFOR wherever they deploy. Force projection operations are inherently joint and require detailed planning and synchronization. As discussed below, force projection encompasses a range of processes—mobilization, deployment, employment, sustainment, and redeployment.

2-91. The Army must change its mindset from depending on an "intelligence buildup" to performing intelligence readiness on a daily basis in order to meet the requirements for strategic responsiveness. MI personnel, even in garrison at the lowest tactical echelons, must use their analytic and other systems and

prepare for possible operations on a daily basis. When a unit has an indication that it may be deployed or have a contingency mission in an area of the world, they can begin to generate intelligence knowledge on their projected AO.

2-92. Built on a foundation of intelligence readiness, the intelligence warfighting function provides the commander with the intelligence needed to plan, prepare, and execute force projection operations. Successful intelligence during force projection operations relies on continuous collection and intelligence production before and during the operation. In a force projection operation, higher echelons will provide intelligence to lower echelons until the tactical ground force completes entry and secures the lodgment area. The joint force J-2 must exercise judgment when providing information to subordinate G-2s/S-2s to avoid overwhelming them.

2-93. Key planning factors for intelligence in force projection include—

- Stay out front in intelligence planning:
  - Begin to generate intelligence knowledge as soon as possible.
  - Develop a steady effort.
  - Prioritize intelligence requirements for surge.
- Understand how to get intelligence support:
  - Identify information and asset requirements.
  - Know what is available and how and when to get it.

2-94. The G-2/S-2 must anticipate, identify, consider, and evaluate all threats to the entire 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 enemy actions because of its limited combat power and knowledge of the AO. Intelligence personnel must, therefore, emphasize the delivery of combat information and intelligence products that indicate changes to the threat or AO developed during predeployment IPB. The G-2/S-2 should—

- Review available databases on assigned contingency AOIs, conduct IPB on these AOIs, and develop appropriate IPB products.
- Comply with higher headquarters SOPs and manuals for specific intelligence operations guidance.
- Coordinate for and rehearse electronic message transfers (for example, Internet Protocol addresses, routing indicators) using the same communications protocols with theater, higher headquarters, subordinate, and lateral units that the unit would use when deployed.
- Plan, train, and practice surging intelligence functions on likely or developing contingency crises.
- Prepare and practice coordination from predeployment through redeployment with other elements and organizations (for example, HUMINT, IMINT, SIGINT, MASINT, information operations, staff weather officer, CA, PSYOP, and SOF units, to include databases and connectivity).
- Include the following as a part of daily (sustainment) operations:
  - USAR and other augmentation.
  - A linguist plan with proficiency requirements. (Alert linguists through early entry phases of deployment.)
  - Training (individual and collective).
- Establish formal or informal intelligence links, relationships, and networks to meet developing contingencies.
- Forward all RFIs to higher headquarters in accordance with SOPs.
- Establish statements of intelligence interests, other production, and I&W requirements.

2-95. To draw intelligence from higher echelons and focus intelligence downward, based on the commander's needs, the G-2/S-2 must—

- Understand the J-2's multiple echelon and broadcast dissemination capability to ensure near-real time (NRT) reporting to all deployed, in transit, or preparing to deploy forces.
- Maintain or build intelligence databases on the environment and threats for each probable contingency.
- State and record the CCIR (as a minimum, list the PIRs and ISR tasks or requests).

2-96. Until the unit's collection assets become operational in the AO, the G-2/S-2 will depend upon intelligence from the ARFOR or JTF to answer the unit's intelligence needs. Intelligence and ISR considerations during force projection are discussed below.

MOBILIZATION

2-97. 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 USAR, and assembling and organizing personnel, supplies, and materiel. A unit may be brought to a state of readiness for a specific mission or other national emergency. This process, called mobilization, is where specific US Active Army, ARNG, ARNGUS, and USAR units, capabilities, and personnel are identified and integrated into the unit. During mobilization, theG-2/S-2 must—

- Monitor intelligence reporting on threat activity and I&W data.
- Manage IRs and RFIs from their unit and subordinate units to include updating ISR planning.
- Establish habitual training relationships with their US Active Army, ARNG, ARNGUS, and USAR augmentation units and personnel as well as higher echelon intelligence organizations as identified in the existing OPLAN.
- Support the USAR units and augmentation personnel by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify ISR force requirements for the different types of operations and contingency plans.
- Identify individual military, civilian, and contractor augmentation requirements for intelligence operations. The Army, and the Intelligence warfighting function in particular, cannot perform its missions without the support of its Department of the Army Civilians and contractors. The force increasingly relies on the experience, expertise, and performance of non-uniformed personnel and has fully integrated these non-uniformed personnel into the warfighting team.

2-98. During mobilization the G-2/S-2, in conjunction with the rest of the staff, must ensure the adequacy of training and equipping of US Army Active and USAR MI organizations and individual augmentees to conduct intelligence operations. Predictive intelligence also supports the decisions the commander and staff must make about the size, composition, structure, and deployment sequence of the force in order to create the conditions for success.

2-99. The G-2/S-2 supports peacetime contingency planning with IPB products and databases on likely contingency areas. The G-2/S-2 establishes an intelligence synchronization plan that will activate upon alert notification. For smooth transition from predeployment to entry, the G-2/S-2 must coordinate intelligence synchronization and communications plans before the crisis occurs. The intelligence synchronization plan identifies the intelligence requirements supporting those plans, to include—

- ISR assets providing support throughout the AOI.
- Command and support relationships of ISR assets at each echelon.
- Report and request procedures not covered in unit SOPs.
- Sequence of deployment of ISR personnel and equipment. Early deployment of key ISR personnel and equipment is essential for FP and combat readiness. Composition of initial and

follow-on deploying assets is influenced by the factors of METT-TC, availability of communications, and availability of lift.

- Communications architecture supporting both intelligence staffs and ISR assets.
- Friendly vulnerabilities to hostile intelligence threats and plans for conducting FP measures. The staff must begin this type of planning as early as possible to ensure adequate support to FP of deploying and initial entry forces.
- Monitor time-phased force and deployment data (TPFDD) and recommend changes in priority of movement, unit, or capability to enable ISR operations.

2-100. The G-2/S-2 must continually monitor and update the OPLANs to reflect the evolving situation, especially during crisis situations. National intelligence activities monitor regional threats throughout the world and can answer some intelligence requirements supporting the development of OPLANs.

2-101. Upon alert notification, the G-2/S-2 updates estimates, databases, IPB products, and other intelligence products needed to support command decisions on force composition, deployment priorities and sequence, and the AOI. Units reassess their collection requirements immediately after alert notification. The G-2/S-2 begins verifying planning assumptions within the OPLANs. CI and ISR personnel provide FP support and antiterrorism measures.

2-102. Throughout mobilization, unit intelligence activities will provide the deploying forces with the most recent intelligence on the AO. The intelligence staff will also update databases and situation graphics. The G-2/S-2 must—

- Fully understand the unit, ARFOR, and joint force intelligence organizations.
- Revise intelligence and intelligence-related communications architecture and delete or integrate any new systems and software with the current architecture.
- Support 24-hour operations and provide continuous intelligence.
- Plan all required intelligence reach procedures.
- Determine transportation availability for deployment and availability when deployed.
- Determine all sustainability requirements.
- Determine intelligence release requirements and restrictions; releasability to multinational and HN sources.
- Review status of forces agreements (SOFAs), ROE, international laws, and other agreements, emphasizing the effect that they have on intelligence collection operations. (Coordinate with the staff judge advocate on these issues.)
- Ensure ISR force deployment priorities are reflected in the TPFDD to support ISR operations based upon the factors of METT-TC.
- Ensure intelligence links provide the early entry commander vital access to multi-source army and joint intelligence collection assets, processing systems, and databases.
- Review the supporting unit commanders' specified tasks, implied tasks, task organization, scheme of support, and coordination requirements with forward maneuver units. Address issues or shortfalls and direct or coordinate changes.
- Establish access to national HUMINT, **Error! Bookmark not defined.**IMINT, SIGINT, MASINT, and CI databases, as well as automated links to joint service, multinational, and HN sources.

DEPLOYMENT

2-103. Deployment is the movement of forces and materiel from their point of origin to the AO. This process has four supporting components: predeployment activities, fort-to-port, port-to-port, and port-to-destination. Success in force projection operations hinges on timely deployment. The size and composition of forces requiring lift are based on the factors of METT-TC, availability of pre-positioned assets, the

capabilities of HN support, and the forward presence of US forces. Force tailoring is the process used to determine the correct mix and sequence of deploying units.

2-104. During deployment, intelligence organizations at home station or in the rear area take advantage of modern satellite communications, broadcast technology, and automated data processing systems to provide graphic and textual intelligence updates to the forces enroute. Enroute updates help eliminate information voids and, if appropriate, allow the commander to adjust the plan prior to arrival in JOA in response to changes in the operational environment.

2-105. Intelligence units extend established networks to connect intelligence staffs and collection assets at various stages of the deployment flow. Where necessary, units establish new communications paths to meet unique demands of the mission. If deployed, theater and corps analysis and control elements play a critical role in making communications paths, networks, and intelligence databases available to deploying forces.

2-106. Space-based systems are key to supporting intelligence during the deployment and the subsequent stages of force projection operations by—

- Monitoring terrestrial AOIs through ISR assets to help reveal enemy location and disposition, attempting to identify the enemy's intent.
- Providing communications links between forces enroute and in the continental United States (CONUS).
- Permitting MI collection assets to accurately determine their position through the Global Positioning System.
- Providing timely and accurate data on meteorological, oceanographic, and space environmental factors that might affect operations.
- Providing warning of theater ballistic missile launches.
- Providing timely and accurate weather information to all commanders through the Integrated Meteorological System.

2-107. Situation development dominates intelligence operations activities during initial entry operations. The G-2/S-2 attempts to identify all threats to arriving forces and assists the commander in developing FP measures. During entry operations, echelons above corps organizations provide intelligence. This support includes providing access to departmental and joint intelligence and deploying scalable intelligence assets. The entire effort focuses downwardly to provide tailored support to deploying and deployed echelons in response to their CCIRs (PIRs and FFIR).

2-108. Collection and processing capabilities are enhanced, as collection assets build up in the deployment area, with emphasis on the build-up of the in-theater capability required to conduct sustained ISR operations. As the build-up continues, the G-2/S-2 strives to reduce total dependence on extended split-based intelligence from outside the AO. As assigned collection assets arrive into the JOA, the G-2/S-2 begins to rely on them for tactical intelligence although higher organizations remain a source of intelligence.

2-109. As the ARFOR headquarters arrives in the JOA, the joint force J-2 implements and, where necessary, modifies the theater intelligence architecture. Deploying intelligence assets establishes liaison with staffs and units already present in the AO. Liaison personnel and basic communications should be in place prior to the scheduled arrival of parent commands. ISR units establish intelligence communications networks.

2-110. CONUS and other relatively secure intelligence bases outside the AO 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 split-based support of a force projection operation. These systems provide a continuous flow of intelligence to satisfy many operational needs.

2-111. The G-2/S-2, in coordination with the G-3/S-3, participates in planning to create conditions for decisive operations. The G-2/S-2 also adjusts collection activities as combat power strength builds. During entry operations the G-2/S-2—

- Monitors FP indicators.
- Monitors the ISR capability required to conduct sustained intelligence operations.
- Monitors intelligence reporting on threat activity and I&W data.
- Develops measurable criteria to evaluate the results of the intelligence synchronization plan.
- Assesses—
  - Push versus pull requirements of intelligence reach.
  - Effectiveness of the intelligence communications architecture.
  - Reporting procedures and timelines.
  - Intelligence to OPLANs and OPORDs, branches, and sequels (to include planning follow-on forces).

ENTRY OPERATIONS

2-112. Enemies often possess the motives and means to interrupt the deployment flow of Army forces. Threats to deploying forces may include advanced conventional weaponry (air defense, mines) and weapons of mass destruction. Sea and air ports of debarkation should be regarded as enemy HPTs because they are the entry points for forces and equipment. Ports of debarkation are vulnerable because they are fixed targets with significant machinery and equipment that is vulnerable to attack; in addition to military forces and materiel, HN support personnel, contractors, and civilians may all be working there.

2-113. An enemy attack, or even the threat of an enemy attack, on a port of debarkation can have a major impact on force projection momentum. Commanders at all levels require predictive intelligence so that they may focus attention on security actions that reduce vulnerabilities. To avoid, neutralize, or counter threats to entry operations, the commanders rely on the ability of the G-2/S-2 to support future operations by accurately identifying enemy reactions to US actions, anticipating their response to our counteractions and predicting additional enemy COAs.

SUSTAINMENT

2-114. Sustainment involves providing and maintaining levels of personnel and materiel required to sustain the operation throughout its duration. Sustainment may be split-based between locations within and outside continental United States (OCONUS). For intelligence, sustainment may be focused on force rotation—ensuring that intelligence personnel or units entering an established AO have current intelligence and the appropriate level of detailed knowledge of ongoing intelligence operations. This includes providing data file updates through the generate intelligence knowledge step of the intelligence process prior to the deployment of replacement personnel or units as well as a coordinated intelligence hand-off of ongoing intelligence operations such as military source operations. Sustainment also includes ensuring units have the MI assets required to accomplish the mission, such as personnel (including linguists), communications systems, ISR systems, and appropriate maintenance support.

REDEPLOYMENT

2-115. Redeployment is the process by which units and materiel reposture themselves in the same theater; transfer forces and materiel to support another JFC's operational requirements; or return personnel and materiel to the home or demobilization station upon completion of the mission. Redeployment operations encompass four phases:

- Recovery, reconstitution, and predeployment activities.
- Movement to and activities at the port of embarkation.
- Movement to the port of debarkation.

- Movement to homestation.

2-116. As combat power and resources decrease in the AO, FP and I&W become the focus of the commander's intelligence requirements. This in turn drives the selection of those assets that must remain deployed until the end of the operation and those that may redeploy earlier. The S-2—

- Monitors intelligence reporting on threat activity and I&W data.
- Continues to conduct intelligence to FP.
- Requests ISR support (theater and national systems) and intelligence in support of redeployment.

2-117. After redeployment, MI personnel and units recover and return to predeployment activities. ISR units resume contingency-oriented peacetime intelligence operations. USAR ISR units demobilize and return to peacetime activities. G-2/S-2s must—

- Monitor intelligence reporting on threat activity and I&W data.
- Update or consolidate databases.
- Maintain intelligence readiness.
- Provide their input into the Force Design Update process to refine modified table of organizations and equipment and evaluate the need for individual mobilization augmentee personnel.

PART TWO

Intelligence in Full Spectrum Operations

Part Two discusses the role of intelligence and the intelligence warfighting function within full spectrum operations and the interaction of the intelligence process with the operations process. It describes how both MI and the intelligence warfighting function provide commanders and warfighters with the intelligence they require in order to drive operations.

Chapter 3 discusses the role of intelligence within full spectrum operations. It provides an overview of intelligence readiness, particularly the intelligence requirements associated with force projection. The doctrinal concept of MI asset technical channels is discussed as a complement to, not a replacement of, the Army's command and support relationships.

Chapter 4 presents the intelligence process, describes its interaction with the operations process, and discusses the methodology that accomplishes the primary focus of intelligence in full spectrum operations, to provide the warfighter with effective intelligence.

Chapter 3

Fundamentals in Full Spectrum Operations

THE OPERATIONAL CONCEPT

3-1. *The Army's operational concept is full spectrum operations: Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and appreciation of all aspects of the situation guides the adaptive use of Army forces* (FM 3-0).

3-2. Intelligence supports the commander across full spectrum operations. It helps the commander decide when and where to concentrate sufficient defeat threat COAs. ISR is essential for the commander to achieve surprise against the threat, preclude surprise from the threat, maintain the initiative on the battlefield, and win battles. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to see and strike the enemy simultaneously throughout the AO.

3-3. Every Soldier in the command is responsible for detecting and reporting threat activities, dispositions, and capabilities. In order to accomplish this, the task of Soldier surveillance and reconnaissance was developed to help commanders get combat information and reports. This task is critical because the environment we operate in is characterized by violence, uncertainty, complexity, and asymmetric methods by the threat. The Every Soldier is a Sensor program is supported through Soldier

surveillance and reconnaissance. (See FM 2-91.6 for a detailed discussion of Soldier surveillance and reconnaissance.)

3-4. The increased situational awareness that Soldiers develop through personal contact and observation is a critical element of that unit's ability to more fully understand the battlefield. Soldiers collect combat information that is then processed into intelligence by unit intelligence analysts. While medical personnel cannot be assigned ISR tasks due to their Geneva Convention category status, medical personnel who gain information through casual observation of activities in plain view while discharging their humanitarian duties will report the information to their supporting intelligence element.

INTELLIGENCE SUPPORT TO THE ELEMENTS OF FULL SPECTRUM OPERATIONS

3-5. Full spectrum operations require continuous, simultaneous combinations of offensive, defensive, and stability or civil support tasks. Intelligence through ISR facilitates understanding of the portions of the mission variables of enemy, terrain, weather, and civil considerations, the latter in coordination with the G-9/S-9. This allows the commander to conduct operations at a time and place of our choosing rather than reacting to enemy operations. Operations are organized as decisive, shaping, and sustaining.

OFFENSIVE OPERATIONS

3-6. *Offensive operations are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers* (FM 3-0). Offensive operations at all levels require effective intelligence to help the commander avoid the enemy's main strength and to deceive and surprise the enemy. During offensive operations, intelligence must provide the commander with updated IPB products and an intelligence running estimate in a timely manner for the commander to significantly affect the enemy. The intelligence running estimate ensures commanders have the intelligence they need to conduct offensive operations with minimum risk of surprise.

3-7. The G-2/S-3 develops IPB products to assist the commander in identifying all aspect within the AO or AOI that will affect mission accomplishment. The entire staff, led by the echelon intelligence staff, uses the IPB process to identify any aspects of the AO or AOI that will affect enemy, friendly, and third-party operations. The IPB process is collaborative in nature and requires information from all staff elements and some subordinate units. All staff and subordinate elements use the results and products of the IPB process for planning. FM 2-01.3 describes the IPB process.

3-8. The G-2/S-2 supports the commander's use of unit ISR assets to analyze the terrain and confirm or deny the enemy's strengths, dispositions, and likely intentions. These assets also gather information concerning the civilian considerations within the AO. The G-2/S-2 and operations officers, in coordination with the rest of the staff, develop an integrated ISR plan that satisfies the commander's maneuver, targeting, and information requirements.

3-9. In offensive operations, a commander's information requirements often include—

- Locations, composition, equipment, strengths, and weaknesses of the defending enemy force, to include high-payoff targets (HPTs) and enemy ISR capabilities.
- Locations of possible enemy assembly areas.
- Locations of enemy indirect fire weapon systems and units.
- Locations of gaps and assailable flanks.
- Locations of areas for friendly and enemy air assaults.
- Locations of enemy air defense gun and missile units.
- Locations of enemy electronic warfare (EW) units.
- Effects of terrain and weather and civil considerations on current and projected operations.
- Numbers, routes, and direction of movement of dislocated civilians.

- Withdrawal routes for enemy forces.
- Anticipated timetable schedules for the enemy's most likely COA and other probable COAs.
- Locations of enemy C2 and ISR systems and the frequencies used by the information systems linking these systems.

DEFENSIVE OPERATIONS

3-10. Defensive operations are combat operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations. The immediate purpose of defensive operations is to defeat an enemy attack. Commanders defend to buy time, hold key terrain, hold the enemy in one place while attacking in another, or destroy enemy combat power while reinforcing friendly forces.

3-11. Intelligence should determine the enemy's strength, COAs, and location of enemy follow-on forces. Defending commanders can then decide where to arrange their forces in an economy-of-force role to defend and shape the battlefield. Intelligence support affords commanders the time necessary to commit the striking force precisely.

3-12. Intelligence supports the commander's defensive operations with IPB products to identify probable enemy objectives and various approaches; patterns of enemy operations; the enemy's vulnerability to counterattack, interdiction, EW, air attacks, and canalization by obstacles; and the enemy's capability to conduct air attacks against his force, insert forces behind friendly units, and employ CBRNE weapons. The G-2/S-2 must also evaluate how soon follow-on forces can join the fight against an enemy attacking in echelons.

3-13. The G-2/S-2 also supports the commander with synchronization of ISR operations to answer the CCIRs. ISR operations must be continuously assessed and updated during operations. The ISR plan must provide early identification of as many of the commander's requirements as possible. It is critical that the G-2/S-2 support the commander's ability to see the enemy during the conduct of all defensive operations. In defensive operations, these requirements often include—

- Locations, composition, equipment, strengths, and weaknesses of the advancing enemy force.
- Enemy reconnaissance objectives or goals.
- Locations of possible enemy assembly areas.
- Locations of enemy indirect fire weapon systems and units.
- Locations of gaps, assailable flanks, and other enemy weaknesses.
- Locations of areas for enemy helicopter and parachute assaults.
- Locations of artillery and air defense gun and missile units.
- Locations of enemy EW of civilian populations.
- Effects of terrain and weather and civil considerations on current and projected operations.
- Likely withdrawal routes for enemy forces.
- Numbers, routes, and direction of movement of dislocated civilians.
- Anticipated timetable for the enemy's most likely COA.
- Locations of enemy command posts, fire direction control centers, EW sites, and target acquisition sensor and target fusion sites and the frequencies they are using.

STABILITY OPERATIONS

3-14. *Stability operations encompass various military missions, tasks, and activities conducted outside the US in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief* (JP 3-0).

3-15. The environment is often much more complex during stability operations and as a result intelligence is often more complex. Elements of combat power are discussed below. As a result, commanders must be even more involved in and knowledgeable of ISR during stability operations.

3-16. In stability operations, commanders often require even more detailed intelligence and IPB products necessary to determine how best to influence the environment and enhance regional stability. The identification and analysis of the threat, terrain, weather, and civil considerations (civil considerations are described using the acronym ASCOPE) are important in conducting stability operations. A lack of knowledge concerning insurgents, how to separate local combatants, local politics, customs, and culture could lead to US actions which attack unsuitable targets or which may offend or cause mistrust among the local population. This could potentially threaten mission accomplishment.

CIVIL SUPPORT OPERATIONS

3-17. *Civil support is the Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities* (JP 1-02). Civil support includes operations that address the consequences of natural or manmade disasters, accidents, terrorist attacks, and incidents within the United States and its territories. Army forces conduct civil support operations when the size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

3-18. The ARNG often acts as a first military responder for civil support operations on behalf of State authorities while serving in State active duty status or when functioning under Title 32 U.S. Code authority. State active duty status refers to ARNG forces and State defense force personnel under State control. In State active duty status, the State Governor commands the ARNG and the State defense force. The State defense force is sometimes known as the State organized defense force or State militia (some States do not have a State defense force). Missions are planned and executed in accordance with the needs of the State and within the guidelines of State laws and statutes. ARNG forces in State active duty status can perform civil law enforcement missions in accordance with the laws and statutes of their State.

3-19. Intelligence support in civil support operations is conducted strictly within the guidelines of US law and focused on the specific missions directed by the Secretary of Defense. IPB can identify natural threats and hazards such as areas likely to flood during heavy rain or in the event of a dam or levee break.

3-20. Intelligence analysts can fuse the information from a variety of DOD supporting agencies and develop information and intelligence products to answer PIRs. Intelligence analysis can also assist local authorities in identifying areas in which the military can provide support in restoring essential services. ISR assets can assist search and rescue, damage assessment, potential hazards, and locating displaced persons. ISR assets can also help identify CBRNE materiel and weapons manufacturing and storage locations. ISR assets require authorization from the Secretary of Defense. For more information on intelligence support to civil support operations, see FMI 2-91.501.

ELEMENTS OF COMBAT POWER

3-21. *Combat power is the total means of destructive, constructive, and information capabilities which a military unit or formation can apply at a given time. Army forces generate combat power by converting potential into effective action* (FM 3-0). There are eight elements of combat power. The first two—leadership and information—are applied throughout and multiply the effects of the other six elements of combat power, collectively described as the Army warfighting functions. (Refer to FM 3-0, chapter 4, for a full discussion of the elements of combat power.)

- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- C2.

- Protection.

ARMY CAPABILITIES

3-22. An ARFOR is the Army Service component headquarters for a JTF or a joint and multinational force (FM 3-0). MI has responsibilities and functions that support full spectrum operations at all echelons. The distribution of specific intelligence assets enhances the capability of the combined arms team. The planning and analysis of force tailoring identifies intelligence resources and capabilities required and blends the mission requirements necessary for mission success. The task organization that follows force tailoring establishes an ordered command and support structure for the intelligence assets to conduct their support missions.

COMBINED ARMS

3-23. Combined arms is the synchronized and simultaneous application of the elements of combat power—to achieve an effect greater than if each element of combat power was used separately or sequentially
(FM 3-0). As an integral part of combined arms, staffs must identify all intelligence capabilities that will be required to conduct operations in an assigned AO. Specific units with those specific intelligence capabilities will then be requested for the force pool for force tailoring.

FORCE TAILORING

3-24. *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* (FM 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 intelligence capabilities and resources to support the commander's guidance, intent, and mission objectives.

TASK-ORGANIZING

3-25. *Task-organizing is the act of designing an operating force, support staff, or logistic package of specific size and composition to meet a unique task or mission. Characteristics to examine when task-organizing the force include but are not limited to training, experience, equipage, sustainability, operating environment, enemy threat, and mobility. For Army forces, it includes allocating available assets to subordinate commanders and establishing their command and support relationships* (FM 3-0).

3-26. Once intelligence assets have been allocated, each echelon task-organizes those intelligence assets to provide maximum mission support. Task-organizing of intelligence assets occur within a tailored force package as commanders organize units for specific missions. Intelligence assets are task-organized to force packages based on intelligence capability requirements for each force's mission. As commanders reorganize units for subsequent missions, intelligence assets may be redistributed in order to support new or changing requirements.

COMMAND AND SUPPORT RELATIONSHIPS

3-27. Command and support relationships provide the basis for unity of command in operations. Command and relationships may limit the ability of a commander to affect task organization. Commanders use Army command and support relationships when task-organizing MI assets. Since most MI forces are task-organized to support operations, MI leaders at all echelons must understand the impact of command and support relationships on their units, personnel, and assets. Command and support relationships may fall within the framework of joint doctrine. See JP 1 for a discussion of joint command relationships and authorities. See FM 3-0, appendix B, for a discussion of command and support relationships.

3-28. Table 3-1 lists the Army command relationships and their inherent responsibilities.

3-29. While not an actual command or support relationship, technical channels often affect certain intelligence operations. Intelligence commanders and the intelligence staff maintain control of each intelligence discipline during operations through technical channels to ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant US law, the law of war, international law, directives, DOD Instructions, and orders. In specific cases, regulatory authority is granted to national and DOD intelligence agencies for specific intelligence discipline collection and is passed through technical channels.

3-30. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and assess portions of the unit's collection effort. Technical channels also involve translating ISR tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the ISR effort. Technical channels include, but are not limited to—

- Defining, managing, or guiding the employment of specific ISR assets.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized training for specific MI personnel or units.

3-31. An example of technical channels is the Prophet control team converting the PIR and ISR tasks developed during the MDMP and assigning times and anticipated enemy frequencies for subordinate Prophet teams to collect.

2679 **Table 3-2. Army command relationships and inherent responsibilities**

If relationship is:	Then inherent responsibilities:							
	Have command relationship with:	May be task-organized by:	Unless modified, ADCON responsibility goes through:	Assigned position or AO by:	Provides liaison to:	Establish/ maintain communications with:	Has priorities established by:	Can impose on gaining unit further command or support relationship of:
Organic	All organic forces organized with the HQ	Organic HQ	Army HQ specified in organizing document	Organic HQ	NA	NA	Organic HQ	Attached; OPCON; TACON; GS; GSR; R; DS
Assigned	Combatant command	Gaining HQ	Gaining Army HQ	OPCON chain of command	As required by OPCON	As required by OPCON	ASCC or Service assigned HQ	As required by OPCON HQ
Attached	Gaining unit	Gaining unit	Gaining Army HQ	Gaining unit	As required by gaining unit	Unit to which attached	Gaining unit	Attached: OPCON; TACON; GS; GSR; R; DS
OPCON	Gaining unit	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ[1]	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	OPCON; TACON; GS; GSR; R; DS
TACON	Gaining unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by parent unit	Gaining unit	TACON; GS; GSR; R; DS

Note 1. In NATO, the gaining unit may not task organize a multinational force. (See TACON.)

ADCON – administrative control
AO – area of operations
ASCC – Army service component command
DS – direct support
GS – general support
GSR – general support-reinforcing
HQ – headquarters
NA – not applicable
NATO – North Atlantic Treaty Organization
OPCON – operational control
R – reinforcing
TACON – tactical control

2680

Chapter 4

Intelligence Process in Full Spectrum Operations

THE INTELLIGENCE PROCESS

4-1. Commanders use the operations process of plan, prepare, execute, and assess to continuously design and conduct operations. Figure 4-1 shows this process. The commander cannot successfully accomplish the activities involved in the operations process without information and intelligence. The design and structure of intelligence operations support the commander's operations process by providing him with intelligence regarding the threat, terrain and weather, and civil considerations.

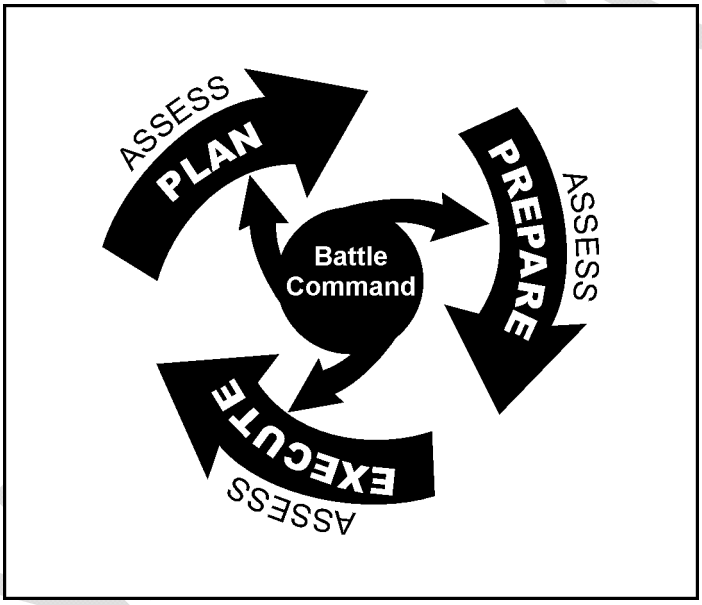


Figure 4-1. The operations process

4-2. The operations process and the intelligence process are mutually dependent. The commander provides the guidance and focus through CCIRs (PIRs and FFIRs) that drives the operations and intelligence processes. The intelligence process operates during all parts of the operations process in order to provide the continuous intelligence essential to the operations process. Intelligence about the threat, terrain and weather, and civil considerations supports Army forces in combining offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. IPB is one of the integrating processes that occurs during all operations process activities and must be synchronized with each other as well as integrated into the overall operation. Figure 4-2 shows the relationship between the operations and intelligence processes.

4-3. Intelligence operations consist of the five steps that constitute the intelligence process and four continuing activities. Just as the activities of the operations process overlap and recur as the mission demands, so do the steps of the intelligence process. Additionally, the analyze, commander's input, assess,

and propagate continuing activities of the intelligence process occur continuously throughout the intelligence process.

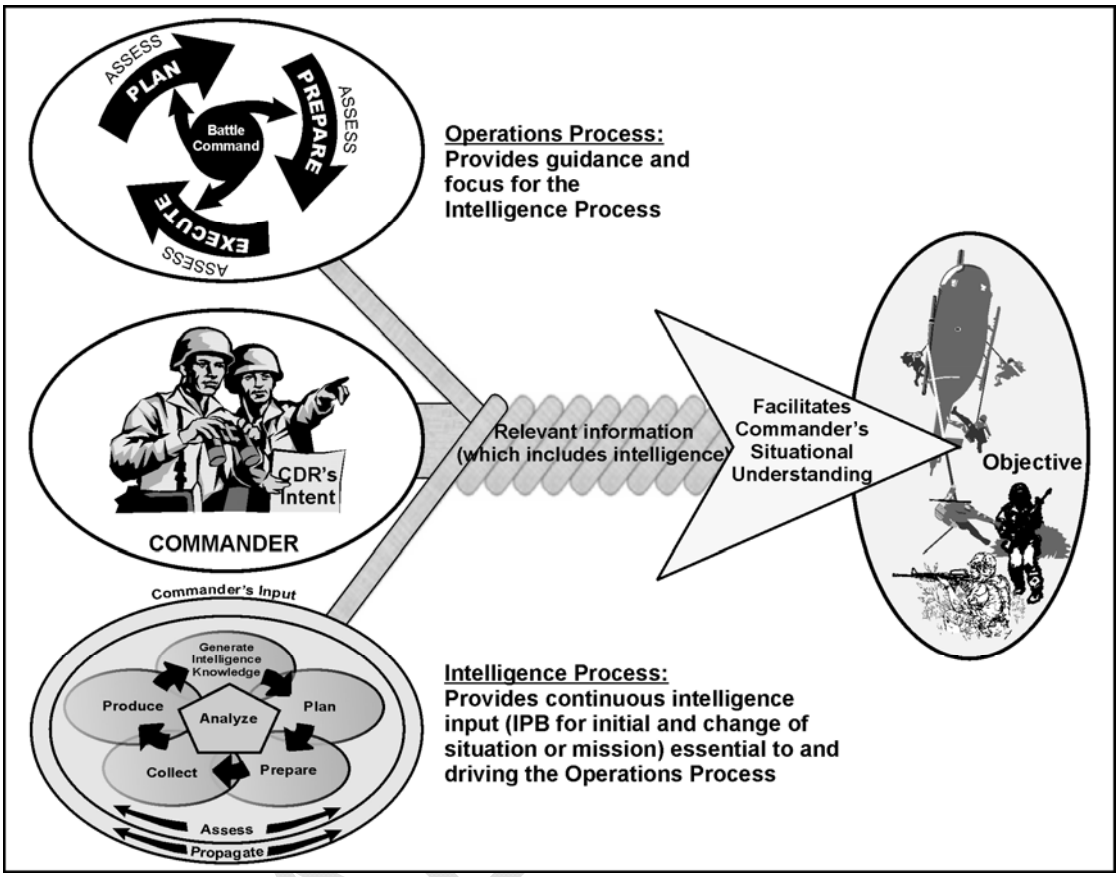


Figure 4-2. The relationship between the operations and intelligence processes

GENERATE INTELLIGENCE KNOWLEDGE

4-4. Generate intelligence knowledge consists of all activities necessary to collect the initial (baseline) information and intelligence from existing sources in order to develop an initial intelligence survey and an initial intelligence estimate in preparation for the MDMP with the staff. Additionally, the G-2/S-2 must retrieve, update, or develop any required intelligence databases.

4-5. The generate intelligence knowledge step of the intelligence process must be accomplished well in advance of the mission analysis step of MDMP and prior to conducting the initial IPB. This step must be completed thoroughly in order to prepare the intelligence staff for the planning step. It also sets the stage for developing ISR operations. For further information on generate intelligence knowledge, see paragraph 1-56.

PLAN

4-6. The planning step of the intelligence process consists of activities that include assessing the situation, envisioning the commander's desired endstate, identifying pertinent information and intelligence requirements in coordination with the commander, developing an ISR plan to satisfy those requirements in coordination with the operations officer, directing intelligence operations, and synchronizing the intelligence effort.

4-7. The G-2/S-2 must ensure that they are working closely with the G-3/S-3 on the ISR plan and that both are working from the same intelligence baseline. The commander's intent, planning guidance, and CCIRs (PIRs and FFIRs) drive the planning of intelligence operations. Planning, managing, and coordinating these operations are continuous activities necessary to obtain information and produce intelligence essential to decision making.

Coordinate

4-8. Staff and leaders coordinate with various organizations to ensure the necessary resources, such as linguist support (see appendix B), information, intelligence, training, and procedures are in place to facilitate effective intelligence operations.

- Coordination for and Management for Movement of ISR Assets. All ISR assets at one time or another will move through or near another unit's AO. To avoid fratricide, ISR elements must coordinate with units, G-3/S-3, G-2/S-2, and each other, ISR elements must also coordinate with appropriate staff elements to establish no-fire areas and/or other fire support coordination measures around ISR assets, airspace control measures, and appropriate weapons control status (in reference to aerial ISR assets).
- Coordination for and Management of Information and Intelligence. The intelligence staff must prepare and practice coordination and management with personnel from all MI units, non-MI units, other Service components, and multinational organizations that may contribute to or facilitate the ISR effort. This coordination enables the G-2/S-2 to share and update databases, information, and intelligence and ensures connectivity with those organizations. All units are sources of relevant information regarding the enemy and the operational environment.
- Liaison. In order to accomplish the mission, exchange information and intelligence, move through certain areas and ensure protection, it may be necessary to coordinate with many different elements, organizations, and LNs of the country in which friendly forces are conducting operations. LNs include police, town officials, foreign military forces, and political and other key figures within the AO. Operations may also necessitate coordination with other US and multinational forces; for example, the International Security Assistance Force, the International Police Task Force, Organization for Security and Cooperation in Europe, and Defense HUMINT.
- Movement. Coordination with the G-3/S-3 and proper management ensures ease of movement and safe passage of friendly forces through an area. Coordinating movement also helps avoid fratricide.

Planning Considerations for Intelligence Warfighting Function

4-9. The intelligence warfighting function is a unified system that anticipates and satisfies intelligence needs. Commanders ensure its proper employment by clearly articulating intent, designating CCIRs (PIRs and FFIRs), and prioritizing targets. Commanders must, however, understand the limitations of the intelligence warfighting function to preclude unrealistic expectations of the system. The following are intelligence warfighting function considerations:

- Intelligence only reduces uncertainty in the AO; it does not eliminate it entirely. The commander will always have to determine the presence and degree of risk involved in conducting a particular mission.
- The intelligence warfighting function is composed of finite resources and capabilities. Intelligence systems and Soldiers trained in specific ISR skills are limited in any unit. Once lost to action or accident, these Soldiers and systems are not easily replaceable; for some, 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 enemy actions. The loss of qualified language-trained Soldiers, especially Soldiers trained in low-density languages or skills, could adversely affect intelligence operations as well.

- In order to effectively and efficiently provide timely, relevant, accurate, predictive, and tailored intelligence, the intelligence warfighting function must have adequate communications equipment, capacity, and connectivity. Commanders and G-2/S-2s must ensure communications support to intelligence has the appropriate priority.
- Commanders and G-2/S-2s cannot expect that higher echelons will automatically send them everything they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from conducting detailed analysis and focusing the efforts of higher headquarters. Nor can they expect products pushed to them to be always at the level of detail they require. Utilizing the DCGS-A enterprise, commanders and G-2/S-2s must focus higher echelons by clearly articulating and actively pursuing intelligence requirements. By providing higher echelons with a clear picture of the required intelligence products, commanders can also narrow the flow of intelligence and information and preclude being overwhelmed by too much information.

4-10. Commanders should be aware that intelligence collection is enabled by, and subject to, laws, regulations, and policies to ensure proper conduct of intelligence operations. While there are too many to list here specifically, categories of these legal considerations include United States Codes, Executive Orders, National Security Council Intelligence Directives, Army Regulations, United States Signal Intelligence Directives, SOFAs, ROE, and other international laws and directives.

Red Teaming

4-11. Whenever possible, commanders employ red teams to examine plans from a threat's perspective. Red team is a special staff section whose members primarily participate in planning in the future operations and plans cells unless integrated into another cell. Red team members anticipate cultural perception of partners, enemies, adversaries, and others, and conducts independent critical reviews and analysis. The red team provides the commander with an enhanced capability to explore alternatives during planning and execution.

4-12. Red teaming provides commanders alternative perspectives by challenging planning assumptions, assisting in defining the problem and end-state, identifying friendly and enemy vulnerabilities, and identifying assessment measures. These alternative perspectives not only account for the threat and environment in plans, concepts, organizations, and capabilities but also address the standpoint of our multinational partners, enemies, and adversaries, and other perspectives.

ISR Planning Considerations

4-13. ISR planning consists of two significant staff processes: ISR synchronization and ISR integration. ISR synchronization is the responsibility of the intelligence officer and the G-2/S-2 staff. The operations officer is responsible for ISR integration with the support of the intelligence officer. ISR synchronization involves the entire staff and all of the warfighting functions. All staff sections within a command post have the responsibility to satisfy information requirements. Satisfying information requirements through staff element coordination facilitates ISR planning by eliminating the necessity to task an asset to collect information that another unit or asset already observed in the course of operations. The commander may designate an ISR working group; however, the primary staff's responsibilities cannot be delegated.

4-14. When planning, preparing, conducting, and assessing ISR operations, the intelligence staff must strive to achieve maximum efficiency and effectiveness. The intelligence staff considers six essential criteria in conducting ISR synchronization for the following:

- **Anticipate**. The intelligence officer must recognize when and where to shift collection or identify new intelligence requirements. The intent of this principle is to identify a new or adjust an existing requirement and present it to the commander before the commander or other staff members identify the need. By participating in the decision making, planning, and operations processes, intelligence officers can best anticipate requirements.

- **Coordinate**. The intelligence staff must coordinate and collaborate with all staff sections and with both higher headquarters, subordinate, and adjacent units in order for ISR operations to be continuously synchronized. The intelligence staff must be engaged in the unit's planning and orders production activities to ensure early identification of intelligence requirements. The intelligence staff must also be integrated into the combat information reporting and battle tracking of current operations to anticipate the need for dynamic or ad hoc ISR taskings. Early and continuous consideration of ISR planning factors enhances the unit's ability to direct ISR assets in a timely manner in support of developing situations, ensures thorough planning, and increases flexibility in selecting and retasking assets.
- **Prioritize**. The priority for ISR operations begins with the CCIR. Then intelligence officers prioritize each validated intelligence requirement based upon its importance in supporting the commander's intent and decisions and the current situation so that low-density and high-demand ISR assets and resources are directed against the most critical requirements.
- **Balance**. Balance involves using a combination of redundancy, mix, and cueing of a variety of ISR capabilities to complement each other. Balance is simply achieving maximum efficiency using an appropriate mix of disciplines, ISR assets, and resources to satisfy as many competing intelligence requirements as possible.
  - *Redundancy* is achieved using several same-type ISR assets to cover the same named area of interest (NAI).
  - *Mix* means planning for complementary coverage by a combination of assets from multiple units and intelligence disciplines designed to increase the probability of collection success and reduce the chances of successful threat deception.
  - *Cueing* involves the use of one or more sensors to provide data that result in another system to conducting collection. Balance also means that the intelligence staff should resist favoring or becoming too reliant on one particular unit, discipline, or system.
- **Control**. Units should first use organic and allocated ISR assets to ensure timely and effective collection as well as overall synchronization. These assets are more responsive to the commander's needs and can be balanced with other resources. ISR assets belonging other units, agencies, or organizations may have limited availability and are likely to receive differing priorities from their respective commanders. Information gathered by other ISR resources is harder to verify and correlate with information collected by organic assets.
- **Reach**. Units can use intelligence reach and RFIs to answer initial information requirements without having to use the echelon's ISR assets. Intelligence which is confirmed by more than one intelligence discipline is generally preferred over single-source reporting. Therefore, a unit should not depend solely on intelligence reach to satisfy a PIR.

4-15. The staff must not only carefully focus ISR plans on answering the CCIRs (PIRs and FFIRs) but also enable the quick retasking of units and assets as the situation changes. ISR synchronization includes continually identifying new and partially filled intelligence gaps. This ensures that the developing threat situation, not just our OPLAN, "drives" ISR operations. Specifically, intelligence officers—

- Evaluate ISR assets for suitability (availability, capability, vulnerability, and performance history) to execute ISR tasks and make appropriate recommendations on asset tasking to the operations officer.
- Assess ISR collection against CCIRs (PIRs and FFIRs) to determine the effectiveness of the ISR plan. They maintain situational awareness in order to identify gaps in coverage and to identify the need to cue or recommend redirecting ISR assets to the operations officer,
- Update the ISR synchronization plan as requirements are satisfied modified, or created. They remove satisfied requirements and recommend new requirements as necessary.
- In coordination with operations staff, monitor satisfactory completion of ISR tasks from higher headquarters. Operations officer integrate the updated synchronization plan into orders tasking ISR assets.

4-16. ISR operations require constant coordination between the current operations, intelligence, and plans cells within an organization. The entire staff participates in ISR planning. The G-2S-2 is the lead for ISR synchronization. The G-3/S-3 creates the ISR plan.

4-17. ISR integration is vital in controlling limited ISR assets. Thoroughly integrated ISR operations add many collection resources, multiplying the potential for multi-source collection of information. The ongoing activities of ISR all contribute to updating the ISR plan.

4-18. FMI 2-01 describes the ISR synchronization process in detail. FM 3-55 (when published) will address ISR overall.

Requirements

4-19. For intelligence purposes there are three types of requirements: PIRs, intelligence requirements, and information requirements. Each requirement is broken down into discrete pieces to answer that requirement. These pieces are referred to as indicators and specific information requirements, which facilitate the answering of the requirements. The indicators and specific information requirements are used by ISR planners to develop the ISR plan. Figure 4-3 shows the process of developing requirements and integrating them into the ISR process.

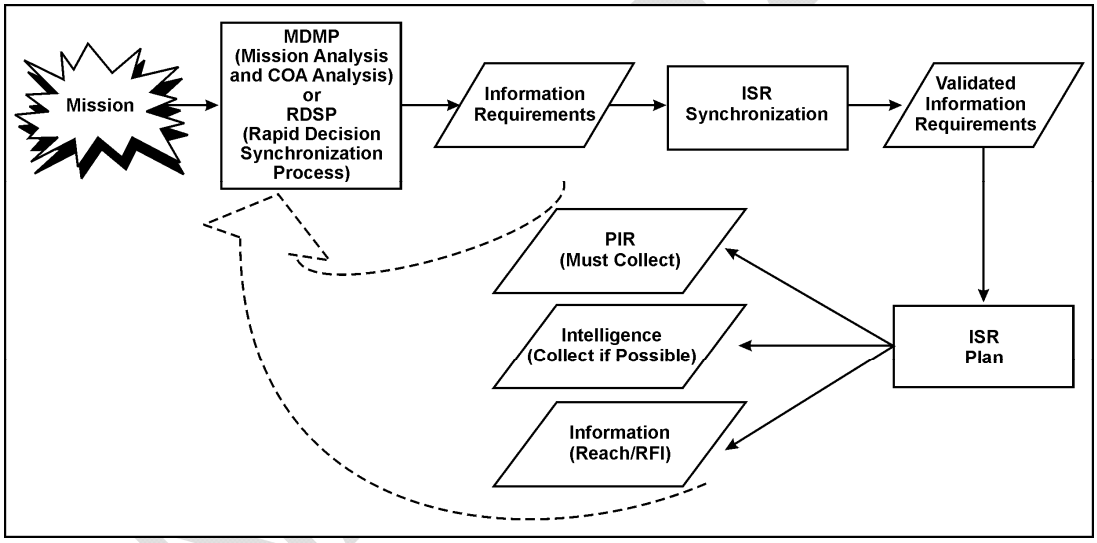


Figure 4-3. Requirements development and integration into the ISR process

Commander's Critical Information Requirement

4-20. *A commander's critical information requirement is an information requirement identified by the commander as being critical to facilitating timely decision making. The two key elements are friendly force information requirements and priority intelligence requirements* (JP 3-0).

4-21. A CCIR directly influences decision making and facilitates the successful execution of military operations. Commanders decide whether to designate an information requirement as a CCIR based on likely decisions and their visualization of the COA. A CCIR may support one or more decisions. The list of CCIRs constantly changes. Commanders add and delete individual requirements throughout an operation based on the information needed for specific decisions.

Validated Information Requirements

4-22. There are three types of validated information requirements that result from ISR synchronization: PIRs, intelligence requirements, and information requirements.

- **Priority Intelligence Requirements.** A priority intelligence requirement is an intelligence requirement, stated by the commander as a priority for intelligence support which the commander needs to support decision making and to understand the AO or the threat. The intelligence officer manages PIRs for the commander, but the PIRs belong solely to the commander. All staff sections may recommend requirements that may become PIRs. PIRs are selected as part of the process of identifying CCIRs during mission analysis; they, along with friendly force information requirements (FFIRs), are updated as part of updating the CCIRs throughout the operation. PIRs have first priority in collection assets tasked to their collection.
- **Intelligence Requirements.** An intelligence requirement is a type of information requirement developed by subordinate commanders and the staff (to include subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. Intelligence requirements are developed by the staff and subordinate commanders (and their staffs) and must be answered to facilitate operations. They require ISR collection assets to be assigned for their collection, second in priority to PIRs.
- **Information Requirements.** Information requirements are all information elements the commander and staff require to successfully conduct operations; that is, all elements necessary to address the factors of METT-TC (FM 6-0). After validated requirements are identified and the ISR plan is completed, there may additional information requirements that support the development of situational understanding, answer gaps in the COP, and provide additional details required for analysis. These are information requirements that do not require collection by ISR assets to be answered. The staff answers these requirements through intelligence reach or RFIs.

PREPARE

4-23. The best plans will not ensure success without meticulous and thorough preparation for operations. The prepare task includes those staff and leader activities which take place upon receiving the OPORD, OPLAN, WARNO, or commander's intent to improve the unit's ability to execute tasks or missions and survive on the battlefield. For intelligence units, these activities include—

- Conducting necessary coordination in accordance with the OPORD, METT-TC, unit SOP.
- Establishing and testing the intelligence architecture. This activity includes complex and technical issues like hardware, software, communications, COMSEC materials, network classification, technicians, database access, LNOs, training, funding, and TTP.
- Establishing intelligence team cohesiveness. This activity includes knowing different unit's and organization's capabilities, training the necessary collective skills, establishing effective relationships with different units and organizations, developing mutual battle rhythms and TTP, and leveraging the right architectures and collaboration tools.
- Coordinating effective analytic collaboration. This activity is necessary to maximize the complementary analytic capabilities of different units and organizations that produce intelligence within the same JOA. Coordinating this collaboration is an effort-intensive activity that requires careful mutual planning, division of labor, defined responsibilities, and procedures for adapting to changing circumstances as they develop.
- Establishing reporting procedures.
- Updating IPB, the intelligence running estimate, and ISR synchronization.
- Producing intelligence estimates.
- Ensuring staff and personnel are trained. If personnel are not adequately trained at this point, they must be trained or the leader must evaluate the risk they bring to the operation.

- Planning refinement, brief-backs, SOP reviews, and rehearsals, and coordinating with various elements and organizations.
- Establishing other troop-leading procedures or coordination, as necessary, in accordance with METT-TC factors.

G-2/S-2 Preparation Activities

4-24. The G-2/S-2 takes numerous steps before mission execution to ensure intelligence operations run smoothly and effectively within the staff section. These steps include, but are not limited to, the following:

- Conduct rehearsals (at a minimum communications, intelligence production, ISR, and unit rehearsals).
- Review and update available databases and IPB products.
- Review applicable SOPs, Army Regulations, DA Pamphlets, Field Manuals, and ROE for guidance in conducting intelligence operations.
- Plan and practice actions supporting likely contingencies, or the branches or sequels to an operation.
- Verify coordination measures are still in effect.
- Conduct essential training (individual and collective) that is realistic and tied to the mission.
- Verify communications protocols with theater and higher headquarters and subordinate and lateral units.
- Update intelligence databases.
- Update the forces with the most recent intelligence on the AO immediately before mission execution.

Inspections

4-25. Once all required equipment and support materials have been acquired, staff and leaders must conduct inspections to ensure that the unit and Soldiers are prepared to conduct their mission. It is crucial that staff and leaders check to verify that procedures, personnel, equipment, and services are in place and ready for mission execution. Leaders can only expect what they inspect.

Rehearsals

4-26. Rehearsals help units prepare for operations by either verifying that provisions and procedures are in place and functioning or identifying inadequacies, which staff and leaders must remedy. They allow participants in an operation to become familiar with and to translate the plan into specific actions that orient them to their environment and other units when executing the mission. They also imprint a mental picture of the sequence of key actions within the operation and provide a forum for subordinate and supporting leaders and units to coordinate.

Communications

4-27. Staff and leaders must work closely with the G-6/S-6 to coordinate for the required communication links. The unit may require classified and unclassified network connections for their equipment. If elements of the unit 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 as well as the latest fills and frequencies. They must possess and be familiar with all the instructions, passwords, policies, regulations, and directives conducive to OPSEC. They must also ensure Soldiers are trained in the use and procedures involved in operating communications equipment. The G-2/S-2 must verify the frequencies, alternate frequencies, and reactions during jamming, as well as the latest time information is of value (LTIOV) for specific information to be reported.

Situation Updates

4-28. Staff preparation includes assembling and continuously updating estimates. For example, continuous IPB provides accurate situational updates for commanders. The G-2/S-2 operations team uses the DCGS-A enterprise and automated tools to continuously integrate information and intelligence products from subordinate G-2/S-2s and supporting ISR organizations to update the threat situation, terrain and weather, and civil considerations.

Intelligence Handoff

4-29. Intelligence handoff may occur in three primary situations: Intelligence handoff when handing over a mission (during relief in place/transition of authority), when handing off targets, or when handing off technical channels for intelligence assets. A well-prepared intelligence handoff will ensure a smooth and seamless transition between units. It is important that the receiving unit becomes familiar with the operation, target, or technical channels requirements as soon as possible to avoid compromising the intelligence production and flow of the mission. The following are points to consider during an intelligence handoff:

- Briefings and reports (learn what briefings are required and when, as well as report formats and requirements—to include technical requirements).
- Past, present, and planned activities within the area of influence.
- Established SOPs (know procedures for reporting; intelligence contingency funds and incentive use if applicable; emplacement and use of ISR equipment).
- Key personalities (introductions are required; establish rapport and a good working relationship with all key personalities).
- Key personnel on the base or camp (their responsibilities; how to contact them).
- Key personnel in other US and multinational service components (coordinate for exchange of information and intelligence).
- Key personalities from surrounding towns (local figures).
- Key national level political and military figures.
- Supporting units (know where to go for sustainment, information, or assistance and POCs within those organizations).
- Current attitudes (understand current attitudes and perspectives of the local populace).
- Equipment operation and idiosyncrasies (equipment may run on different applications; personnel may need to train on specific equipment and procedures).
- Area familiarization (identify NAIs, key terrain, minefields, and boundaries; know camp locations, routes and route names, checkpoints, and towns).
- Handover of databases; for example, analytical, intelligence discipline databases, source registry, technical channels, and POCs.
- Close coordination for cross-boundary target handoff ; for example, complete target information (when not handing off a formal target package) on a target which conducts cross-boundary operations.
- The specific aspects of technical channels.

Rules of Engagement

4-30. Although ROE training was presented during the plan step of the intelligence process, leaders at all levels can take the opportunity during the prepare step to ensure their subordinates completely understand the ROE. During this step commanders may need to consider exceptions to, or modifications of, the ROE to facilitate HUMINT and CI collection or to enable the placement of ISR assets.

COLLECT

4-31. The G-2/S-2 and G-3/S-3 play a critical role in this challenging step because intelligence drives operations. Elements of all units in the AO obtain information and data about the threat, terrain and weather, and civil considerations in the AO. Well-developed procedures and carefully planned flexibility to support emerging targets, changing requirements, and the need to support combat assessment is critical. Once the information has been collected, it must be processed into a form that enables analysts to extract essential information and produce intelligence and targeting data. Collected and processed information must then be reported to the appropriate units, organizations, or agencies for analysis or action.

ISR Tasks and Other Intelligence-Related Tasks

4-32. ISR synchronization and integration results in an effort focused on answering the CCIR through ISR tasks translated into orders. ISR assets must be focused properly to collect the knowledge the commander needs at the right time in order to achieve mission success. Successful ISR operations allow commanders to engage the threat through knowledge rather than assumptions.

4-33. Intelligence tasks are included in annex B of the OPORD under Scheme of Intelligence. They include the following:

- **Intelligence Production**. Intelligence production includes analyzing information and intelligence and presenting intelligence products, conclusions, or projections regarding the operational environment and enemy forces in a format that enables the commander to achieve situational understanding.
- **Request for Information.** Submitting an RFI to the next higher headquarters or adjacent units is the normal procedure for obtaining intelligence information not available through the use of available ISR assets. Users enter RFIs into an RFI management system where every other user of that system can see it. Hence, an echelon several echelons above the actual requester becomes aware of the request and may be able to answer it. A G-2/S-2 who receives an RFI from a subordinate element may use intelligence reach to answer RFIs.
- **Intelligence Reach**. Intelligence reach allows the commander to access the resources of national, joint, foreign, and other military organizations and units. Requestors can acquire information through push and pull of information, databases, homepages, collaborative tools, and broadcast services. Intelligence reach also supports distributed analysis. (See chapter 2 for more information on intelligence reach.)

4-34. For information on surveillance and reconnaissance tasks, refer to FM 3-55 (when published) and FM 7-15 (when published).

Special Reconnaissance

4-35. Special reconnaissance is the complementing of national and theater intelligence collection assets and systems by obtaining specific, well-defined, and time-sensitive information of strategic or operational significance. It may complement other collection methods where there are constraints of weather, terrain, hostile countermeasures, and/or other systems availability. Special reconnaissance places US or US-controlled personnel conducting direct observation in hostile, denied, or politically sensitive territory when authorized. SOF may conduct these missions unilaterally or in support of conventional operations. (See JP 3-05.)

4-36. Army Special Operations Forces elements conduct special reconnaissance missions to obtain information not available through other means. Special reconnaissance operations encompass a broad range of collection activities to include surveillance, reconnaissance, and target acquisition. Special reconnaissance missions provide intelligence or information that is often not available through other means. Typical special reconnaissance missions include—

- Surveillance and target acquisition of hostile C2 systems, troop concentrations, deep-strike weapons, lines of communication, CBRNE capabilities, and other targets.
- Location and surveillance of hostage, enemy prisoner of war (EPW), or political prisoner detention facilities.
- Post-strike reconnaissance for BDA.
- Meteorologic, geographic, or hydrographic reconnaissance to support specific air, land, or sea operations.

4-37. For more information on special reconnaissance, see FM 3-05.102.

Process

4-38. Processing converts relevant information into a form suitable for analysis, production, or immediate use by the commander. Processing includes sorting through large amounts of collected information and intelligence (multidiscipline reports from the unit's ISR assets, adjacent and higher echelon units and organizations, and non-MI elements in the AO). Processing identifies and exploits that information which is pertinent to the commander's intelligence requirements and facilitates situational understanding. Examples of processing include enhancing imagery, translating a document from a foreign language, converting electronic data into a standardized report that can be analyzed by a system operator, and correlating dissimilar or jumbled information by assembling like elements before the information is forwarded for analysis.

4-39. Often collection assets must collect and process their data prior to disseminating it. MI systems have their own reporting and processing systems, the details of which are in the appropriate MI system manuals and technical manuals. Some collection assets, particularly air reconnaissance and ground scouts, can report relevant information that is immediately usable by the tactical commander (for example, for targeting purposes). However, the personnel in the reporting chain still process these reports by evaluating their relevancy and accuracy. In many cases, the output of a collection asset is data, or information of limited immediate use to a commander.

4-40. The intelligence staff processes information collected by the unit's assets as well as that received from higher echelons. Through intelligence reach, the intelligence staff processes many types of information and data from all of the intelligence disciplines and from both the unit's ISR assets and from ISR assets outside the unit.

Reporting

4-41. The most critical information collected is worthless if not reported in a timely manner. Collectors may report information via verbal, written, graphic, or electronic means. Unit SOPs must clearly state the transmission means of different types of reports (for example, sent by satellite communications, FM radios, or by automated means). In general, the transmission of reports for threat contact and actions, CCIRs, exceptional information, and CBRNE reports is by voice FM, and then followed up with automated reports.

4-42. Commanders and staffs must remember that timely reporting, especially of threat activity, is critical in fast-moving operations. Collectors must report accurate information as quickly as possible. Commanders and staff must not delay reports for the sole purpose of editing and ensuring the correct format. This is particularly true for reporting information or intelligence that answers the CCIR.

4-43. The G-2/S-2 coordinates with the unit staff, subordinate and lateral commands, and higher echelon units to ensure that specific reporting assets, personnel, equipment (especially communications), and procedures are in place. The G-2/S-2 requests or establishes the appropriate message addresses, routing indicators, mailing addresses, and special security office security accreditation for units.

Time-Sensitive Reporting

4-44. Intelligence and time-sensitive combat information that affects the current operation is 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 intelligence in time to satisfy the user's intelligence requirements. The routing of combat information proceeds immediately in two directions: directly to the commander and through routine reporting channels, which include intelligence analysis and production elements. Time-sensitive information usually includes reports concerning threat contact and actions and CCIRs.

PRODUCE

4-45. In the production task, the G-2/S-2 integrates evaluated, analyzed, and interpreted information from single or multiple sources and disciplines into finished intelligence products. Like collection operations, the G-2/S-2 must ensure the unit's information processing and intelligence production are prioritized and synchronized to support answering the CCIRs (PIRs and FFIRs).

4-46. Intelligence products must be timely, relevant, accurate, predictive, and tailored. The accuracy and detail of every intelligence product has a direct effect on how well the unit conducts operations. However, the G-2/S-2 and unit must use intelligence (no matter what form the intelligence is in) that meets the requirements but might not be as detailed or refined as possible. A good answer on time is better than a more refined answer that is late.

4-47. The G-2/S-2 produces intelligence for the commander as part of a collaborative process. The commander drives the G-2/S-2's intelligence production effort by establishing intelligence and information requirements with clearly defined goals and criteria. Differing unit missions and operational environments dictate numerous and varied production requirements on the G-2/S-2 and staff. Through the ISR synchronization matrix the G-2/S-2 synchronizes the information, intelligence, and PIRs with the operational timeline.

4-48. The G-2/S-2 must employ collaborative analysis techniques and procedures that leverage intelligence production capability of higher and subordinate echelons to meet these requirements. Proficiency in these techniques and procedures enables the G-2/S-2 to answer the commander's and staff's requirements regardless of the mission, environment, and situation. The G-2/S-2 and staff intelligence products enable the commander to—

- Plan operations and employ maneuver forces effectively.
- Recognize potential COAs.
- Conduct mission preparation.
- Employ effective TTP.
- Take appropriate security measures.
- Focus ISR.
- Conduct effective targeting.
- Conduct assessment of intelligence and operations.

INTELLIGENCE PROCESS CONTINUING ACTIVITIES

4-49. The three continuing activities drive, shape, and develop the intelligence process. They can occur at any time during the process and help to focus and refine both the process and the intelligence products that result.

Analyze

4-50. Analysis occurs at various stages throughout the intelligence process. Leaders at all levels conduct analysis to assist in making many types of decisions. An example is a HUMINT collector's analyzing an

intelligence requirement in order to determine the best possible collection strategy to use against a specific source.

4-51. Analysis in requirements management is critical to ensuring the information requirements receive the appropriate priority for collection. The intelligence staff analyzes each requirement—

- To determine its feasibility, whether or not it supports the commander's intent.
- To determine the best method of satisfying the information requirements.
- To determine if the collected information satisfies requirements.

4-52. During the produce task, the intelligence staff analyzes information from multiple sources to develop all-source intelligence products. The intelligence staff analyzes information and intelligence to ensure the focus, prioritization, and synchronization of the unit's intelligence production is in accordance with the PIRs.

4-53. In situation development, the intelligence staff analyzes information to determine its significance relative to predicted threat COAs and the CCIRs (PIRs and FFIRs). Through predictive analysis, the staff attempts to identify enemy activity or trends that represent opportunities or risks to the friendly force. They use the indicators developed for each threat COA and CCIRs (PIRs and FFIRs) during the MDMP as the basis for their analysis and conclusions.

Assess

4-54. *Assessment is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation* (FM 3-0). Assessment plays an integral role in all aspects of the intelligence process. Assessing the situation and available information begins upon receipt of the mission and continues throughout the intelligence process. The continual assessment of intelligence operations and ISR assets, available information and intelligence, the various aspects of the AO, are critical to—

- Ensure the CCIRs (PIRs and FFIRs) 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 enemy efforts at deception and denial.

4-55. During planning, the intelligence staff conducts a quick initial assessment of the unit's intelligence posture and holdings, status of intelligence estimates, and any other available intelligence products. From this assessment the commander issues his initial guidance and a WARNO.

4-56. During execution the intelligence staff continues assessing the effectiveness of the ISR effort while at the same time assessing the results and products derived from the ISR synchronization effort. The critical aspects of assessment include determining whether—

- The CCIRs have been answered.
- The CCIRs are still likely to be answered with the current ISR operations.
- ISR operations account for changes to the CCIR.
- ISR operations account for changes to the operational environment.
- Some ISR operations must be adjusted in order to answer the CCIRs.

4-57. This type of assessment requires sound judgment and a thorough knowledge of friendly military operations, characteristics of the AO and AOI, and the threat situation, doctrine, patterns, and projected COAs.

Propagate

4-58. Successful operations at all levels require increased demands on the intelligence warfighting function. Timely and accurate dissemination of intelligence is key to the success of operations. Commanders must receive combat information and intelligence products in time and in an appropriate format to support decision making. Additionally, sharing the most current all-source information and intelligence at all echelons is essential for commanders to maintain situational understanding. The DCGS-A enterprise is the primary method for providing intelligence products to users.

4-59. To achieve this, the commander and staff must establish and support a seamless intelligence architecture—including an effective dissemination plan—across all echelons to ensure information and intelligence flow efficiently to all those who need them. 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 these systems and how they contribute to the intelligence warfighting function.

Dissemination

4-60. A dissemination plan can be a separate product, or integrated into existing products such as the ISR synchronization plan or intelligence synchronization matrix, the decision support template, or decision support matrix.

- **Dissemination Methods and Techniques.** 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. Possible dissemination methods and techniques include direct electronic dissemination (a messaging program); dissemination via chat rooms; instant messaging; web posting; printing the information and sending it via courier; or putting the information on a compact disc and sending it to the recipient. G-2/S-2s must plan methods and techniques to disseminate information and intelligence when the normal methods and techniques are unavailable. For example, information and intelligence can be disseminated using LNOs or regularly scheduled logpacks.

Note. When posting information to a website, the intended recipients must be notified when new or critical information has been posted; simply posting information to a website does not ensure that the intended user has received it.

- **Dissemination Procedures.** The G-2/S-2 and intelligence personnel at all levels assess the dissemination of intelligence and intelligence products. Disseminating intelligence simultaneously to multiple recipients is one of the most effective, efficient, and timely methods. This can be accomplished through various means; for example, push, broadcast. However, within the current tactical intelligence architecture, reports and other intelligence products move along specific channels. 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 Channel.** The command channel is the direct chain-of-command link that commanders, or authorized staff officers, use for command-related activities. Command channels include command radio nets, video teleconferences, and the Maneuver Control System.
  - **Staff Channel.** The staff channel is the staff-to-staff link within and between headquarters. The staff uses the staff channel for control-related activities. Through the staff channel, the staff coordinates and transmits intelligence, controlling instructions, planning information, and provides early warning information and other information to support C2. Examples of

staff channels include the operations and intelligence radio net, telephone, the staff huddle, video teleconference, and the warfighting function-specific components of DCGS-A to provide information and intelligence to the rest of the intelligence architecture.

- **Technical Channels.** Staffs typically use technical channels to control specific activities. These activities include fire direction and the technical support and SCI reporting channels of intelligence and ISR operations. The SIGINT tasking and reporting radio net, intelligence broadcast communications, and the wide area networks supporting single intelligence discipline collection, processing, and production are examples of technical channels.

- **Presentation Techniques and Procedures.** The staff's objective in presenting information is to provide the commander with relevant information. The presentation method is based on the commander's guidance. Table 4-1 lists the three general methods that the staff uses to present information and meet its information objective. Specific techniques include METT-TC, PMESII, and PMESII-PT. DCGS-A contains standard report formats, maps, and mapping tools that assist the staff in presenting information in written, verbal, and graphic form. Audio and video systems, such as large format displays and teleconferencing systems, enable the staff to use a combination of the methods in multimedia presentations.

Table 4-1. Presentation methods and products

Method	***Products***
Written Narrative	Reports, Estimates, and Studies
Verbal Narrative	Briefings (information, decision, mission, and staff)
Graphic	Charts, Overlays, and Electronic Displays

Intelligence Communications Architecture

4-61. The intelligence communications architecture transmits intelligence and information to and from various ISR elements, units, and agencies by means of automation and communication systems. The DCGS-A enterprise is the primary method for providing intelligence products to users. With the continued development of sensors, processors, and communications systems, it is increasingly important to understand the requirements of establishing effective communications architecture. The G-2/S-2 must identify the specific intelligence warfighting function requirements of the unit's overall communications architecture. Refer to FM 2-33.5 for more information on intelligence reach.

4-62. The following are some (but not all) of the questions which the staff must answer in order to establish the intelligence communications architecture:

- Where are the unit's collectors?
- What and where are the unit's processors?
- Where are the unit's intelligence production elements?
- Where are the unit's decision makers?
- How does the unit disseminate information from its producers to its decision makers and/or consumers?
- Are the systems which the unit's collectors, producers, processors, and consumers use compatible with each other? If not, what is the plan to overcome this challenge?
- How can the unit access databases and information from higher and other agencies? Are there special requirements necessary to access these databases such as security clearance, polygraph, training, and certification?

Knowledge Management

4-63. 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 with either extraneous or too much information. The G-2/S-2 must also ensure that users do not receive the same information from the same source multiple times. Circular reporting could result in erroneous analysis by intelligence personnel or unsubstantiated decisions by commanders.

Granting Access

Sharing

Posting

Intelligence Reach

4-64. Intelligence reach is an important part of the intelligence effort. Intelligence reach allows intelligence analysts to retrieve existing information, intelligence products, and data which can support answering the CCIRs from outside the unit in a timely manner without having to wait for an answer to an RFI or an ISR task. The information, intelligence products, or data retrieved can then be evaluated for use in the unit's intelligence products or analysis.

Updating the COP

Commander's Input

4-65. Commander's input is provided at the commander's discretion. Commander's input is the key element in focusing the intelligence effort. This input directly influences the focus of the unit's ISR effort, the intelligence collection assets, and the intelligence analysis resources. It also determines which intelligence products are developed, as well as the format of the products.

PART THREE

Military Intelligence Disciplines

Part Three provides a more detailed explanation of the intelligence disciplines introduced in Part One of this manual.

Chapter 5 defines and discusses the role and fundamentals of the All-source Intelligence discipline.

Chapter 6 defines and discusses the role and fundamentals of the Counterintelligence discipline.

Chapter 7 defines and discusses the role and fundamentals of the Human Intelligence discipline.

Chapter 8 discusses the Geospatial intelligence discipline and its role in Army operations.

Chapter 9 defines and discusses the role and fundamentals of the Imagery Intelligence discipline.

Chapter 10 defines and discusses the role and fundamentals of the Measurement and Signature Intelligence discipline.

Chapter 11 defines and discusses the role and fundamentals of the Open-Source Intelligence discipline.

Chapter 12 defines and discusses the role and fundamentals of the Signals Intelligence discipline.

Chapter 13 defines and discusses the role and fundamentals of the Technical Intelligence discipline.

Chapter 5

All-Source Intelligence

DEFINITION

5-1. All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the function used to produce intelligence from multiple intelligence or information sources.

5-2. Army units plan and conduct operations based off the all-source intelligence assessment developed by the intelligence section. The all-source intelligence assessment is expressed as part of the intelligence running estimate.

5-3. All-source intelligence operations are continuous and occur throughout the operations process and the intelligence process. Most of the products resulting from all-source intelligence are initially developed during planning and updated as needed during operations.

ROLE

5-4. The operational environment provides an ever-growing volume of data and information available from numerous sources, from which the commander can use to achieve situational understanding. Situational understanding enables the commander to—

- Make decisions in order to influence the outcome of the operation.
- Prioritize and allocate resources.
- Assess and take risks.
- Understand the needs of the higher and subordinate commanders.

5-5. The commander depends upon a skilled G-2/S-2 working within the commander's intent to provide sound IPB, support the commander's ISR effort and provide all-source intelligence analysis, conclusions, and projections of future conditions or events.

FUNDAMENTALS

5-6. *Intelligence is the product resulting from 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. This term is also applied to activity which results in the product and to the organizations engaged in such activity* (JP 2-0). Using information from all available sources, all-source analysts conduct analysis and produce timely, relevant, accurate, predictive, and tailored intelligence that satisfies the commander's requirements. All-source analysis provides an overall picture of the enemy, terrain and weather, and civil considerations. Thorough all-source analysis reduces the possibility of error, bias, and misinformation through the consideration of multiple sources of information and intelligence.

PLANNING

5-7. During each step of the MDMP the intelligence staff is responsible for providing well-defined, specific all-source intelligence products and tools. These are the "deliverables" expected and required by the commander and staff during the planning process:

- Enemy threat characteristics.
- Enemy situation templates and COA statements.
- Event template and event matrix.
- HPT list (HPTL).
- Weather effects matrix.
- Modified combined obstacle overlay (MCOO) and terrain effects matrix.
- Civil Consideration (ASCOPE) IPB overlays.

MISSION ANALYSIS

5-8. A thorough mission analysis is crucial to planning. Both the process and products of mission analysis help commanders refine their situational understanding and determine their mission. Accurate situational understanding enables them to better visualize the operation. There are 17 separate tasks associated with

mission analysis that depend on all-source intelligence operations. Generally, the intelligence portion of mission analysis is an evaluation of the following battlefield effects: threat, terrain, weather, and civil considerations (ASCOPE). 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 effect ISR operations. Endstate is the development of an initial ISR plan, the refinement of the commander's estimate based on a clear understanding of the situation, and the staff refining staff running estimates based on that same understanding. To avoid misunderstanding and ensure there is a clear and common understanding of what is fact and what is assumption at this point, the all-source analyst must tell the commander and staff "what he knows and why he knows it, what he thinks and why he thinks it, what he does not know and what he is doing about it". This promotes critical thinking and generates the staff discussion required to formulate sound courses of action.

5-9. Task 1: Analyze Higher Headquarters Order. The intelligence staff analyzes the higher headquarters' order to determine how that commander and intelligence view the enemy. In order to provide the best possible support to the commander and minimize the amount of time needed to complete products, the intelligence staff conducts parallel and collaborative planning with the higher headquarters intelligence staff as that staff completes its planning.

5-10. Task 2: Perform Initial Intelligence Preparation of the Battlefield (IPB). The intelligence officer leads the staff though the IBP process. The other staff sections assist the intelligence section in developing the IBP products required for planning. IPB starts during mission analysis, is refined during the rest of the MDMP, and continues during the preparation and execution of operations. It consists of four steps: define the operational environment, describe environmental effects on operations, evaluate the threat, and determine threat courses of action. The major results of initial IPB are terrain and geospatial products developed as a result of examining the physical and human characteristics of the area of operations, enemy situational overlays, enemy event templates and matrices, high value target lists, the identification of intelligence gaps that the commander uses to establish initial information requirements, and an initial ISR plan.

- Evaluate Military aspects of the Terrain. Utilizing the topographic (TOPO) team, analysts conduct a detailed terrain analysis of the area of operations focused on natural and man-made features that may effect operations. Using the OAKOC model (Observation and Fields of Fire, Avenues of Approach, Key Terrain, Obstacles, Cover & Concealment), the analyst briefs the commander and staff on the effects the terrain may have on both friendly and enemy forces. The analyst also briefs what effect the weather will have on terrain. The general product resulting from terrain analysis is the Modified Combined Obstacle Overlay (MCOO). See FM 2-01.3 for a detailed explanation of terrain analysis and the other standard products developed as a result of it.
- Evaluate Civil Considerations (ASCOPE) Analysis. ASCOPE is an acronym for area, structures, capabilities, organizations, people, and events. These are the broad categories the Army uses to analyze and describe the civil considerations that may have an effect on operations. Using the ASCOPE model, the analyst briefs the commander and staff on the effects urban centers may have on friendly and enemy forces. There is no standard product resulting from this analysis. The G2/S-2 generally briefs a series of products developed based on the situation. See FM 2-01.3 and FM 3-06 for a detailed explanation of ASCOPE analysis and the standard products developed as a result of it.
- Evaluate Weather Conditions and Effects. The USAF weather team assigned to the intelligence section provides weather forecasting and analysis under the direction of the intelligence officer. Using the Integrated Weather Effects Decision Aid (IWEDA) function in the Integrated Meteorological System (IMETS) program, the intelligence section briefs the commander and staff on the weather forecast and how it will affect warfighting functions in general as well as personnel and equipment specifically. See FM 2-01.3 for a detailed explanation of weather analysis.

- Develop Enemy threat characteristics. In order to accurately depict how an enemy commander will dispose and maneuver forces on the battlefield an analyst must understand how the enemy is organized and equipped, what the enemy's capabilities are, and how the enemy has employed forces in the past. An understanding of threat characteristics and detailed organizational charts assist in this analysis. This also helps identify what signatures the enemy gives off that can be collected by friendly ISR assets. Maintaining accurate threat characteristics is also essential in conducting combat assessment. This applies to regular and irregular forces as well as insurgent and terrorist organizations. Threat characteristics for conventional forces are generally available within the intelligence community. The analyst will generally have to develop threat characteristics for emerging threats like terrorists and insurgents. This is done by using information gained from national and theater intelligence organizations as well as from the publications of these types of threat groups.
- Develop Enemy Situation Templates (ENSITEMP). Depending on the mission, there are three types of ENSITEMPs generally required for planning. The first two are used in conventional operations; showing the enemy conducting offensive and defensive operations against friendly forces. The third is used in unconventional operations; showing non-conventional forces conducting operations against friendly forces in complex terrain such as an urban area. Each of these overlays is a graphic depiction of the accompanying enemy COA statement. Together, they communicate the enemy's disposition, objectives, goals and endstate, main and shaping efforts, and how the enemy will maneuver. Additionally, these products graphically and textually explain the enemy's intent for fires, ISR, IO, and logistics. Finally, they explain the enemy's failure options and a recommendation on how to defeat the enemy. Both the overlay and statement are included in the mission analysis briefing. Depending on the mission, the analyst will generally develop more than one ENSITEMP to articulate other possible enemy COAs.
- Identify High Value Target List (HVTL). Every ENSITEMP and ECOA statement is accompanied by an HVTL that describes and prioritizes in terms of their relative worth those assets that the enemy commander requires for to achieve stated objectives. The analyst develops the HVTL in coordination with the rest of the staff.
- Develop an Event Template and Matrix. Developed as the basis for the decision support template (DST) and the ISR overlay, this tool assists in the identification of the commander's decision points and in determining ISR strategies. It ensures a consistent and well reasoned portrayal of enemy capabilities throughout the planning process. It is critical in tying ISR and maneuver together as well as assisting in the development of a plan that allows the commander to get inside the enemy's decision cycle. The event template and matrix are not briefed during mission analysis but they must be ready for COA development.

5-11. Task 3: Determine Specified, Implied, and Essential Tasks. The analyst analyzes the higher headquarters order to identify the specified ISR tasks that have been assigned to the unit and develop any implied tasks that must be performed to accomplish stated specified tasks. The analyst then provides a list of specified and implied tasks to the operations section and assists in determining essential tasks for inclusion in the unit's mission statement.

5-12. Task 4: Review Available Assets. The analyst reviews the status of the unit's ISR 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 analyst then determines if the unit has the assets it needs to accomplish all collection tasks. If there are shortages, the intelligence section identifies them and makes recommendations for additional resources.

5-13. Task 5: Determine Constraints. A higher commander normally places some constraints on subordinate commanders. Constraints are restrictions placed on the command by a higher command. They dictate an action or inaction, thus restricting the freedom of action a subordinate commander has for planning. A typical constraint for ISR operations is establishing a limit of advance for air or ground reconnaissance. Constraints are normally contained in the scheme of maneuver, paragraph, concept of

operations paragraph, or coordinating instructions paragraph in the base order. However, they are sometimes stated in the annexes to the order as well.

5-14. Task 6: Identify Critical Facts and Assumptions. Along with the rest of the staff members, the intelligence analyst is responsible for gathering two categories of information concerning assigned tasks; facts and assumptions.

5-15. Task 7: Perform Risk Assessment. This task is performed by the operations section with assistance from the rest of the staff. See FM 5.0 and FM 100-14 for an explanation of risk assessment.

5-16. Task 8: Determine Initial Commander's Critical information Requirements (CCIR) and Essential Elements of Friendly Information (EEFI). Determine initial information requirements. This is the first step in developing a collection plan. PIR are not developed by the staff until COA analysis and are not approved by the commander until COA approval. In the mission analysis briefing, after stating "what he knows, what he thinks he knows, and what he does not know" the analsyt recommends what information the intelligence section should be collecting and analyzing in support of continued planning and COA development. Identifying information requirements at this time helps the commander filter information available by defining what is important to mission accomplishment. It also helps to focus the efforts of the rest of the staff and subordinate commands.

5-17. Task 9: Determine the Initial ISR Plan. The operations section is the staff proponent of the ISR plan. It is an integrated staff product executed by the unit at the direction of the commander. The operations officer, assisted by the intelligence section, uses the ISR plan to task and direct available ISR assets to answer CCIR (PIR and FFIR) and other intelligence requirements. The intelligence section must have its input and products ready to be published as part of the Warning Order that the S-3 issues at the conclusion of mission analysis.

5-18. Task 10: Update the Operational Timeline. Using the enemy operational timeline 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 enemy vulnerability or times when the unit may be at risk from enemy activity.

5-19. Task 11: Write the Restated Mission. The unit chief of staff or executive officer normally drafts a recommended mission statement based on the staff's mission analysis and presents it for approval to the commander at the conclusion of the mission analysis briefing. The intelligence section has already provided input for the restated mission during task three and normally has no further input at this time.

5-20. Task 12: Deliver a Mission Analysis Briefing. Time permitting, the staff briefs the commander on its mission analysis using the outline provided in FM 5.0. The intelligence analyst is responsible for briefing the initial IBP products developed for threat, terrain, weather, and civil considerations (ASCOPE). The analyst may also brief the initial ISR plan if the unit is in a position to begin collection operations. The mission analysis briefing is a decision briefing that results in an approved restated mission, commander's intent, and commander's planning guidance. The analyst, presents only that relevant information the commander needs to develop situational understanding and formulate planning guidance.

5-21. Task 13: Approve the Restated Mission. Immediately after the mission analysis briefing the commander approves a restated mission. Once approved, the restated mission becomes the unit mission. The analyst has no role in this task.

5-22. Task 14: Develop the Initial Commander's Intent. The intelligence section is generally concerned with commander's intent as it applies to all warfighting functions. However, as the staff proponent, the intelligence analyst is most concerned with the intelligence warfighting function and what the commander's intent is for ISR. Given that, the analyst advises the commander on commander's intent for ISR. The analyst makes that recommendation informally prior to the mission analysis briefing or at the conclusion of the intelligence portion of the briefing. The commander considers this recommendation prior to formulating his intent.

5-23. Task 15: Issue the Commander's Planning Guidance. The commander issues his planning guidance after the mission analysis briefing and before the start of course of action development. The analyst has no role in this task unless asked for additional input from the commander.

5-24. Task 16. Issue a Warning Order. Immediately after the commander gives planning guidance the operations officer issues a warning order. At a minimum, the intelligence section input into this order is the enemy situation paragraph, priority of intelligence collection, priority of intelligence support, intelligence tasks to subordinate units, and PIR. Additionally, if initial IPB products have not yet been made available to higher headquarters and subordinate commands they should be issued with the warning order.

5-25. Task 17. During the rest of the MDMP, the commander and staff periodically review all facts and assumptions. New facts may alter requirements and require a re-analysis of the mission. Assumptions may have become facts or may have even become invalid. Whenever the 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 CCIR, if necessary.

COURSE OF ACTION (COA) DEVELOPMENT

5-26. . The purpose of COA development is to update staff running estimates and prepare COA options for the commanders consideration.. The staff develops friendly COAs based on facts and assumptions identified during IPB and mission analysis. Incorporating the results of IPB into COA development ensures that each friendly COA takes advantage of the opportunities the environment and threat situation offer. The intelligence analyst works closely with the operations section and the rest of the staff to analyze relative combat power and develop friendly COAs that can defeat enemy operations. All friendly COAs are developed off the enemy situation template and enemy event template/matrix the analyst produced during mission analysis. At the conclusion of COA development the intelligence section has completed draft information requirements for each friendly COA as well as a draft ISR overlay and synchronization matrix in preparation for COA analysis.

COA ANALYSIS (WARGAMING)

5-27. . COA Analysis is a disciplined process that includes rules and steps followed in sequence. It relies heavily on an understanding of doctrine, tactical judgment, and experience. Each staff member participating must come prepared with the full knowledgeable of the warfighting function represented. The intelligence analyst has two areas of responsibility in the wargame; role-play the enemy commander and act as the ISR officer. First, as the enemy commander, using the enemy situation template as a start-point and the event template/matrix as a guide, the analyst develops critical enemy decision points in relation to friendly COAs, projects enemy reactions to friendly actions, and projects enemy losses. Second, as the ISR officer, the analyst identifies new information requirements, assists the staff in developing PIR, refines the situation and event templates, develops the ISR overlay and synchronization matrix, and assists in the development of the High payoff targets and the decision support template (DST). At the conclusion of the wargame, pending COA approval by the commander, every intelligence product that must be published with the order is complete.

COA APPROVAL

5-28. . At the conclusion of the wargame the staff identifies its preferred COA and makes a recommendation to the commander. This is the COA decision briefing. During this briefing the analyst will brief any changes to the current enemy situation and any environmental factors that have changed since the commander was last briefed.

ORDERS PRODUCTION

5-29. . The staff led by the operations prepares the order by turning the selected COA into a clear, concise concept of operations and supporting information. The order provides all the information subordinate

commands need to plan and execute their operations. However, this is not the first time subordinate commanders and their intelligence staffs have seen this data. As stated previously, within the parallel and collaborative planning process, intelligence analysts at all echelons have been involved in the orders process; reviewing each other's intelligence products as they were developed and, at this point, are clarifying changes and submitting requests for additional information and product support. Prior to the order being issues the intelligence section will conduct an orders crosswalk with the rest of the staff as directed by the brigade operations officer.

RUNNING ESTIMATE, INTELLIGENCE RUNNING ESTIMATE AND THE COP

5-30. A running estimate is a staff section's continuous assessment of current and future operations to determine if the current operation is proceeding according to the commander's intent and if future operations are supportable. (FM 3-0) Running estimates provide information, conclusions, and recommendations from the perspective of each staff section. They serve as a staff technique to support the commander's visualization and decision making, as well as the staff's tool for assessing during preparation and execution. In the running estimate, staff officers continuously update their conclusions and recommendations as they evaluate the impact of new facts.

5-31. Each staff section produces a running estimate. The main difference between the running estimate and the old staff estimates is the emphasis on not only continuously updating the facts of the estimate but also continuously updating the conclusions and recommendations while including projections of future conditions of the entire AO.

5-32. Current doctrine emphasizes the COP as the primary tool that provides the commander a visualization of the current situation. All staff sections provide their respective input to the COP.

5-33. The portion of the COP that depicts the threat situation 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. DCGS-A will be the means for integrating this information into the COP.

5-34. While the COP is primarily a display of current intelligence and information, the running estimate requires the merging of the staff's cognitive processes with automation applications. The primary focus of the staff's cognitive process is to present predictive or anticipatory intelligence in support of the commander's decision making or situational understanding. The running estimate integrates the running estimates from each staff section. The intelligence staff's input to the running estimate is the intelligence running estimate. Training is required (not just within MI) in order to successfully build and maintain the staff's running estimate and COP integration.

5-35. The intelligence running estimate is a continuous flow and presentation of relevant information and predictive intelligence that, when combined with the other staff running estimates, enables the commander's visualization and situational understanding of the AOI in order to achieve information superiority. The intelligence running estimate requires constant verification to support situational understanding of the current situation as well as predictive assessments for future operations.

5-36. The intelligence staff's running estimate details the ability of the intelligence staff to support operations. It focuses analysis and detects potential effects on operations. It supports the commander's visualization throughout the operation. The intelligence running estimate provides a fluid and current picture based on current intelligence products and reports and predictive estimates of future threat activity. The intelligence running estimate consists of all of the continuously updated and monitored intelligence that is available but that is then filtered to provide the specific intelligence relevant to current and projected future operations.

5-37. The intelligence running estimate is initially developed after the generating knowledge step of the intelligence process. The intelligence running estimate is then refined and improved following mission analysis. It is further refined and improved based on the results of ISR operations. It is updated as required

upon changes in the enemy situation, terrain, weather and civil considerations. The intelligence running estimate includes—

- Mission
- Area of Operations
- Enemy/Threat situation
- Enemy/Threat capabilities
- Conclusions

5-38. The G-2/S-2 must clearly understand the weather and terrain effects and the G-2/S-2 must be able to visualize the AO before producing the intelligence staff's running estimate. This understanding facilitates accurate assessments and projections regarding the threat; the threat situation (including strengths and weaknesses); threat capabilities and an analysis of those capabilities (COAs available to the threat); and conclusions drawn from that analysis. The estimate details threat characteristics into threat capabilities and projections of future threat actions.

OPERATIONS

5-39. Successful ISR operations depend of timely, relevant, and well-reasoned all-source analysis. Successful ISR operations are not based on advanced technology or intelligence reach. By themselves, the Army's array of collection systems, intelligence processors, and network advantages will not ensure the commander's information requirements are satisfied. These are just tools that, if used correctly, can enhance a unit's ability to answer questions in a timely manner.

5-40. The key to successful ISR operations is an ISR plan that:

- ***Is developed from well-reasoned enemy situation overlays, course of action statements, and event templates/matrices.***
- Is driven by the commander's CCIR and is focused on command directed tasks.
- Is tied to the commander's decisions (decision points) or actions (lines of operation).
- Facilitates the commander's visualization of his area of operations.
- Is prepared jointly by the intelligence section, and the rest of the staff.
- Remains synchronized with the scheme of maneuver.
- Is issued and updated as part of the orders process.
- Assigns appropriate collection tasks to subordinate units.
- Requests intelligence support as needed from higher and adjacent units.

5-41. Develop Requirements (Requirements Management). Requirements management is the responsibility of the all-source analysis / fusion section. Requirements management is the process of identifying, prioritizing, and refining gaps in data, relevant information, and knowledge concerning the operational environment that must be resolved in order for the commander to achieve situational understanding. Requirements are developed prior to conducting an operation and during on-going operations. An important element in developing requirements is constant collaboration between all warfighting functions as well as between the analysis and collection management cells to redefine information requirements and focus the ISR effort as the situation develops.

5-42. While the rest of the staff contributes to this effort, the analysis cell is the primary element responsible for developing requirements during planning and steady-state operations. Using the commander's current stated requirements, the brigade mission statement, input from the brigade staff, and input from higher headquarters the analysis cell indentifies intelligence gaps and forwards them to the intelligence officer and operations officer for consideration as PIR and collection requirements. Because the ISR synchronization process is continuous and non-sequential, requirements are developed throughout the process and at all stages or phases of operational planning, preparation, and execution.

5-43. The endstate of requirements development is to produce new intelligence requirements that are developed from ongoing operations that will drive new operations, branches and sequels. Effective requirements management depends on detailed IPB; including the maintenance of the intelligence running estimate, to include enemy situation templates/course of action statements as well as the development of event templates/matrices. Timely development of an event template/matrix IAW the unit battle rhythm is critical to the development of the decision support template, intelligence synchronization matrix, ISR overlay, and the execution of ISR operations.

Chapter 6

Counterintelligence

DEFINITION

6-1. Counterintelligence counters or neutralizes intelligence collection efforts through collection, CI investigations, operations, analysis and production, and technical services and support. CI includes all actions taken to detect, identify, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to protect US interests and equities. It assists in identifying essential elements of friendly information (EEFIs), identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against US forces. Refer to FM 2-22.2 for details concerning CI mission and functions.

MISSION

6-2. 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 AFIST collection threat to the US Army and DOD, in order to protect the lives, property, or security of Army forces. Army CI has four primary mission areas: counterespionage; support to FP; support to research and technology protection; cyber CI.

ROLE

6-3. The role of CI is to deny, degrade, disrupt, or mitigate AFIST ability and capability to successfully execute intelligence collection targeting US or friendly force interests. CI will focus on countering AFIST intelligence collection activities targeting information or material concerning US or friendly force personnel, activities, operations, plans, equipment, facilities, publications, technology, or documents—either classified or unclassified. It does this without official consent of designated US release authorities, for any purpose that could cause damage or otherwise adversely impact the interests of national security of the US ability to fulfill national policy and objectives.

6-4. CI elements are instrumental in contributing to situational awareness in the area of influence. CI elements may corroborate other intelligence discipline information as well as cue other intelligence assets through the CI core competencies and through CI technical services.

- CI core competencies are investigations of national security crimes within CI jurisdiction, collection of AFIST threat information and targeting, operations, and analysis and production.
- CI technical services include computer network operations (CNO), technical surveillance countermeasures (TSCM), and polygraph. CI focuses on combating AFIST intelligence activities targeting Army personnel, plans, operations, activities, technologies, and other critical information and infrastructure.
- With proper approval, CI may employ electronic surveillance, investigative photography, cyber CI support, polygraph, and TSCM.

COUNTERINTELLIGENCE FUNCTIONS

6-5. CI functions are interrelated, mutually supporting, and can be derived from one another. No single function or technical capability can defeat AFIST intelligence efforts to target US interests. CI functions are discussed below.

CI INVESTIGATIONS

6-6. Investigative activity is essential to countering the adversary intelligence threat to Army interests. CI places emphasis on investigative activity to support force, infrastructure and technology protection, homeland defense, information assurance, and security programs. CI investigations focus on resolving allegations of known or suspected acts that may constitute National Security Crimes under US law which include—

- Treason.
- Espionage.
- Subversion.
- Sedition.

6-7. Other CI investigations include unreported contact with foreign government personnel, persons or groups involved in foreign terrorism or intelligence, or unauthorized requests for classified or sensitive unclassified information, and military personnel or Army civilians who perform unofficial travel to those countries designated in the operational planning list.

6-8. The primary objective in any CI investigation is the detection, identification, exploitation, and/or neutralization of adversary intelligence threats directed against the US Army. CI investigations are also conducted to identify systemic security problems that may have damaging repercussions to Army operations and national security interests. All CI investigations are conducted within guidelines established in
AR 381-10, AR 381-12, AR 381-20, applicable DOD policy and directives, and US laws.

CI OPERATIONS

6-9. CI operations are characterized as those activities that are not solely associated with investigative, collection, analysis, or production functions. CI operations can be either offensive or defensive in nature; they are derived from or transition to a collection or investigative activity depending on the scope, objective, or continued possibility for operational exploitation. CI operations fall into the following two categories:

- **CI Support Operations.** These are defensive operations used to support Army operations, technology protection, security projects, and programs. They include technical services support, support to acquisition, FP, SAPs, international security, foreign visitor or contact, treaty verification, information assurance, homeland defense, and advice and assistance programs conducted by CI teams to improve the security posture of supported organizations. CI support operations also include—
  - Conducting inspections, security planning, and resolution of security problems.
  - Developing classification guides.
  - Conducting surveys.
  - Conducting technical inspections.
  - Providing pre-construction technical assistance.
  - Conducting SAEDA briefings and other approved projects and programs.
- **CI Sensitive Operations.** These operations are generally offensive in nature and involve direct or indirect operations against a known or suspected AFIST intelligence threat. These operations include counterespionage and CI projects and are conducted by designated units.

CI COLLECTION

6-10. **CI Collection Activities.** While CI and HUMINT both have a collection mission, it should be understood that there are distinct differences between CI and HUMINT collection objectives. HUMINT focuses on answering the CCIRs concerning the plans, intentions, capabilities, and disposition of the adversary as a whole. CI specifically targets the AFIST intelligence collection threat targeting US forces. CI collection is—

- The systematic acquisition of information concerning the AFIST intelligence collection threat targeting US Army equities. CI elements conduct collection activities in support of the overall CI mission.
- Conducted through the use of sources, elicitation, official liaison contacts, debriefings, screenings, and OSINT to obtain information that answers the standing CI collection requirements or other collection requirements based upon the CCIRs.
- Conducted to understand how AFIST is targeting US forces so other CI initiatives can be devised to deny the adversary the ability to collect on, target, or react to US military operations.

6-11. **CI Source Operations.** CI conducts source operations to gather information the commander needs to make decisions in support of the overall mission. The commander focuses the CI effort by carefully assigning missions and clearly defining the desired results. While using CI collection as a means of targeting, the use of single-source reporting could lead to targeting based on tribal, regional, or cultural differences rather than threat-based targeting. In all instances, CI reporting should be corroborated by other sources of information and/or intelligence disciplines to determine accuracy and truthfulness prior to targeting by the commander. CI source operations—

- Are not intended to be used as a substitute for tactical HUMINT military source operations (MSO).
- Can be used to initiate CI investigations, identify potential leads for offensive operations, or develop additional CI leads.
- Consist of three different collection categories:
  - Offensive CI Operations (OFCO) activities support Army, Theater, Army component commands (ACCs), Army service component commands (ASCCs), and local intelligence requirements, as well as DOD, Joint Chiefs of Staff, unified and specified commands, JTF, and multinational and national intelligence community strategic requirements in order to deter, detect, and neutralize espionage. (For more information on OFCO, refer to AR 381-47 (S)).
  - CI Defensive Source Operations (DSO) are only employed by units with a CI investigative and operational mission. CI DSO will not be employed in combat operations. CI DSO activities are only employed by units with a CI investigative and operational mission. They are conducted in support of theater-level operations in mature and stable environments to answer theater-level information requirements. CI DSO will be proposed through the submission of a CI Special Operation Concept and have to be approved by Commander, INSCOM, or designated representative. (For more information concerning DSO, refer to TC 2-22.201 (S)).
  - CI Force Protection Source Operations (CFSO) use source operations to collect FP and AFIST collection and threat I&W. CFSO are conducted in all OCONUS locations to satisfy the supported commander's information requirements. CFSO is employed on the basis of a CFSO OPLAN approved by the supported commander or the S/G/J/C2X if approval authority has been delegated by the ASCC or JTF commander. CFSO will only be conducted OCONUS except for unit training.

6-12. **Liaison.** CI elements conduct liaison with US, multinational, and HN military and civilian agencies, to include NGOs, for the purpose of obtaining information of CI interest and coordinating or deconflicting

CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements and to develop CI leads for further exploitation.

6-13. **Screening.** CI Screening is a systematic process for obtaining information of CI interest from a specific person or target audience. Information of CI interest includes all standing CI collection requirements established in AR 381-20, CCIRs, or any information that includes but is not limited to the plans, intentions, capabilities, methods of operation, personalities, structure, and personal associations with any AFIST entity.

6-14. CI screening uses a variety of questioning techniques to obtain information. This includes interviewing methods using basic interrogatives to identify and exploit information of CI interest; a structured debriefing format utilizing a prepared question list when the source has knowledge of a specific topical interest; and elicitation utilizing a discreet form of questioning which does not let the source know the specific AOI of the CI Special Agent.

> ***Note.*** CI screening does not use any types of interrogation or screening approaches utilized by HUMINT collectors defined in FM 2-22.3. CI screening normally is not confrontational unless the source initiates a hostile attitude and forces the CI Special Agent to maintain control through the exercise of the CI Special Agent's official authority.

6-15. Each of the interviewing methods can be used or combined dependent upon the situation. CI screenings include the following:

- **Local Employee Screening.** Local employee screening is conducted primarily to identify individuals who may be a security risk. It can, however, be used as a means to obtain intelligence information or to identify personnel with placement and access to be used for source operations.
- **CI Support to Joint Interrogation and Debriefing Centers.** During combat and other contingency operations, CI will normally be included in the manning and support requirements for Joint Interrogation and Debriefing Center (JIDC) operations. While the priority for intelligence collection during JIDC operations is focused on CCIRs and other HUMINT-specific collection requirements, JDIC operations offer an excellent opportunity for CI collection. Detainees held in JDIC facilities will include adversarial military, security, intelligence, insurgent, and terrorist personnel who can answer specific CI requirements to include but not limited to the plans, intentions, capabilities, methods of operation, personalities, structure, and personal associations of AFIST elements targeting US forces.
- **Local Community or Area Screening.** Local area screening is normally done in coordination with other operations such as a cordon and search operation. CI Special Agents accompany the forces conducting the operation and screen the general population to identify individuals of CI interest.

6-16. **CI Debriefing.** CI debriefings focus on two different types of targets. Debriefing of repatriated US personnel or special category absentees and personnel who are pre-briefed and debriefed as part of an approved CI operation or project. CI personnel assigned to combat units may also participate in intelligence debriefing of US or multinational patrols or other tactical elements that may support the CCIRs. (For more information on CI debriefings, see FM 2-22.2.)

6-17. **CI Technical Services and Support.** CI technical services are used to assist the CI 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 the commercial markets enables any AFIST the ability to increase their capability and effectiveness in collecting on US Army interests. To mitigate this increasing threat requires a specialized expertise. CI organizations with technically trained CI Special Agents are chartered with providing this

unique technical capability to augment and provide specialized support to the CI mission. This includes CI Special Agents trained to—

- Conduct physical and electronic surveillance in support of authorized CI investigative activities.
- Perform TSCM to identify adversarial electronic collection activities.
- Perform cyber CI activities that provide protection to information networks as well as to identify vulnerabilities and attempted intrusions into Army and DOD computer networks.
- Perform CI scope polygraph examinations in support of CI investigative activities and sensitive program support.

6-18. **CI Covering Agent Program (CICAP).** CICAP is the assignment of a primary supporting CI Special Agent to a command or agency. This agent conducts all routine liaisons and provides advice and assistance to the unit. The agent must become fully knowledgeable with the unit's operations, security, personnel, and vulnerabilities. The agent is the point of contact for reporting information of actual or potential CI interest.

ANALYSIS

6-19. CI analysis is conducted as a single-source feed into the all-source intelligence analysis process and to focus CI operations. CI analysis and production will be accomplished at any level at which Army CI assets are assigned. CI analysis focuses on the plans, intentions, and capabilities of an AFIST entity known or suspected of targeting US forces for targeting and/or information exploitation to support FP of US personnel, property and operations; protect the R&D of critical technologies; and to support information operations to protect US forces information systems.

Intelligence Analysis

6-20. CI analysis should be focused on predictive, assessments of AFIST plans, intentions, and capabilities. CI analysis supports the development of countermeasures recommendations to deny, disrupt, or negate the ability of an AFIST entity to successfully collect and exploit information concerning US forces. Accurate CI analysis also increases the visibility of proactive and effective CI support and establishes credibility with the supported commander. This in turn leads commanders to trust and rely upon their CI assets and often give them more flexibility to execute CI operations.

Operational Analysis

6-21. Operational analysis allows the operational management elements (2X, Counterintelligence Coordinating Authority [CICA] and Operational Management Team [OMT] leaders) to gauge the effectiveness and success of their subordinate operational CI teams. Operational analysis—

- Is done through assessments on source production (quantity and quality), source vetting (reliability, accuracy, response to control), and requirements coverage.
- Also allows operational managers to deconflict CI operations and to provide direction and focus to eliminate redundancy and/or increase the efficiency of the CI teams.

PRODUCTION

6-22. CI products consist of but are not limited to target nomination, threat assessments, CI estimates, and investigative and intelligence information reports. CI is responsible for providing the AFIST threat assessment, which can stand alone or be included as part of a vulnerability assessment. Threat assessments are a comprehensive assessment of the plans, intentions, capabilities, tactics, and focus of a known or suspected AFIST entity. A vulnerability assessment is a detailed assessment of a unit, agency, facility, operation, or mission to identify vulnerabilities to security or operational TTP that could impact the successful execution of the mission or operation.

6-23. Vulnerability assessments are planned and coordinated by the unit FP officer and consists of multiple agencies providing subject matter expertise to the final product which should include not just the vulnerabilities but risk mitigation measures. (VAs are conducted to identify weaknesses and vulnerabilities in security and FP posture and to provide countermeasures recommendations.) Finalized intelligence derived from CI activities are incorporated into joint and national intelligence databases, assessments, and analysis products. CI products are also incorporated into the COP to support battlefield situational awareness. CI production takes place at all levels.

- Operational and tactical production includes—
  - Spot reports and current intelligence.
  - CI threat and/or vulnerability assessments tailored to specific activities, units, installations, programs, or geographic areas.
  - CI studies to support contingency planning and major exercises.
  - Studies of adversary intelligence organization, modus operandi, personnel, activities, and intentions that pose a current or potential threat to the supported command.
- Strategic products include—
  - Assessments supporting national and Army programs including SAPs and acquisition programs.
  - Worldwide assessments of the organization, location, funding, training, operations capabilities, and intentions of terrorist organizations.
  - Global trends in adversary intelligence modus operandi.
  - After-action studies of individual espionage cases.
  - Analyses of the intelligence collection capabilities of international narcotics trafficking organizations.
  - Multimedia threat products to support Army CI awareness programs.

COUNTERINTELLIGENCE STRUCTURE

6-24. CI organizations and force structure are designed to support the modular force construct through scalable team, operations management, and technical channels packages. CI elements assigned to division, battlefield surveillance brigades, ASCC, and strategic units are capable of operating at all echelons and throughout the full spectrum of military operations. The Joint *2X organizational and operational concept has been established in Army Force structure to decentralize CI operational approval and execution. As the primary force provider for the DOD CI in contingency and combat operations, the establishment of the *2X and the CICA throughout the Army ensures a trained and experienced cadre of CI professionals capable of filling Army, joint, and combined 2X and CICA/Task Force Counterintelligence Coordinating Authority (TFCICA) positions.

*2X

Note. *2X denotes the 2X staff officer at all echelons, S-2X (Brigade), G-2X (Division, Corps, ASCC), J-2X (JTF), C-2X (Combined Task Force), and Army G-2X (Department of the Army [DA] level).

6-25. The *2X is the CI and HUMINT manager who is authorized to coordinate, deconflict, and synchronize all CI and HUMINT missions in the area of intelligence responsibility. The *2X manages CI and HUMINT intelligence requirements including HUMINT collection requirements, time-sensitive collection requirements, report evaluations with source-directed requirements, and source assessments. At each echelon the *2X Section may be structured differently, but there is always a requirement for three components: CICA, a HUMINT operations cell (HOC), and an operations support cell (OSC). Figure 6-1 shows the 2X organization. The *2X is responsible for—

- Participating in predeployment or deployment planning for CI and HUMINT assets in support of operations.
- Coordinating, through the HOC and TFCICA/CICA, all CI and HUMINT activities to support intelligence collection and the intelligence aspects of FP for the deployed commander.
- Managing collection requirements for CI and HUMINT in coordination with the requirements manager.
- Coordinating and deconflicting all CI and HUMINT operations within the operational area.
- Serving as the release authority for CI and HUMINT reporting.
- Releasing reports to the all-source system only after ensuring all technical channels measures for reporting have been met.

6-26. The *2X is a commissioned officer with a CI or HUMINT area of concentration (AOC) (35E/F). Within joint and combined force commands, the C/J2X may be either an Army, Navy, Air Force or Marine officer or civilian depending upon the requirements of the approved joint manning document. (See TC 2-22.303 for details on the 2X.)

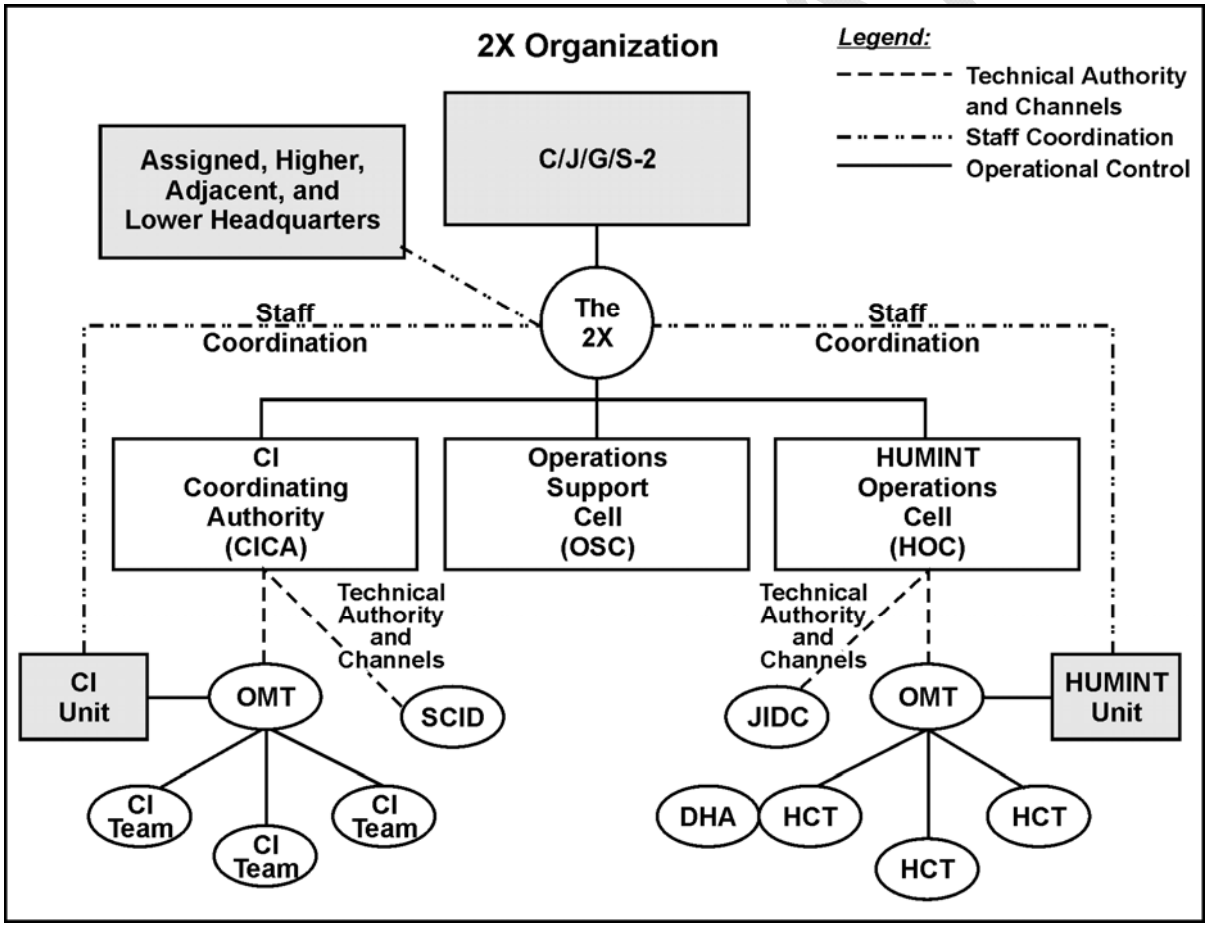


Figure 6-1. 2X organization

COUNTERINTELLIGENCE COORDINATING AUTHORITY

6-27. The CICA is the coordinating authority for all CI activities for all assigned or attached Army CI assets. The CICA for Army Divisions and Corps will normally be a senior 351L CI warrant officer (WO).

At the ASCC, the CICA may be a senior CI WO, CI officer (35E) or equivalent Military Intelligence Civilian Excepted Career Program government civilian employee.

6-28. Within Joint and multinational force commands, the TFCICA may be either an Army, Navy, Air Force, or Marine WO, officer, or civilian depending upon the requirements of the approved Joint Manning Document. Army CICA components generally consist of four personnel (a CI WO and three enlisted CI Soldiers); however, size and structure may vary depending upon the unit and mission. Units engaged in operational and strategic missions may also have a higher standard of grade for CICAs to include the use of appropriately credentialed government civilian employees. CICA personnel may be assigned, attached, or under operational control (OPCON).

6-29. Regardless of echelon or service component, the CICA's mission is to manage, coordinate, and synchronize all CI activities in the designated area of intelligence responsibility. The CICA exercises technical channels for all CI entities and deconflicts CI activities with higher, lower, and adjacent CI elements. The CICA accomplishes all responsibilities through coordination with the operational units and other 2X staff elements. (See TC 2-22.303 for details on the CICA.)

6-30. The CICA performs the following functions:

- Is responsible for coordinating and staffing all CI FP source operations (CFSO) proposals with the Army Component or JTF approval authority and US national agency representatives.
- Serves as the single focal point for all matters associated with CI in the area of intelligence responsibility. The CICA tracks CI activities and keeps the 2X informed so the 2X in turn can keep the C/J/G/S-2 and commander informed.
- Exercises technical authority of all CI entities and coordinates all CI activities in the area of intelligence responsibility. Coordinates with MI unit commanders who possess CI assets that execute CI activities in the area of intelligence responsibility.
- Coordinates and deconflicts all CI source operations with the source registry manager in the area of intelligence responsibility.
- Ensures a robust CI Education and Awareness Training Program by coordinating Subversion and Espionage Directed Against the Army (SAEDA) refresher training, as required, and by ensuring the establishment of SAEDA reporting channels and procedures in the area of intelligence responsibility.
- Is responsible for implementation of the intelligence program for all CI activities in the AO in accordance with AR 381-10.

Note. The military departments always remain in control of CI investigations. The Army Theater CI Coordinating Authority (ATCICA) and Army CI Coordinating Authority (ACICA) provide investigative technical channels for all Army CI conducted investigations. While Army CI investigative reports will pass through the CICA and *2X, they will go simultaneously to the ATCICA and ACICA.

- Keeps the 2X, C/J/G/S-2, and commander informed on the status of CI activities.
- Coordinates with the analytical element and with the ISR synchronization staff to identify and refine requirements for CI collection, operations, or investigations.
- Ensures CI reporting is disseminated to the analytical element for inclusion into all-source analysis, as appropriate.
- Develops and disseminates requirements, orders, and RFIs to CI entities in the area of intelligence responsibility.
- Ensures registration of all CI sources with the OSC or other designated source registry manager. (If there is no OSC, the CICA will maintain the source registry.)
- Routinely evaluates CI source operations to ensure proper handling by CI Special Agents, source ability to satisfy requirements, and to determine value of continuing the operation.

- Ensures exploitation opportunities are preserved while conducting vulnerability assessments and other FP initiatives.
- Ensures investigations are planned, prepared, executed, and assessed in accordance with applicable directives and regulations.
- Establishes and maintains connectivity with the supporting ATCICA for investigative oversight for Army CI-conducted investigations.
- Participates in the operations staff targeting process to provide input on the placement, access, availability of sources, and reporting reliability of CI sources that support operations.
- Ensures CI support is provided to the JIDC and detainee holding areas in the area of intelligence responsibility.
- Establishes quality control and executes release for all CI reporting.
- Routinely provides feedback to all CI entities in the area of intelligence responsibility regarding their collection activities, operations, and investigations.
- After a determination has been made to release a detainee, ensures screening is performed of the detainee to be released to determine the detainee's suitability as a potential lead for CI or other collection activities.
- Interacts with the HOC and OSC to ensure CI activities do not conflict with HUMINT activities in the area of intelligence responsibility.
- Conducts liaison with the Provost Marshal Office and intelligence entities conducting liaison with HN LEAs to ensure CI activities are coordinated and deconflicted.
- Conducts liaison with HN and US national level CI organizations.
- Provides staff oversight to locally employed personnel (LEP) screening activities within the area of intelligence responsibility.
- Provides technical oversight and guidance for requests for coordination or approval for CI operations which require approvals outside the local approval authority.
- Recommends to the supported C/J/G/S-2 and maneuver commander the designation of an MI unit or intelligence staff element, as appropriate, to serve as the repository for CI Badge and Credentials in the area of intelligence responsibility with responsibility for accountability and issue of CI Badge and Credentials.
- Coordinates requests for CI technical services (cyber CI unit, TSCM, and polygraph support).

COUNTERINTELLIGENCE OPERATIONAL MANAGEMENT TEAM

6-31. The OMT is the first operational management element that provides technical channels to subordinate CI teams. The OMT manages subordinate CI teams to ensure operational execution and direction, quality and control of reporting, and satisfaction of intelligence requirements. An OMT can manage between one to four CI teams depending on the operational tempo mission and geographic requirements. OMTs generally consist of four personnel (a 351L, CI WO and three 97L, CI enlisted Soldiers); however, size and structure may vary depending upon the unit and mission.

6-32. Units engaged in operational and strategic missions may also have a higher standard of grade for OMTs to include the use of appropriately credentialed government civilian employees. OMT personnel may be organic, attached, or assigned under OPCON. OMTs and subordinate CI teams may be pushed down from higher echelon units to lower echelon units. Depending upon mission requirements, CI OMTs may be held at the next higher echelon of the subordinate CI teams. CI OMTs will normally never be located below the brigade level. (See TC 2-22.303 for details on the OMT.)

6-33. The OMT performs the following functions:

- Is responsible for passing all intelligence or time-sensitive information to the command channels for action.
- Provides guidance and technical channels for operational activity.

- Provides the collection focus and operational focus for CI teams.
- Provides quality control and dissemination of reports for subordinate CI teams; receives, edits, and provides feedback on all administrative reports (for example, resource status reports), operational reports (for example, contact reports), and intelligence reports (for example, intelligence information reports) provided by subordinate teams.
- Ensures that CI reporting and related traffic from above and below are fused into the all-source picture.
- Conducts CI analysis and assists in mission analysis for the supported commander.
- Coordinates CI activities with the CICA and with CI element commanders in the area of intelligence responsibility.
- Performs liaison with HN and US national level security, intelligence, and law enforcement organizations.
- Informs respective CICA when Army CI elements are conducting CI investigative activities within the purview of AR 381-20.
- Acts as a conduit between subordinate CI teams, the CICA and 2X, and the supported unit headquarters.
- Provides administrative support for subordinate CI teams to include reporting mission and equipment status to the CICA or HOC and the supported unit headquarters.
- Educates the supported commander on the capabilities of subordinate teams.
- Integrates subordinate CI teams directly into the unit's ISR planning.

COUNTERINTELLIGENCE TEAM

6-34. The CI team conducts CI investigations, CI operations, CI collection (debriefings, source operations, liaison, and screening), CI analysis, and CI technical services support to protect the supported unit from threat intelligence activities.

6-35. The CI team provides the supported commander, through 2X channels, a capability to help protect the force and affect the adversaries' understanding of friendly force operational capabilities. The CI team also provides a capability to help answer PIRs related to AFIST collection activities targeted against the supported unit, US Army, and DOD equities.

6-36. A CI team generally consists of four 35L, CI noncommissioned officers (NCOs) and enlisted Soldiers. Units engaged in higher echelon missions may also have a higher standard of grade for CI teams to include the use of appropriately credentialed government civilian employees. Specialized CI teams, to include technical counterintelligence, cyber CI and polygraph, may vary in composition (2- to 3-person military and/or civilian teams) based upon mission requirements and unit organization. CI teams—

- May be assigned, attached, or OPCON.
- May be pushed down from higher echelon units to lower echelon units.
- May be pushed down to brigade level depending upon mission requirements.

6-37. The CI team performs the following functions:

- Prepares and submits command reports, such as readiness status reports that provide status of equipment, personnel, and intelligence contingency funds in accordance with supporting OMT SOPs.
- Prepares protected reports, such as contact reports, in accordance with OMT SOPs, that document each source contact.
  - Disseminates contact reports to their supporting OMT for review or comment.
  - Maintains contact report files on every source.
  - Provides contact report files to replacing team during relief in place or transfer of authority.

- Prepares and submits intelligence reports, such as SPOT reports using the SALUTE (size, activity, location, unit, time, equipment) format and intelligence information reports in accordance with OMT SOPs.
- Assists in the production of threat assessments and vulnerability assessments. This function provides support to evaluations of installations and operating bases in conjunction with MP, CA, engineers, and medical units to identify the intelligence threat to the operating location. The vulnerability assessment identifies weaknesses in operational and physical security procedures and recommends countermeasures to mitigate intelligence collection on friendly forces; this limits the ability of adversaries to plan and conduct hostile acts on US and multinational activities and locations.
- Conducts CI analysis to support mission requirements and contributes to the COP. To verify adequate area coverage, uses backwards planning and source profiling to choose CI targets.
- Develops and uses CI target overlays and other CI analytical tools that illustrate the CI situation, identify CI gaps, and help refocus CI collection efforts.
- Conducts CI debriefings. This function involves the systematic questioning of individuals to procure information to answer specific CI collection requirements by direct and indirect questioning techniques. Sources for debriefing include friendly forces (for example, MP, CA, engineers, and medical units), US and non-US civilians to include members of NGOs, refugees, displaced civilians, and local inhabitants. The supported S-2, with the help of the CI team, regularly and systematically debriefs all ISR assets.
- Conducts CI investigations within the jurisdictional boundaries of Army CI regulations and the guidelines of AR 381-10, AR 381-12 and AR 381-20. Regularly coordinates with the supporting staff judge advocate to ensure investigations are conducted in such a way as to support eventual trial and prosecution, if necessary, and to be in compliance with all DOD policy and US laws.
- Conducts CI screening.
- Conducts CI collection.
- Registers all CI contacts through the OMT and CICA in the source registry. Disseminates CI administrative, technical, and intelligence reports through the OMT and CICA.
- Conducts CI liaison with US, multinational, and HN military and civilian agencies, to include NGOs, for the purpose of obtaining information of CI interest and to coordinate and deconflict CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements and to develop CI leads for further exploitation.
  - Maintains constant contact with the supported S-2 in order to identify intelligence requirements and information gaps and to deconflict operations within the support commander's AO.
  - Maintains constant contact with other ISR assets in order to coordinate and deconflict operations in adjacent AOs and cross-checks collected information.
- Supports the CI Education and Awareness Training Program by coordinating with the S-2 of all units in their area of intelligence responsibility to present SAEDA awareness training. CI teams should be the focal point for all SAEDA training in order to identify incidents of CI interest and educate Army personnel concerning their responsibilities to report incidents that are outlined in AR 381-12. The CI Education and Awareness Training Program supports the commander's overall FP program.
- Provides CI technical service support (for example, TSCM, polygraph, computer forensics) to the supported unit when properly trained and equipped personnel are provided.

ARMY COUNTERINTELLIGENCE LEVELS OF EMPLOYMENT

6-38. CI is critical to Army operations at all echelons, during peacetime and throughout the full spectrum of operations. The only difference in the operational execution is generally what mission areas are being

supported. Even CI Special Agents providing CI technical services and support are leveraged to provide their unique capabilities during peacetime and during garrison and during deployed operations.

6-39. Due to the transformation of CI to a HUMINT collection function in recent operations, the true mission and proper employment of CI as a warfighting enabler need to be articulated to commanders.

STRATEGIC AND DEPARTMENTAL

6-40. Strategic operations are conducted by CI elements supporting national and DOD missions (for example, support to North Atlantic Treaty Organization and special operations and missions). Strategic CI also conducts compartmented investigations and operations to affect the knowledge of adversarial intelligence regarding contingency operations (CONOPs) and defense information. Strategic CI executes the full range of CI functions and missions including CI investigations and operations, OFCO, research and technology protection, SAP support, treaty verification, and technical CI services (polygraph, TSCM, and computer forensics). Strategic CI also supports SOF and special mission units within the scope of applicable national, DOD, and DA policies and regulations. Strategic and departmental CI assets generally conduct the following activities:

- **Advice and Assistance.** Assists unit security managers and commanders with knowledge on security programs and provides details on reporting potential AFIST targeting and incidents of CI interest.
- **Education and Awareness.** Provides AFIST threat and US Army program briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for incidents of CI interest.
- **Target Acquisitions and Vulnerability Assessments.** Conducts collection and analysis of AFIST threat data for a specific unit, facility, operation, or activity to provide the supported commander knowledge on FP and security posture and make countermeasures recommendations to overcome deficiencies.
- **CI Investigations.** Exploits or neutralizes potential AFIST collection threats targeting US Army and DOD equities.
- **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US forces and devises other CI initiatives to counter, exploit or neutralize the AFIST collection capability.

Army G-2X

6-41. At the departmental level the Army G-2X is the executive agent for all Army CI activities to include policy implementation, operational oversight, intelligence funding programs, and Army staff level management. The Army G-2X—

- Coordinates with other military service and national agency intelligence and CI services to coordinate CI strategies and mutually supporting activities, to include joint CI operations and investigations.
- Is responsible for making recommendations to the DA G-2 concerning all budgetary issues concerning CI and HUMINT.
- Provides oversight and guidance for Army CI elements. It staffs and coordinates approval of CI Operational Concepts and Plans as outlined AR 381.20, chapter 2, to ensure they meet legal sufficiency and satisfy validated requirements and provides oversight for all approved Army CI Operational Concepts and Plans.
- Manages and maintains the Army's centralized CI and HUMINT source registry and product library as part of a Joint Service CI and HUMINT database.
- Coordinates functional and technical support services, as well as comprehensive worldwide AFIST threat analysis products.

- Collaborates with CI staffs and field elements at all echelons to ensure unity of the CI effort and efficient use and employment of Army CI assets.

Army Counterintelligence Coordinating Authority

6-42. The ACICA is subordinate to the Army G-2X and is responsible for implementing and enforcing US and DOD policy within the Army and providing technical channels for all Army CI Activities. The ACICA—

- Reviews, staffs, and coordinates all special investigative and collection techniques requested by Army CI elements. The ACICA—
- Is responsible for approving all Army CI investigations.
- Reviews, staffs, and coordinates all CI operational plans and concepts with the appropriate agencies and approval authorities.
- Coordinates with other US government and military CI agencies to assist in the development and implementation of national CI strategies.

Intelligence and Security Command

6-43. INSCOM executes departmental and operational CI activities in accordance with guidance from the Army G-2X. INSCOM has the responsibility for administrative C2 of all Army Theater Military Intelligence Brigades (MIBs) supporting their respective theater ASCC. INSCOM CI assets are task-organized and operationally employed based upon mission and geographic requirements. Most MIBs organize their CI assets into detachments with subordinate field or resident offices.

OPERATIONAL

6-44. These CI assets are generally assigned to ASCC and are generally focused on a specific theater. CI at the operational level is primarily focused on counterespionage and CI support to FP. Operational CI assets are instrumental in protecting bases of operations from infiltration, collection, planning, and targeting by AFIST entities. Although operational CI elements have a vital mission to counter the AFIST threat on a daily basis, they may be tasked to deploy and support contingency or combat operations. This is especially true in major combat operations when the size, scale, and scope of the operation exceed the capability of organic tactical CI assets to provide adequate support in the AO. Operational CI assets may also be tasked to support strategic CI operations when required. Operational CI assets generally conduct the following activities:

- **Advice and Assistance.** Assists unit security managers and commanders with knowledge on security programs and provides details on reporting potential AFIST targeting and incidents of CI interest.
- **Education and Awareness.** Provides AFIST threat and SAEDA briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for incidents of CI interest.
- **Threat Assessments and Vulnerability Assessments.** Conduct collection and analysis of AFIST threat data for a specific unit, facility, operation, or activity to provide the supported commander knowledge on FP and security posture and make countermeasures recommendations to overcome deficiencies.
- **CI Screening.** Vets LEP in overseas and deployed locations for suitability to work, FP liabilities, associations, or contacts that may allow them to be used in other CI collection initiatives.
- **CI Investigations.** Exploits or neutralizes potential AFIST collection threats targeting US Army and DOD equities.

- **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US forces and to devise other CI initiatives to counter, exploit, or neutralize the AFIST collection capability.

Theater G-2X

6-45. The Theater G-2X is the principal advisor to the theater ASCC G-2 and commander for all CI and HUMINT matters. The theater G-2X consists of the G-2X staff officer, theater HOC, ATCICA, and OSC. The theater G-2X—

- Provides guidance and oversight based upon Army G-2X directives and theater requirements.
- Provides technical channels and operational coordination for all theater Army CI and HUMINT elements.
- Also coordinates technical support services, source registration and national level product support with the Army G-2X. Regional analysis and production is provided to theater consumers and forwarded to the Army G-2X for inclusion into the national database.

Army Theater Counterintelligence Coordinating Authority

6-46. The ATCICA is subordinate to the Theater G-2X and is responsible for providing guidance and technical channels for all Army CI collection and investigative and operational activities within their theaters of operation, to include CI elements assigned to tactical organizations. ATCICA—

- Is responsible for reviewing and staffing all requests for special investigative and collection techniques and investigative and operational plans and concepts.
- Is the interface between subordinate Army CI operational management elements and the ACICA.
- Is responsible for implementing Army CI policy as directed by the ACICA and Army G-2X.
- Conducts liaison with other US government and military, HN intelligence, security, and LEAs to coordinate and deconflict CI activities.

Military Intelligence Brigade

6-47. MIBs provide operational support to the separate ASCCs. CI elements in MIB support CCDRs, generally in combatant commander's AORs. Operational level CI activities and functions include investigations, collection, analysis and production, and technical services and support. CI elements must be capable of quickly transitioning from a peacetime mission to crisis operations to support CCDR requirements. Theater CI assets conduct Army, joint, and multinational operations in their JOAs. Operational elements may also be deployed to support or reinforce tactical forces in CONOPs.

TACTICAL

6-48. Tactical CI generally denotes all CI assets assigned to Army corps and below. This includes CI assigned directly to brigade combat teams, divisions, and corps units. CI at the tactical level is primarily focused on CI support to FP to their supported commanders during contingency and combat operations or to the war on terrorism. CI assets at the tactical level are instrumental in protecting bases of operations from infiltration, collection, planning, and targeting by AFIST entities.

6-49. Tactical CI assets generally do not have a robust peacetime mission since their focus is providing support to their combat arms parent organization; however, in some cases operational and strategic CI elements may formally request their support on a case-by-case basis or through formal written agreements. Even during peacetime garrison operations, tactical CI assets are essential in providing advice and assistance to their supported command and other CI operational activities that can assist and be the instigator for more complex CI initiatives. Depending upon the size, scale, and scope of ongoing

operations, operational and strategic CI assets may also be tasked to augment tactical operations. CI assets assigned to tactical units generally conduct the following activities:

- **Advice and Assistance.** Assists unit security managers and commanders with knowledge on security programs and provides details on those CI assets that can respond to AFIST targeting.
- **Education and Awareness.** Provides AFIST threat and SAEDA briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for CI elements chartered to conduct investigations during peacetime.
- **Threat Assessments and Vulnerability Assessments.** Conducts collection and analysis of AFIST threat data for a specific unit, facility, operation, or activity to provide the supported commander knowledge on FP and security posture and make countermeasures recommendations to overcome deficiencies.
- **CI Screening.** Vets LEPs in overseas and deployed locations for suitability to work, FP liabilities, associations, or contacts that may allow them to be used in other CI collection initiatives.
- **CI Investigations.** Identifies potential CI investigation requirements and triages those incidents for other CI assets chartered to conduct the investigation. This can be accomplished during peacetime and contingency or combat operations. During contingency or combat operations, the chartered CI element may request the assistance of tactical CI personnel to fulfill investigative requirements. Tactical CI assets generally do not have the resources to effectively execute a complex CI or counterespionage investigation.
- **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US forces and devises other CI initiatives to counter or neutralize the AFIST collection capability. CI collection is only conducted in contingency or combat operational environments and when approved by the CICA.

Corps/Division/Brigade G-2X

6-50. The G/S2X is the principal advisor to their supported commander for all CI and HUMINT matters within their area of intelligence responsibility. The G/S2X consists of the G/S2X staff officer, HOC, and the CICA. At lower echelons (for example, Stryker Brigade Combat Team and brigade combat team levels), an OSC may not be authorized or resourced and may have to be task-organized from assigned and attached resources in order to provide this capability.

6-51. The G/S2X provides direct technical channels for all CI and HUMINT assets within their unit and area of intelligence responsibility. The G/S2X—

- Coordinates and deconflicts all CI and HUMINT activities between higher, lower, and adjacent *2X elements.
- Is responsible for providing and maintaining a consolidated source registration for all CI and HUMINT elements within their area of intelligence responsibility and providing source data to the next higher echelon *2X element.
- Coordinates requests for technical support services, source registration, and higher level analytical support with the next higher echelon *2X element.
- Must have knowledge of the CI and HUMINT resources and capabilities for all military, DIA, and US Government agencies. The G-2X must be able to transition from an Army Force operation to functioning as a J-2X if their unit is designated as a JTF headquarters.

Corps or Division CICA

6-52. The Corps or Division CICAs are directly subordinate to their respective Corps or Division G-2X element. The CICA provides direct oversight and control for all CI activities within their supported unit and area of intelligence responsibility. The CICA is responsible for coordinating and deconflicting all CI activities with the next higher echelon CICA. It conducts liaison with other US Government and military

and HN intelligence, security, and LEAs within their area of intelligence responsibility to coordinate and deconflict CI activities. The CICA—

- Reviews and provides quality control and dissemination of all CI reporting from subordinate CI elements.
- Provides operational analysis to focus CI activities, assess responsiveness and effectiveness of CI activities, and ensures coverage of information requirements for their supported commander.
- Must have knowledge of the CI resources and capabilities for all military, DIA, and US Government agencies.
- Must be able to transition from an Army Force operation to functioning as a TFCICA if their unit is designated as a JTF headquarters.

Corps or Division CI Elements

6-53. CI assets supporting division and JTF operations are generally leveraged from tactical battlefield surveillance brigades (BFSBs). The G-2X at division will provide CI investigation and technical channels for CI elements supporting division elements. The division G-2X will coordinate CI activities through the JTF J-2X in theater and their theater CICA and/or senior CI staff officer. The Division G-2X must be trained and equipped to act as a J-2X in the event the division is designated as the JTF command element during a CONOP.

6-54. At corps or division level, the BFSB battalion has three companies with CI assets. The collection and exploitation (C&E) company has one CI OMT that controls three CI teams. Each CI team consists of four enlisted CI Soldiers. The C&E company's mission is to provide general support coverage for the division. Each of the two CI and HUMINT companies has two CI teams and no CI OMTs. The CI and HUMINT company's mission is to provide its assets in DS to the BCTs.

Brigade Combat Team

6-55. Within a BCT there are no organic CI OMTs or CI teams in the MI company. CI support pushed down to the BCT must include an OMT or be controlled by the BCT S-2X/CICA. CI teams pushed down to the BCT conduct operations in a DS role throughout the brigade's AOR during contingency or combat operations.

JOINT OPERATIONS

6-56. In a joint or combined operation, the J-2X and the TFCICA are the senior authorities for the conduct of all CI agencies involved in the operation. All subordinate Army G/S-2X and CICAs will coordinate and deconflict their CI and HUMINT activities with the senior JTF J-2X and TFCICA. In a JTF, DOD policy and joint doctrine will be the basis for the conduct of all CI operations throughout the joint operational environment.

6-57. Subordinate Army element CI assets may use service specific doctrine for guidance but must ensure that activities are conducted within the parameters established by the JTF. The separate military departments always remain in control of CI investigations. The ACICA provides investigative technical channels for all Army CI-conducted investigations. While Army CI investigative reports will pass through the CICA and *2X, they will go simultaneously to the ATCICA and ACICA.

SUPPORT TO CONTINGENCY OPERATIONS

6-58. The initial phase of operations from peacetime military engagement to major theater war lays the foundation of future team operations. In general, the priority of effort focuses inward on security of operating bases, areas of troop concentration, and C2 nodes to identify the collection threat to US forces that could be used by adversary elements to plan hostile acts against US activities and locations.

6-59. Once security of the operating bases has been established, the operational focus of CI teams shifts outside the operating base to continue to detect, identify, and neutralize the collection threat to US forces as well as to provide I&W of hostile acts targeting US activities. The CI team uses several collection methods, to include CFSO, elicitation, and liaison, to answer the supported commander's requirements. This is referred to as the continuation phase. The CI team conducts CI investigations to identify, neutralize, and exploit reported threat intelligence collection efforts.

6-60. A key element to the CI team's success is the opportunity to spot, assess, and develop relationships with potential sources of information. Operating as independent teams, without being tied to ISR or combat assets, enables the CI team's maximum interaction with the local population, thereby maximizing the pool of potential sources of information. Along with the opportunity to spot, assess, and interact with potential sources of information, a second key element of a CI team's success is its approach ability to the local population. A soft posture enables a CI team to appear nonthreatening. Experience has shown that the local population in general is apprehensive of fully and openly armed patrols and Soldiers moving around population centers.

6-61. During some operations, civilian attire or nontactical vehicles may be used to lower the CI team profile. In some special situations, these measures are taken to make the operation less visible to the casual observer. Also, in some cultures, sharing food and beverages among friends is expected; exceptions to restrictions or general orders should be considered to facilitate successful CI team operations, many of which are geared towards developing relationships with potential sources of information.

SUPPORT TO INSTALLATIONS AND OPERATING BASES

6-62. CI teams, as part of a multi-agency team consisting of MPs, CA, medical, and explosive ordnance disposal, support the conduct of threat assessments and vulnerability assessments of installations and operating bases to identify the intelligence threat to the operating locations. Detailed threat assessments and vulnerability assessments identify weaknesses in operational and physical security procedures and recommend countermeasures to mitigate intelligence collection on friendly forces. Threat assessments and vulnerability assessments limit the ability of the threat to plan hostile acts on US activities and locations. CI activities supporting installations and operating bases include—

- Interviewing walk-in sources and LEP.
- Screening LEP. Commanders, staff planners, and G-2/S-2s should always provide input to personnel assigned to establish and negotiate contracts using LN hires. This requirement ensures that LN hires can be screened, interviewed, and in some instances used as CI sources or assets in order to provide intelligence information that impacts the security of the base camp.
- Debriefing friendly force personnel who are in contact with the local population, such as—
  - ISR patrols.
  - MP patrols.
  - Combat patrols.
  - Liaison personnel.
  - CA and PSYOP teams.
- Conducting limited local open-source information collection.
- Providing support to threat assessments and vulnerability assessments of the base camp.

OPERATIONAL CONSIDERATIONS

6-63. CI must be represented and integrated into all phases of operational planning. The success of a CI team is measured by the operational emphasis, resourcing, and equipping they receive from their supported command. While operational security and freedom of movement are critical to effective CI operations, conditions within the AO—specifically high threat areas—will often require the CI team to find non-

doctrinal solutions to allow them to operate. This may mean the CI team is paired with other combat and non-combat units to facilitate movement in a particular AO.

6-64. The mission of the CI team must be integrated into the overall scheme of maneuver in order to support the commander's requirements. CI teams are often resourced or outfitted with non-TOE equipment, resources, and personnel that serve a specific purpose and provide them a unique capability to support their commander. These resources should not be used for non-CI missions or redirected without the commander's approval; if this occurs, the commander is accepting a significant degradation to the unit's ISR capability.

TACTICS, TECHNIQUES, AND PROCEDURES

6-65. At the CI team level, team members conduct mission analysis and planning specific to their AO. Backwards planning and source profiling are used extensively to choose CI targets. To verify adequate area coverage, the CI team may periodically develop and use CI target overlays and other CI analytical tools that illustrate the CI situation, identify CI gaps, and help refocus the collection effort.

6-66. The CI team is also in constant contact with the supported S-2 and the other ISR assets (Scouts, PSYOP, CA, and MP) in order to coordinate and deconflict operations and to cross-check collected information. The supported unit S-2, with the help of the CI team, regularly and systematically debriefs all ISR assets.

6-67. The CI team must be integrated into the supported unit's ISR plan. The CI OMT chief will advise the supported unit on the specific capabilities and requirements of the team to maximize mission success.

OPERATIONAL RISK MITIGATION

6-68. The employment of CI teams includes varying degrees of contact with the local population. As the degree of contact with the population increases, both the quantity and quality of CI collection increases. In many instances, however, there is a risk to the CI team inherent with increased exposure to the local population. The decision at what level to employ a CI team is METT-TC dependent. The risk to the CI assets must be balanced with the need to collect on PIRs and to protect the force as a whole. ROE, SOFA, direction from higher headquarters, and the overall threat level may also restrict the deployment and use of CI teams.

6-69. Risks are minimized through the situational awareness of CI team members. They plan and rehearse to readily react to any situation and carry the necessary firepower to disengage from difficult situations. If it becomes necessary to call for assistance, adequate and redundant communications equipment is critical. These scenarios and actions should be trained prior to deployment into a contingency area and rehearsed continuously throughout the deployment.

6-70. A supported unit commander is often tempted to keep the CI team within friendly bases when the threat condition level increases. The supported commander must weigh the risk versus potential information gain when establishing operational parameters of supporting CI teams. This is necessary especially during high threat condition (THREATCON) levels when the supported unit commander needs as complete a picture as possible of the threat arrayed against US and multinational forces.

6-71. When it is not expedient to deploy the CI team independently due to THREATCON levels or other restrictions, the team can be integrated into other ongoing operations. The CI team may be employed as part of a combat, ISR, or MP patrol or used to support CA, PSYOP, engineer, or other operations. This method reduces the risk to the team while allowing a limited ability to collect information. It also has the advantage of placing the team in contact with the local population and allowing it to spot, assess, and interact with potential sources of information. However, this deployment method restricts collection by subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into which it is integrated and does not allow for the conduct of sensitive source operations.

Note. This method of employment should be considered a last resort.

INTEGRATION OF LINGUISTS

6-72. Integrating linguists into the CI team should take place as soon as possible. Security clearances and contractual agreements will help the team determine the level of integration.

6-73. Along with the basic briefing of what is expected of the civilian linguists as interpreters, CI teams should be informed about civilian chain of command and the scope of their duties beyond interpreting. The CI team leader must ensure that linguists are trained and capable of completing all tasks expected of them.

COUNTERINTELLIGENCE EQUIPMENT

6-74. Basic C2, transportation and weapons requirements do not differ significantly from most Soldier requirements and are available as unit issue items. However, CI teams have unique communications, collection, processing, and mission-specific requirements.

COMMUNICATIONS

6-75. Dedicated and Secure Long-Range Communications. These are keys to the success of the CI team mission. CI team operations require a secure, three-tiered communications architecture consisting of inter- and intra-team radios, vehicle-based communications, and a CI and HUMINT base station.

6-76. Communications Network. The CI team must have access to existing communications networks such as the tactical LAN. The CI team must also be equipped with its own COMSEC devices. It is imperative that the CI team acquire access to the public communication system of the HN. This can be in the form of either landlines or cellular telephones. Such access enables the CI team to develop leads which can provide early indicators to US forces.

6-77. Interoperability. Communications systems must be equipped with an open-ended architecture to allow for expansion and compatibility with other service elements, government organizations, NGOs, and multinational elements to effectively communicate during CONOPs. All ISR systems must be vertically and horizontally integrated to be compatible across all warfighting functions and with all US Army organizations.

6-78. Satellite Communications On The Move. To provide real-time and NRT information reporting, CI elements must have the capability to transmit voice, data, imagery, and video while on the move. CI teams must be able to transmit while geographically separated from their parent unit while operating remotely. This broadband requirement can only be achieved through a satellite communications capability and must be achievable while mobile.

CI COLLECTION AND PROCESSING SYSTEMS

6-79. The CI team must rely on automation to achieve and maintain information dominance in a given operation. With time, effective collection planning and management at all echelons, the CI team can collect a wealth of information. The processing and analysis of this information in a timely and efficient manner are crucial to operations. Automation helps the CI team to report, database, analyze, and evaluate the collected information quickly and to provide the supported unit with accurate data in the form of timely, relevant, accurate, predictive, and tailored intelligence.

6-80. Automation hardware and software must be user friendly as well as interoperable among different echelons and services. They must interface with the communications equipment of the CI team as well as facilitate the interface of audiovisual devices. Technical support for hardware and software must be available and responsive.

6-81. The demand for accurate and timely CI reporting, DOMEX, and open-source information has grown tremendously. Biometric (physiological, neurological, thermal analysis, facial and fingerprint recognition) technologies will allow rapid identification, coding, and tracking of adversaries and human sources; as well as cataloging of information concerning EPWs, detainees, and civilians of CI interest on the battlefield. Biometrics will also provide secure authentication of individuals seeking network or facility access.

6-82. CI teams work with multinational forces and other foreign nationals and require the ability to communicate in their respective languages. Often CI personnel have little or no training in the target language, and lack of skilled interpreters can hinder CI activities. CI teams require textual and voice translation devices, source verification, and deception detection machines (biometrics) to improve collection capability and accuracy.

6-83. CI teams require dynamic machine language translation tools that provide both non-linguists and those with limited linguist skills a comprehensive, accurate means to conduct initial CI screenings and basic interviews in a variety of situations. CI elements will focus on in-depth interviews and communications with persons of higher priority. Machine language translation tools minimize reliance on contract linguists and allow Soldiers to concentrate on mission accomplishment.

MISSION SPECIFIC

6-84. In order to conduct night operations, each CI team member must be equipped with night vision devices, photographic equipment, and weapons. The CI team also may operate in urban and rural areas, where the threat level can vary from permissive to hostile. Some of the CI team missions may require the documentation of incidents. The CI teams can use the following equipment in their open-source collection efforts.

- Small, rugged, battery-operated digital camcorders and cameras which are able to interface with the collection and processing systems as well as communication devices.
- Global positioning systems that can be mounted and dismounted to move in the AO efficiently.
- Short-range multichannel RF scanning devices that can also identify frequencies which enhance their security.
- In some cases CI teams require a stand-off, high resolution optical surveillance and recording capability that can provide target identification at extended ranges to protect the intelligence collector while avoiding detection by the adversary target. An advanced optical capability provides intelligence collectors the ability to locate and track adversary targets (passive and hostile) for identification, collection, and target exploitations. High power, gyro-stabilized binoculars—which can be used from a moving vehicle—increase the survivability of the CI team and also give the team another surveillance and collection device.

Chapter 7

Human Intelligence

HUMAN INTELLIGENCE-RELATED DEFINITIONS AND TERMS

7-1. HUMINT is a category of intelligence derived from information collected and provided by human sources (JP 2-0).

7-2. A HUMINT source is a person from whom 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, EPWs, refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and nongovernmental organizations (NGOs).

7-3. A HUMINT collector is a person who is trained 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 MOS 35M, warrant officers in MOS 351C and 351M, commissioned officers in MOS 35F, and their Federal civilian employee and civilian contractor counterparts. Trained means successful completion of one of the following courses, which are the only accepted sources of interrogation training for military personnel:

- 35M Basic HUMINT Collector Course at US Army Intelligence Center, Fort Huachuca, AZ.
- US Marine Corps Basic Marine Air-Ground Task Force (MAGTF) CI/HUMINT Course at the Navy and Marine Corps Intelligence Center, Dam Neck, VA.
- Joint Interrogation Certification Course at HUMINT Training-Joint Center of Excellence, Fort Huachuca, AZ.
- Defense Intelligence Agency I-10 Course in Alexandria, VA.

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

7-4. HUMINT collection operations must be conducted in accordance with all applicable US law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, DOD Directive 2310.1E, DOD instructions, FM 2-22.3, and military execute orders including fragmentary orders. Additional policies and regulations apply to the management of contractors engaging in HUMINT collection. (See FM 2-33.3, appendix K.)

ROLE OF HUMAN INTELLIGENCE

7-5. HUMINT operations focus on determining the capabilities, threat characteristics, vulnerabilities, and intentions of enemy and potential threat forces. The operations target actual and potential adversary decision-making architecture with the intent of helping to shape friendly forces' visualization of enemy and potential threat forces. HUMINT collection activities and operations include tactical questioning, screening, interrogation, debriefing, liaison, human source operations, DOMEX, and CEE operations.

7-6. Once the type of operation has been determined, leaders use the operations process of plan, prepare, execute, and assess to conduct the operation. The following paragraphs briefly discuss the different types of HUMINT operations.

HUMINT COLLECTION METHODOLOGIES

7-7. 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, and reporting. They 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.

7-8. HUMINT collection methodologies include five general categories:

- Screening.
- Interrogation.
- Debriefing.
- HUMINT Collection in Military Source Operations.
- Liaison.

SCREENING OPERATIONS

7-9. Screening is the process of evaluating and selecting human sources and documents for the prioritized collection of information based on the collection requirements and mission of the unit conducting the screening or its higher headquarters. Screening categorizes and prioritizes sources based on the probability of a particular source having priority information and the level of cooperation of the source. Screening is also used to determine if a source matches certain criteria that indicate that the source should be referred to another agency. Screening is conducted at all echelons of command and in all operational environments. There are two general categories of screening: human source screening, and document and media screening.

7-10. Media is screened for content which answers PIRs or other information of intelligence interest. Screening operations also assist to determine which intelligence discipline or agency could best conduct the exploitation of a given source. Screening operations include, but are not limited to—

- Tactical screening in support of combat or contingency operations.
- Checkpoint screening (mobile or static) of local populations as they transit through and within the AO or to screen large numbers of individuals such as refugees or DP as they enter the AO.
- Local population screening of personnel within their own neighborhoods.
- Collection facility screening conducted as a normal part of HUMINT collection operations at collection facilities, such as theater interrogation and debriefing facilities and refugee camps.
- Local employee screening to determine possible security risks or identify sources who can provide information in response to CCIR.

INTERROGATION OPERATIONS

7-11. Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Some examples of interrogation sources include EPWs and other detainees. Interrogation sources range from totally cooperative to highly antagonistic. Interrogations may be conducted at all echelons in all operational environments.

7-12. Detainee interrogation operations conducted at a Military Police (MP) facility, multinational-operated facility, or other agency-operated collection facility are more robust and require greater planning,

but have greater logistical support. Interrogations may only be conducted by personnel trained and certified in the interrogation methodology, including personnel in MOSs 97E, 351M (351E), or select others as may be approved by DOD policy. Interrogations are always to be conducted in accordance with the Law of War, regardless of the echelon or operational environment in which the HUMINT collector is operating.

7-13. Interrogation operations are specific operations normally conducted at detainee collection facilities directed at the wide-scale collection of information from detainees using interrogation techniques. Although field interrogations are conducted at all echelons and during all operations in which there are detainees, detention facilities where interrogation operations occur are normally located only at theater or JTF level.

DEBRIEFING OPERATIONS

7-14. Debriefing is the systematic questioning of cooperating human sources to satisfy intelligence requirements consistent with applicable law. The source is usually not in custody and is usually willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments. The primary categories of sources for debriefing are refugees, émigrés, displaced persons, local civilians, and friendly forces.

FRIENDLY FORCE DEBRIEFING OPERATIONS

7-15. Every member of the friendly force is a potential source for HUMINT collection. Friendly force personnel frequently have contact with the threat, civilian population, or the environment. Although many individuals report their information in the form of combat information, many do not report the information, do not realize its significance, or do not know how to report key information. Frequently a systematic questioning by a trained HUMINT collector will identify key information that can contribute to the intelligence picture and help an individual recall details. It also helps to place this information into a systematic format for the analyst to use.

HUMINT COLLECTION IN MILITARY SOURCE OPERATIONS

7-16. HUMINT collection in Military Source Operations (MSO) are directed toward the establishment of human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. Within the Army, MSO are conducted by trained personnel under the direction of military commanders. The entire range of HUMINT collection operations can be employed.

7-17. MSO sources include one-time contacts, continuous contacts, and formal contacts from debriefings, liaison, and contact operations. MSO consist of collection activities that utilize human sources to identify attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel, and capabilities of those elements that pose a potential or actual threat to US and multinational forces. MSO are also employed to develop local source or informant networks providing early warning of imminent danger to US and multinational forces and contribute to mission planning.

7-18. Formal contacts are individuals who have agreed to meet and cooperate with HUMINT collectors for the purpose of providing information. HUMINT collectors who have met with a particular continuous contact three or more times should consider assessing the contact for use as a formal contact. Formal contacts can be tasked, trained, and paid. Formal contacts meet repeatedly with HUMINT collectors, and their operation and tasking must be carried out in accordance with FM 2-22.3. Formal contacts are employed to develop HUMINT sources who can provide early warning of imminent danger to US and multinational forces and contribute to mission planning.

7-19. HCTs must be able to travel to meet sources and be able to remain at a meeting location for long enough to conduct their meeting. This requirement to remain in one location for up to several hours means that HUMINT teams require dedicated security. Placing an HCT with a combat patrol for movement will

not serve to provide them with the support they need for stationary operations since combat patrols need to keep on the move.

LIAISON OPERATIONS

7-20. Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander. The HUMINT collector meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information. Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison normally tends to reflect the official positions of their superiors and may not be entirely accurate or complete.

SUPPORT TO DOMEX, SITE EXPLOITATION, AND CAPTURED ENEMY EQUIPMENT EXPLOITATION OPERATIONS

7-21. The execution of DOMEX, site exploitation, and CEE exploitation operations is not exclusively a HUMINT function but may be conducted by any intelligence personnel with appropriate language support. Of particular interest to HUMINT collectors are CEDs. A CED is any document that has been in possession of the enemy, whether or not the enemy has created it for their use. HUMINT collectors can very effectively use CEDs to further exploit information of intelligence value during the conduct of operations.

CAPABILITIES AND PLANNING CONSIDERATIONS

7-22. The fundamentals of HUMINT include capabilities and planning considerations as discussed below.

CAPABILITIES

7-23. HUMINT collection capabilities include the ability to—

- Collect information and cross-cue from an almost endless variety of potential sources including friendly forces, civilians, detainees, and source-related documents.
- Focus on the collection of detailed information not available by other means. This includes information on threat intentions and local civilian and threat force attitudes and morale. It also includes building interiors and facilities that cannot be collected on by other means due to restrictive terrain.
- Corroborate or refute information collected from other reconnaissance and surveillance (R&S) assets.
- Operate with minimal equipment and deploy in all operational environments in support of offensive, defensive, stability and reconstruction operations, or civil support operations. Based on solid planning and preparation, HUMINT collection can provide timely information if deployed forward in support of maneuver elements.

PLANNING CONSIDERATIONS

7-24. The following are important considerations when conducting planning for HUMINT operations.

- **Interpersonal skills.** HUMINT is dependent on the subjective interpersonal capabilities of the individual rather than on the abilities to operate collection equipment. HUMINT collection capability is based on experience within a specific AO that can only be developed over time.
- **Availability of trained and certified personnel.** There are never enough HUMINT collectors to meet all requirements. Limited assets must be prioritized in support of units and operations based on their criticality.

- **Time.** HUMINT collection, particularly source operations, takes time to develop. Collection requirements must be developed with sufficient lead time for collection.
- **HUMINT language limitations.** While HUMINT collectors can normally use an interpreter, a lack of language proficiency by the collector can significantly slow collection efforts. Such language proficiency takes time to develop.
- **Misuse of HUMINT personnel.** HUMINT collectors are frequently utilized incorrectly and assigned missions that belong to CA, MP, CI, interpreters, translators, or other operational specialties for which they are not trained or certified to conduct or supervise. Employing HUMINT collectors in any capacity other than HUMINT collection missions severely impacts their ability to answer intelligence requirements.
- **HUMINT collection capability.** HUMINT collection capability is limited when commanders do not provide support specifically to the HCT for the conduct of HUMINT collection missions. Often HCTs are required to travel with patrols in order to have mobility within the AO. While this does get the HCT off the base or camp, it does not allow them the time or flexibility to conduct a HUMINT collection mission. The nature of patrol missions requires them to keep on the move most of the time. HUMINT collection missions often require the HCT to remain at location for extended periods. In order for HUMINT collection missions to be successful, commanders must provide dedicated mission support to allow for this requirement.
- **HUMINT risk management.** Maneuver commanders, in weighing the risks associated with employing HCTs, should consider the potential loss of a wealth of information such as enemy activities, locations of high-value personnel, and threats to the force that they may incur if they restrict HCT collection activities.
- **HUMINT legal obligations.** Applicable US law and regulations and international law govern HUMINT collection operations. HUMINT operations may be further restricted by SOFAs and other agreements, execution orders, ROE, and local laws. Such documents, however, cannot permit interrogation actions which are illegal under US or international law.
- **HUMINT connectivity and bandwidth requirements.** With the exception of the SALUTE report, most HUMINT reporting requires considerable bandwidth. Deployed HCTs must be able to travel to and report from all areas in the AO. Digital communication equipment must be able to provide reliable connectivity with team reporting channels and sufficient bandwidth for transmission of reports, including digital imagery.
- **HUMINT reporting and immediate access to sources.** Except in tactical situations when HUMINT collectors are in immediate support of maneuver units, HUMINT collection and reporting takes time. In stability operations, sources need to be assessed and developed. Once they are developed, they need to be contacted which often takes time and coordination. In offensive and defensive operations, HUMINT collection at EPW holding areas sometimes may still be timely enough to meet tactical and operational requirements.

HUMAN INTELLIGENCE ORGANIZATIONS

7-25. Brigade Combat Team (BCT). The BCT's organic MI Company's Ground Collection Platoon has one four-person HUMINT OMT (consisting of a WO (351M), a HUMINT NCO (35M) and two junior enlisted Soldiers (35M) and three organic four-person HCTs (consisting of one E6 35M3L, one E5 35M2L, one E4 35M10, and one E3 35M10). The HUMINT OMT provides the first level of technical channels, as well as management to subordinate HCTs that conduct HUMINT operations. The OMT must be prepared to control any additional HCT that may be pushed down from higher echelon to support the BCT.

7-26. Stryker Brigade Combat Team (SBCT). The SBCT's organic MI Company's CI and HUMINT Collection Platoon has two organic HUMINT OMTs and four organic HUMINT teams, each with an organic CI agent. Additional HCTs (and OMTs) may be pushed down to the SBCT from the Division MI

Battalion. Within the SBCT Reconnaissance Squadron there is a total of 36 HUMINT collectors (35M) organic (12 per Reconnaissance Troop, four per Platoon, one per Squad.)

7-27. Division. Within a Division the Battlefield Surveillance Brigade (BFSB) MI Battalion has three companies with HUMINT assets, and a HUMINT and CI team organic to the BFSB S-2. The C&E company has three HUMINT OMTs that control a total of 12 HCTs. The C&E company provides general support coverage for the division. The two CI/HUMINT companies each has four organic HUMINT OMTs that each controls a total of 16 HCTs. The CI/HUMINT company provides DS to the BCT. When HCTs are pushed down to SBCT or BCT level, OMTs may also be required to be pushed down to control the additional HUMINT assets.

7-28. Theater. At Theater or JTF level, the INSCOM Military Intelligence Brigade has HUMINT assets that could be employed as HUMINT OMTs and HCTs to provide coverage for the supported unit or that could be pushed down to subordinate units.

7-29. ASCC. HUMINT operations to satisfy Army-level intelligence requirements are satisfied by INSCOM's Army Operational Activity. The Army Operational activity also has the capability to provide HUMINT subject matter expert support to deployed commanders.

HUMAN INTELLIGENCE AUTHORITIES

7-30. The Secretary of Defense (SECDEF) has designated the Director of DIA as the Defense HUMINT Manager for the entire DOD. To assist the Defense HUMINT manager, a new organization called the Defense HUMINT Management Office has been established to provide standardization across DOD for HUMINT policy, training, and operations.

7-31. The Undersecretary of Defense for Intelligence has promulgated new policy for the conduct of DOD HUMINT. The new policy designates the CCDRs, the Director of DIA, and the military service senior intelligence officers (Headquarters, Department of the Army [HQDA] DCS, G-2) as HUMINT executors. The SECDEF has given the HUMINT executors authority to approve their respective component's HUMINT activities in support of military operations. This means that the Army DCS G-2, can approve HUMINT activities conducted by the US Army in support of departmental or CCDR requirements.

HUMAN INTELLIGENCE TECHNICAL CHANNELS

7-32. HUMINT falls under the appropriate echelon 2X. See chapter 6 for details about 2X operations.

Chapter 8

Geospatial Intelligence

INTRODUCTION

8-1. There are many producers of GEOINT, and the users of GEOINT extend from the national level down to the lowest tactical level. The overall GEOINT enterprise that supports operations extends across all Services, multinational partners, and other organizations during joint operations and unified action. GEOINT requirements, methods of collection (and associated systems), and products vary widely based on the echelon of support and the various types of operations.

8-2. The Army does not conduct GEOINT operations in isolation. GEOINT is comprised of many ongoing operations and activities across DOD. The NSG manages operations through guidance, policy, programs, and organizations. The NSG is the combination of technology, policies, capabilities, doctrine, activities, people, data, and communities necessary to produce GEOINT in the form of integrated intelligence across multiple environments. The NSG community consists of members and partners:

- Members include the intelligence community, joint staff, military departments (to include the Services), and combatant commands.
- Partners include civil applications committee members, international partners, industry, academia, defense service providers, and civil community service providers.

NATIONAL SYSTEM FOR GEOSPATIAL-INTELLIGENCE AND NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

8-3. The Director of NGA serves as the functional manager for GEOINT in accordance with applicable laws, DNI and DOD directives, guidance, and agreements. In that role, Director, NGA, also informs and guides NSG activities on GEOINT operations. Additionally, the NSG functional manager is responsible for the "end-to-end GEOINT process"; sets standards for the GEOINT architecture and products; and provides technical guidance for systems using GEOINT.

8-4. Title 10 US Code § 467 establishes GEOINT. GEOINT 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. GEOINT consists of imagery, imagery intelligence, and geospatial information* (NGA Publication 1).

- **Imagery:** A likeness or representation 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 representations produced by satellites, airborne platforms, unmanned aircraft systems (UASs), or similar means This does not include handheld or clandestine photography taken by or on the behalf of HUMINT collection organization.
- **Imagery Intelligence:** The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.
- **Geospatial Information:** Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including statistical data and information derived from, among other things, remote sensing, mapping and surveying technologies, and mapping, charting, geodetic data, and related products.

8-5. The NGA as the functional manager published NSG Publication 1, the capstone GEOINT doctrine publication, in September 2006. This NSG doctrine explains that GEOINT is an intelligence discipline that has evolved from the integration of imagery, IMINT, and geospatial information. The basic capabilities and products of these three areas still exist as the foundation of GEOINT.

8-6. NSG doctrine discusses four fundamental aspects of GEOINT:

- The discipline of GEOINT.
- The data that comprise GEOINT.
- The process used to develop GEOINT products.
- The products derived from GEOINT data.

8-7. GEOINT provides a common framework for supporting joint operations to better enable mission accomplishments across the range of military operations and with all mission partners. GEOINT support to joint operations supports the multidirectional flow and integration of geospatially referenced data from all sources to achieve shared situational awareness of the operational environment, NRT tracking, and collaboration between forces. The GEOINT cell at the combatant command coordinates closely with the JFC GEOINT cell (if the combatant command and JFC are two different organizations) to ensure continuity in operations across all functions, organization levels, and levels of warfare.

8-8. GEOINT activities necessary to support joint operations include 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 and then interfaces with the NSG to obtain and provide the best quality GEOINT possible directly to the warfighter in fulfillment of the broad range of requirements depicted by the various mission functions. The GEOINT cell supports joint operations with five activities:

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

8-9. The use of GEOINT can be categorized into five general areas:

- GMI and I&W.
- Safety of navigation.
- Operational environmental awareness.
- Mission planning and C2.
- Target intelligence.

8-10. The combatant commands develop area and point target GEOINT requirements to support the planning and execution of joint operations. The GEOINT cell assigned to combatant commands is responsible for coordinating all GEOINT requirements within its AOR while ensuring that the supporting commands or component commands are executing theater and mission-specific GEOINT requirements. This includes planning provisions for war reserve requirements and enabling the COP with a GEOINT framework for all needed layers of geospatial information.

8-11. Each combatant command (except the US Strategic Command) has also established a JIOC to plan, prepare, integrate, direct, synchronize, and manage continuous full-spectrum defense intelligence operations. The goal of all JIOCs is the integration of intelligence into operations in order to increase the speed, power, and effectiveness of DOD operations. These organizations facilitate access to all available intelligence sources and analyze, produce, and disseminate timely, relevant, accurate, predictive, and tailored all-source intelligence and GEOINT to support planning and execution of military operations. The combatant commands have imagery exploitation capabilities and geospatial information and services capabilities.

8-12. The types of imagery-derived products generated by the combatant commands include text reports, database entries, target materials and support products, visualization products, and annotated graphics. The GEOINT cell provides advice to the CCDR on all geospatial information and geodetic sciences. While the combatant commands rely heavily on basic maps, charts, target coordinates, geodetic surveys, and other standard geospatial information provided by NGA, they also research, develop, and produce their own mission-specific, specialized geospatial products and services for the CCDR and components. These products (for example, aeronautical and hydrographic products, terrain graphics and data, charts, perspective views, image graphics, target materials) provide value-added improvements to NGA digital products.

8-13. The NGA support team (NST) is the primary mechanism for interaction between the combatant commands and NGA. The NST coordinates NGA's operational, policy, and training support to its customers. NGA maintains NSTs at the Joint Staff, combatant commands, Services, and DOD agencies.

8-14. A typical NST is composed of a senior representative (a military O-6 or a defense intelligence senior leader), staff officers, and imagery and geospatial analysts. A reach component at NGA HQ focuses NGA production support. In addition to using NSTs, NGA may deploy crisis or geospatial support teams of imagery and geospatial analysts upon request, either independently, as augmentation to an existing NST, or as part of a NIST. A NIST is a nationally sourced team composed of intelligence and communications experts from DIA, CIA, National Security Agency (NSA), or any combination of these agencies.

8-15. A NIST is a nationally sourced team composed of intelligence and communications experts from DIA, CIA, NSA, or any combination of these agencies. These teams of government and/or contract personnel employ deployable GEOINT production systems. NST personnel have reachback to NGA for data and products, fuse this information with tactical and theater sources, and work with users to produce products tailored to their needs. For more information on joint GEOINT doctrine, refer to JP 2-03.

GEOSPATIAL INTELLIGENCE WITHIN ARMY DOCTRINE

8-16. Based on the Army's organizational construct, GEOINT is described as intelligence derived from the exploitation and analysis of imagery with geospatial information to describe, assess, and visually depict physical features and geographically referenced activities in the operational environment. GEOINT consists of imagery, IMINT, and geospatial information.

8-17. There are unique characteristics of each Service's portion (or extension) of the GEOINT enterprise. Each member of the enterprise has unique requirements. Within intelligence, the nature of a Service's requirements drives the conduct of unique intelligence operations (tasking, collection, processing, exploitation, dissemination, and the ultimate presentation).

8-18. Army GEOINT operations are complementary to NGA and joint operations, and the Army works within the same enterprise (the NSG) to improve the quality of intelligence support to all operations. Both the Army Intelligence and Engineer communities recognize the DOD GEOINT enterprise—and everything encompassed in the enterprise—and acknowledge GEOINT as an intelligence discipline. However, the Army doctrinal distinction is based on the operational construct of an intelligence discipline that is intelligence-product oriented. The full power of GEOINT for the Army is achieved from the integration and analysis of all three capabilities, which results in more comprehensive and tailored intelligence products for a wide scope of Army requirements and users across all of the warfighting functions.

8-19. The Army implements GEOINT through both Engineer and MI units. Previously, Engineer and MI units worked independently in the creation of GEOINT products. Currently, permanent Geospatial Planning Cells (GPCs) are situated at the Army Service Component Command (ASCC); and the creation of GEOINT Cells from the Brigade Combat Teams (BCT) to the ASCC provide for fully fused GEOINT analysis functions as an inherent capability of J-2/G-2/S-2. The primary GEOINT services each brings to the GEOINT cells are—

- MI units and organizations provide imagery and IMINT to the enterprise.

- Engineer (topographic) units and organizations provide geospatial data and information to the enterprise.

8-20. Geospatial engineer units that are located at the ASCC level are the GPCs. The GPC's mission is to collect, create, manage, and disseminate geospatial data, information and products for their AOR. The GPC is responsible for providing the geospatial data, information, and products to geospatial engineering units for dissemination to Army Battle Command Systems (ABCS) and to coordinate the acquisition and production activities of geospatial engineering units operating within the GPC's AOR. The GPC also coordinates with NGA, host or allied nation geospatial support activities, and higher headquarters in order to create and maintain geospatial architecture from national to tactical levels.

8-21. The conduct of operations depends on geospatial data and imagery. That geospatial data and imagery is the foundation for the COP, and it facilitates situational understanding for all of the warfighting functions. The COP is a critical tool to integrate all Army operations by providing a common view of operations and the operational environment. One of the primary data managers for the COP is the geospatial engineer (within the GEOINT cell) at every echelon. The GEOINT cell is responsible for creating and maintaining the GEOINT database of the COP. The GEOINT database establishes the geospatial data foundation for the GEOINT cell. These databases include enterprise databases such as Theater Geospatial Database (TGD) and Imagery Product Library (IPL).

8-22. The GEOINT cell provides direct support to create GEOINT products. The GEOINT cell is responsible for coordinating GEOINT requirements within the AOR. The GEOINT cell provides the commander visualization of the battlespace and manages the geospatial and imagery foundations of the COP. GEOINT cells provide a collaborative environment for the geospatial engineer and imagery analyst to achieve maximum development of GEOINT products.

8-23. A cell is a group of personnel with specific skills brought together to accomplish key functions. GEOINT cells are comprised of geospatial engineers and imagery analysts working together to provide commanders a more complete picture of the physical environment and infrastructure in his operational environment. The advantages of GEOINT cells include centralized GEOINT production, synchronization of effort, reduction of redundancy, and maximization of the imagery analyst and the geospatial engineer skills.

8-24. There are other differences in the Army construct: The Army—

- Views the current categories of imagery, IMINT, and geospatial information as sufficient and more specific for Army purposes. GEOINT is unique and necessary to describe a value-added to intelligence operations through analysis and integration and/or combination of imagery, IMINT, and geospatial information.

Note. According to NSG Publication 1-0, "Almost any type of GEOINT can be produced without using intelligence analysis …."]

- Geospatial engineers are not the sole providers of geospatial data and information to the enterprise. All Soldiers and units provide this data; the geospatial engineers verify and manage this data for the Army. Geospatial engineers also produce data and GEOINT products, enhance existing data, reconcile data conflicts, and analyze and disseminate data.
- Maintains a tactical intelligence architecture and uses systems that are significantly different from the other aspects of the GEOINT enterprise. NGA develops GEOINT architecture and standards for the GEOINT enterprise. Army intelligence units and organizations do not control all the different forms of data (imagery and geospatial), the different systems, and the tactical C2 network.
- Manages commander's requirements for information that falls across all of the Army's warfighting functions and differs from NGA requirements to support DOD.

- Has a doctrinal information hierarchy established in FM 6-0 that builds from data to information to knowledge to understanding. In this hierarchy, intelligence (depending on the level of detail) can be resident anywhere from the information to the understanding levels.

8-25. The Army recognizes, as stated in NSG Publication 1-0, that GEOINT's added value is based on the prerequisite for analysis and the integration and/or combination of all three elements which results in more comprehensive and tailored intelligence support. Also, just like NGA, Army doctrine recognizes four fundamental aspects of GEOINT:

- GEOINT as an intelligence discipline. The GEOINT discipline encompasses all intelligence tasks and intelligence activities involved in the planning, collection, processing, analysis, exploitation, and dissemination of GEOINT.
- GEOINT as the product defined above.
- Unique processes used to develop GEOINT.
- Unique data that is used to develop GEOINT.

8-26. The goal of Army GEOINT operations is to provide tailored products that serve as the foundation for the COP and facilitate the commander's gaining situational understanding. Just as it states in NSG GEOINT Basic Doctrine Publication 1-0, "Advances in technology and the use of geospatial data have created the ability to integrate and/or combine elements of any or all of the areas, along with other elements of information, resulting in many new, more sophisticated capabilities for producing products and conducting analysis. … Advanced technology now provides the capability to use and combine geospatial data in different ways to create interactive/dynamic, customized visual products. It allows the analyst to quickly make more complex connections between different types of data and information than previously possible." GEOINT is a major step toward improving Army intelligence and intelligence operations

Chapter 9

Imagery Intelligence

DEFINITION

9-1. *IMINT is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials* (JP 2-03).

9-2. Imagery analysis is the science of converting information extracted from imagery into intelligence about activities, issues, objects, installations, and/or AOIs.

9-3. 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 likeness and presentations produced by satellites, airborne platforms, UASs, 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).

ROLE

9-4. The role of IMINT is to assist the commanders in applying and protecting their combat power. Imagery often enhances the commander's situational understanding of the AO. Imagery assets, particularly MTI systems, are useful in cueing other ISR systems. Other than direct human observation, imagery is the only intelligence discipline that allows the commanders to see the AO in NRT as the mission progresses. In those cases where maps are not available, digital imagery in hardcopy or softcopy can be used as a substitute. Imagery can also be used to update maps or produce grid-referenced graphics. Detailed mission planning often requires imagery, to include three-dimensional stereo images, in order to provide the degree of resolution necessary to support such specialized planning. (See FM 2-22.501, when published, for more information on IMINT.)

FUNDAMENTALS

9-5. Some imagery assets are very responsive to the individual CCIRs. Some imagery systems can directly transmit imagery into the tactical operations center; examples include imagery from unmanned aircraft systems and the Joint Surveillance Target Attack Radar System and Airborne Reconnaissance Low (ARL). This direct downlink enables the G-2/S-2 to use the imagery as soon as possible instead of having to wait for finished imagery products. Anyone can look at an image but a trained imagery analyst is necessary to accurately assess the intelligence value of the imaged data.

9-6. Imagery-related equipment has undergone a reduction in size as well as a reduction in the time it takes to provide products, particularly softcopy imagery. The modularity and size reduction of imagery analysis, processing, and display systems makes transport easier; this allows commanders to deploy with fewer systems than in the past and still retain those capabilities and systems (or subsystems) required to complete the mission. Imagery and imagery considerations include bandwidth, classification, releasability, and necessary equipment and software for imagery analysts to perform their mission. Additionally, data compression allows faster transmission of imagery products directly to the warfighter.

SOURCES OF IMAGERY

9-7. There are two general sources of imagery: national technical means and commercial that includes satellite and airborne platforms. National imagery traditionally refers to imagery collected by DOD imagery systems. However, there are other sources of imagery provided by non-national sources such as the shuttle radar topography mission and commercial remote sensing efforts.

NATIONAL TECHNICAL MEANS

9-8. National systems are developed specifically for supporting the President of the United States, the SECDEF, other national agencies, and US military forces. These systems respond to the needs of the nation and those of the combatant commands.

COMMERCIAL

9-9. Commercial companies build, launch, and operate satellite and airborne imagery systems for profit. In times of crises, license agreements with the US Government obligate US commercial satellite imaging systems to provide data only to the US Government at the market value. This protects information concerning US operations from threat exploitation from commercial systems such as the Google Earth. However, the US Government could never afford to buy all the commercial imagery available for a crisis and foreign commercial imagery systems are not bound to this arrangement, so these imagery sources may be used by our nation's enemies and adversaries. Commercial imagery has become increasingly valuable for many reasons:

- Due to its unclassified nature, civil and commercial imagery is useful in an open environment, may be released to other government agencies, intergovernmental organizations, NGOs, and multinational partners, and can be made available for public release.
- The use of civil and commercial imagery allows national technical means systems more time to focus on other intelligence functions.
- Civil and commercial imagery sources and companies offer electro-optical and radar imagery. Some offer large area collection useful for broad area coverage purposes.

9-10. The National Geospatial-Intelligence Agency's Source is responsible for ordering commercial imagery. The Commercial Satellite Imagery Library and the Unclassified National Imagery Library are available to research DOD-purchased commercial imagery. The G-2/S-2 should consult the NGA Source when forming commercial imagery requests. NGA will deliver the imagery primarily on CD-ROM media via courier or mail service. Limited digital or electronic delivery is available as well.

TYPES OF IMAGERY SENSORS

9-11. There are two general types of imagery sensors: electro-optical and radar. Electro-optical sensors include panchromatic (visible), infrared, spectral (multispectral and hyperspectral), polarmetric, and light detection and ranging. Radar sensors are synthetic aperture radar systems. These systems collect and display data as either fixed target indicators or moving target indicators. Each sensor and platform has a unique capability, with distinct advantages and disadvantages. The G-2/S-2 must understand each sensor's and platform's capability in order to select the best for the mission and thus enable the user to better understand the intelligence received. Certain sensors are better suited for military operations than others. Table 9-1 lists sensor capabilities.

5062

Table 9-1. Sensor characteristics matrix

SENSORS	*ADVANTAGES*	*DISADVANTAGES*
Panchromatic (Visible) Best tool for daytime, clear weather, detailed analysis. Includes video and electro-optical.	• Affords a familiar view of a scene. • Offers system resolution that cannot be achieved in other optical systems or in thermal images and radars. • Preferred for detailed analysis and mensuration. • Offers stereoscopic viewing.	• Restricted by terrain and vegetation. • Limited to daytime use only. • Reduced picture size. • Degraded imagery in other than clear weather.
Infrared Best tool for nighttime, clear weather, detailed analysis. Includes Overhead Non-Imaging Infrared.	• A passive sensor and is impossible to jam. • Offers camouflage penetration. • Provides good resolution. • Nighttime imaging capability.	• Not effective during thermal crossover periods. • Product not easily interpretable. • Requires skilled analysis. • Cannot penetrate clouds.
Radar Useful for detecting presence of objects at night and in bad weather. Includes synthetic aperture radar, coherent change detection, and MTI.	• All weather; can penetrate fog, haze, clouds, smoke. • Day or night use. • Does not rely on visible light nor thermal radiation. • Good standoff capability. • Large area coverage. • Allows moving target detection. • Foliage and ground penetration.	• Product not easily interpretable. • Requires skilled analysis. • Terrain masking inhibits use.
Multispectral Imagery Best tool for mapping purposes and terrain analysis.	• Large database available. • Band combinations can be manipulated to display desired requirements. • Images can be merged with other digital data to provide higher resolution.	• Product not easily interpretable. • Requires skilled analysis. • Computer manipulation requires large amounts of memory and storage; requires large processing capabilities.

5063 # IMAGERY INTELLIGENCE IN THE INTELLIGENCE PROCESS

5064 9-12. The IMINT discipline has several unique considerations throughout the steps of the intelligence
5065 process.

5066 ## GENERATE INTELLIGENCE KNOWLEDGE

5067 9-13. The G-2/S-2 should research targets using online imagery databases early and request those imagery
5068 products that are not perishable for contingency planning. National and combatant command imagery
5069 databases may hold recently imaged areas that could meet the commander's immediate needs instead of
5070 requesting new imagery.

PLAN

9-14. The first step in planning for IMINT is determining the need for IMINT products based on the PIRs and the initial IPB. The staff must clearly articulate their intelligence requirements to include communicating what the mission is and how the requested product will aid in mission accomplishment. The G-2/S-2 should submit the imagery exploitation and collection requirements in the Requirements Management System using established procedures such as those in the unit's SOP or as established by the combatant command.

9-15. The G-2/S-2 must also determine the specific imagery requirements to avoid burdening the system with unnecessary requests. The desire for imagery products often exceeds the capabilities of the imaging system. Therefore, it is imperative that the G-2/S-2 consider what type of analysis is needed and request only that which they require. The specifications of the request for IMINT products often affect the timeliness of the response. For example, determining if vehicles are tanks takes less time and requires less resolution than determining the make, model, and capabilities of the tank.

9-16. IMINT products to be considered for requirements by the G-2/S-2 include—

- Imagery to detect and/or identify and locate, for example, specific unit types, equipment, obstacles, and potential field fortifications from which intelligence analysts are able to analyze enemy capabilities and develop possible COAs.
- Imagery to update maps and enhance the interpretation of information from maps. Detailed mission planning uses imagery to include stereo images for three-dimensional viewing of the terrain and many other geospatial uses.
- Moving target indicator (MTI) and full-motion video displays or products that provide an NRT picture of an object's movement by indicating its speed, location, and direction of travel. MTI systems do not differentiate friendly from enemy.
- Imagery to support protection of the force by helping commanders visualize how their forces look—including their disposition, composition, and vulnerabilities—as exploited by enemy IMINT systems.
- Target packets with imagery of the HVTs or HVIs and HPTs that include the critical elements of the targets and potential collateral damage.
- Imagery to support combat assessment to confirm destruction, determine the percentage of destruction, or whether the target was unaffected.
- Advanced geospatial intelligence products that can determine change detection, specific weapon system identifications, chemical compositions and material content, and a threat's ability to employ these weapons.

PREPARE

9-17. The G-2/S-2 IMINT-related actions during the prepare step of the intelligence process include establishing or verifying the portion of the intelligence communications architecture that supports IMINT display and analysis functions properly. Additionally, the G-2/S-2 must ensure that required IMINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Lastly, the G-2/S-2 must also ensure IMINT reporting and dissemination channels and procedures are in place and rehearsals are conducted with all pertinent IMINT elements to ensure interoperability.

COLLECT

9-18. As previously mentioned, there are two general types of imagery sensors. Depending on the type, the sensor or platform can record hardcopy or softcopy still (single frame) imagery or motion imagery. A given target will not necessarily receive continuous coverage due to the possible conflict between the number and priority of targets and the number and availability of imaging assets. However, a commander may decide to have continuous surveillance of certain targets, for specified periods, usually using organic imaging assets

(for example, unmanned aircraft systems) even though this detracts from the commander's ability to use these assets for other imagery targets within the AOI.

9-19. Processing IMINT involves converting geospatial data into an image format that is suitable for performing analysis and producing intelligence. Examples of imagery processing include developing film, enhancing imagery, converting electronic data into visual displays or graphics, and constructing electronic images from geospatial data.

PRODUCE

9-20. The imagery analyst must ensure the IMINT product satisfies the associated intelligence requirements and that the product is in the required format. The quality and resolution of the product is highly dependent upon the type of sensor, the platform, the time of day, and the weather conditions, as well as the imagery analyst's ability to identify objects and analyze activity within the images.

ANALYZE

9-21. Timeliness is critical not only to imagery collection but also to imagery analysis and reporting. It is difficult to separate IMINT reporting from imagery analysis in this discussion; this is demonstrated by the three phases of IMINT reporting presented below; all are dependent upon the timeliness requirements. Each phase represents a different degree of analysis and period available to accomplish the exploitation of the imagery.

- **First Phase** imagery analysis is the rapid exploitation of newly acquired imagery and reporting of imagery-derived information within a specified time from receipt of imagery. This phase satisfies PIRs and/or identifies changes or activity of immediate significance. First phase imagery analysis results in an Initial Phase Imagery Report and is usually completed within 45 minutes after receipt of the imagery.
- **Second Phase** imagery analysis is the detailed exploitation of newly acquired imagery and the reporting of imagery-derived intelligence and information while meeting the production and timeliness requirements. Other intelligence discipline source material may support Second phase imagery as appropriate. Second phase imagery analysis results in a Supplemental Imagery Report.
- **Third Phase** imagery analysis is the detailed analysis of all available imagery pertinent to a SIR and the subsequent production and reporting resulting from this analysis within a specified time. This phase provides an organized detailed analysis of an imagery target or topic, using imagery as the primary data source but incorporating data from other sources as appropriate.

9-22. The two types of imagery exploitation are national and direct support.

- **National exploitation** is imagery exploitation that supports presidential requirements, National Security Council requirements, congressional requirements, or requirements of a common concern to the intelligence community.
- **Direct support exploitation** is imagery exploitation that supports assigned missions of a single agency, department, or command.

9-23. Imagery analysts will complete DS exploitation in order to satisfy (First Phase) requirements and report the results as soon as possible. Timelines for completing first phase exploitation varies depending on unit SOPs; however, the most commonly accepted timeline is to have the exploitation completed within four hours after receipt of the imagery. Collectors will complete national exploitation in order to satisfy (Second and Third Phases) requirements and report the results within the time specifications of each individual requirement.

ASSESS

9-24. The requestor should immediately assess the imagery product upon receipt for accuracy and relevance to the original request. The requestor must then notify and inform the imagery analyst of the extent to which the product answered the PIR. Providing feedback to the producer regarding the product helps ensure the producer will provide the required information in the correct format. The following are some of the questions which the requestor should consider when providing feedback to the producer.

- Is the format of the product acceptable?
- Is additional information needed on the product or future products?
- Is excess information included on the product?
- Does the IMINT product satisfy the requirement?

PROPAGATE

9-25. IMINT products are propagated in hardcopy and digital formats. The distribution of hardcopy products will be via couriers or other types of mail systems. The requestor must ensure that the requested product is transmittable over the available communications systems.

Chapter 10

Measurement and Signature Intelligence

DEFINITION

10-1. MASINT 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).

10-2. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, RF, nuclear detection, and seismic sensors, as well as techniques for collecting CBRNE and other materiel samples.

10-3. It requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communication, data, and display processing technologies now provide MASINT in support of commanders in full spectrum operations.

10-4. There are six subdisciplines within MASINT:

- **Radar.** The active or passive collection of energy reflected from a target or object by line of sight, bistatic, or over-the-horizon radar systems. Radar derived collection provides information on radar cross-sections, tracking, precise spatial measurements of components, motion and radar reflectance, and absorption characteristics for dynamic targets and objectives. A side-looking airborne radar system, coupled with advanced MASINT processing techniques—
  - Provides a high resolution, day-and-night collection capability.
  - Can produce a variety of intelligence products that identify or provide change detection, terrain mapping, underwater obstacles, dynamic sensing of targets in clutter, and radar cross-section signature measurements.
- **RF.** The collection, processing, and exploitation of electromagnetic emissions from a RF weapon, an RF weapon precursor, or an RF weapon simulator; collateral signals from other weapons, weapon precursors, or weapon simulators (for example, electromagnetic pulse signals associated with nuclear bursts); and spurious or unintentional signals.
  - ***Electromagnetic Pulses.*** Measurable bursts of energy that result from a rapid change in a material or medium, resulting in an explosive force, produces RF emissions. The RF pulse emissions associated with nuclear testing, advanced technology devices, power and propulsion systems, or other impulsive events can be used to detect, locate, identify, characterize, and target threats.
  - ***Unintentional Radiation.*** The integration and specialized application of MASINT techniques against unintentional radiation sources that are incidental to the RF propagation and operating characteristics of military and civil engines, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.
- **Electro-Optical.** The collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (ultraviolet, visible, and infrared) of the electromagnetic spectrum. MASINT electro-optical provides detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the materials composition of a target.

Electro-optical data collection has broad application to a variety of military, civil, economic, and environmental targets. Electro-optical sensor devices include radiometers, spectrometers, non-literal imaging systems, lasers, or laser detection and ranging systems.

- ***Infrared.*** A subcategory of electro-optical that includes data collection across the infrared portion of the electromagnetic spectrum where spectral and thermal properties are measured.
- ***LASER.*** Integration and specialized application of MASINT electro-optical and other collection to gather data on laser systems. The focus of the collection is on laser detection, laser threat warning, and precise measurement of the frequencies, power levels, wave propagation, determination of power source, and other technical and operating characteristics associated with laser systems—strategic and tactical weapons, range finders, and illuminators.
- ***Hyperspectral Imagery.*** A subcategory of electro-optical intelligence produced from reflected or emitted energy in the visible and infrared spectrum used to improve target detection, discrimination, and recognition. Hyperspectral imagery can detect specific types of foliage (supporting drug-crop identification; disturbed soil); supporting the identification of mass graves, minefields, caches, underground facilities or cut foliage; and variances in soil, foliage, and hydrologic features—often supporting CBRNE contaminant detection.
- ***Spectroradiometric Products.*** Products that include electro-optical spectral (frequency) and radiometric (energy) measurements. A spectral plot represents radiant intensity versus wavelength at an instant in time. The number of spectral bands in a sensor system determines the amount of detail that can be obtained about the source of the object being viewed. Sensor systems range from multispectral (2 to 100 bands) to hyperspectral (100 to 1,000 bands) to ultraspectral (1,000+ bands). More bands provide more discrete information, or greater resolution. The characteristic emission and absorption spectra serve to signature or define the makeup of the feature that was observed. A radiometric plot represents the radiant intensity versus time. An example is the radiant intensity plot of a missile exhaust plume as the missile is in flight. The intensity or brightness of the object is a function of several conditions including its temperature, surface properties or material, and how fast it is moving. For each point along a time-intensity radiometric plot, a spectral plot can be generated based on the number of spectral bands in the collector.

- **Geophysical.** Geophysical MASINT involves phenomena transmitted through the earth (ground, water, atmosphere) and manmade structures including emitted or reflected sounds, pressure waves, vibrations, and magnetic field or ionosphere disturbances. Unattended ground sensors are an example of geophysical sensors.
  - ***Seismic.*** The passive collection and measurement of seismic waves or vibrations in the earth surface.
  - ***Acoustic.*** The collection of passive or active emitted or reflected sounds, pressure waves, or vibrations in the atmosphere or in the water. Water-based systems detect, identify, and track ships and submarines operating in the ocean.
  - ***Magnetic.*** The collection of detectable magnetic field anomalies in the earth's magnetic field (land and sea). Magnetic sensors have the capability to indicate the presence and direction of travel of an iron object.
- **Nuclear Radiation.** The information derived from nuclear radiation and other physical phenomena associated with nuclear weapons, reactors, processes, materials, devices, and facilities. Nuclear monitoring can be done remotely or during onsite inspections of nuclear facilities. Data exploitation results in characterization of nuclear weapons, reactors, and materials. A number of systems detect and monitor the world for nuclear explosions, as well as nuclear materials production.
- **Materials.** The collection, processing, and analysis of gas, liquid, or solid samples. Materials intelligence is critical to collection against CBRNE warfare threats. It is also important to

analyzing military and civil manufacturing activities, public health concerns, and environmental problems. Samples are both collected by automatic equipment, such as air samplers, and directly by humans. Samples, once collected, may be rapidly characterized or undergo extensive forensic laboratory analysis to determine the identity and characteristics of the sources of the samples.

ROLE

10-5. MASINT provides intelligence to the commander in full spectrum operations to facilitate situational understanding. MASINT can defeat many of the camouflage, concealment, and deception techniques currently used to deceive ISR systems.

10-6. By application of NRT analysis and dissemination, MASINT has a potential ability to provide timely situational awareness and targeting not necessarily available to other disciplines. Specifically, MASINT sensors have unique capabilities to detect missile launch; detect and track aircraft, ships, and vehicles; perform non-cooperative target identification and combat assessment; and detect and track fallout from nuclear detonations. Often, these contributions are the first indicators of hostile activities.

10-7. The MASINT systems most familiar on today's battlefield are employed by ground surveillance and CBRN reconnaissance elements. MASINT spans the entire electromagnetic spectrum and its capabilities complement, rather than compete with, the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—

- Use automatic target recognition and aided target recognition.
- Penetrate manmade and/or natural camouflage.
- Penetrate manmade and/or 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 CBRNE agents to include prior to, during, or after employment.
- Detect signature anomalies that may affect target-sensing systems.

FUNDAMENTALS

10-8. Within DOD, there are two agencies that provide policy and guidance for MASINT. NGA is responsible for the radar and electro-optical subdisciplines while DIA maintains the other four. While NGA and DIA provide policy and guidance for MASINT, their policy and guidance remain transparent to the service component. Each service, in turn, has a primary command or staff activity to develop requirements and coordinate 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 the Army Reprogramming Analysis Team or INSCOM channels for data collection and processing.

10-9. The S&TI community also performs MASINT collection and processing primarily to support R&D 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 R&D centers such as the Communications-Electronics Command Research, Development, and Engineering Center, the Army Research Laboratory (ARL), and the Night Vision and Electronic Systems Laboratory are also involved in developing sensor systems for collecting and processing MASINT.

10-10. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based operational collection to support the ASCC and subordinate units. This capability will expand upon the standup of INSCOM MIBs.

MEASUREMENT AND SIGNATURE INTELLIGENCE IN THE INTELLIGENCE PROCESS

10-11. The MASINT discipline has several unique considerations throughout the steps of the intelligence process.

GENERATE INTELLIGENCE KNOWLEDGE

10-12. The G-2/S-2 section must research targets' characteristics and capabilities that may impact on the employment and use of MASINT sensors utilizing all available data prior to conducting operations. Additionally, the G-2/S-2 section must collect any existing MASINT products and identify all units, organizations, and systems that may potentially answer the commander's requirements. National and combatant command databases may hold more recent or updated information that can assist MASINT planners in determining the most effective MASINT means of supporting the commander's requirements.

PLAN

10-13. Some MASINT sensors can provide extremely specific information about detected targets, whereas other sensors may only be capable of providing an indication that an entity was detected. Additionally, there are varying capabilities of detection, identification, and classification among MASINT sensors. It is these varying capabilities that require synchronizing the employment of MASINT sensors both within the MASINT discipline and within the ISR effort as a whole. See FM 2-01 for more information on ISR synchronization.

10-14. Depending on the type of sensor employed, a given MASINT collection target or NAI may not necessarily receive continuous coverage due to the possible conflict between the number and priority of targets and the number and availability of MASINT assets. However, a commander may decide to have continuous surveillance of certain targets by using available MASINT assets (for example, Unattended Ground Sensors (UGS) OmniSense, Silent Watch, and Scorpion).

10-15. Another consideration when planning MASINT missions is whether to use active, passive, or a combination of sensors when planning MASINT coverage. This must be planned based on the commander's intent, the mission, the mission variables and the capabilities of the sensors. Additionally, personnel must be detailed to emplace the sensors (and retransmission systems, if necessary) and monitor the signatures that they transmit upon detection.

PREPARE

10-16. The primary responsibility of the G-2/S-2 during the prepare function of the intelligence process or MASINT is to support the G-3/S-3 in identifying the best locations to emplace MASINT assets and to ensure that the G-2/S-2 analysts can receive and verify the information transmitted by those assets. Additionally, the G-2/S-2 must ensure that required MASINT analytical assets and resources are prepared to provide support or are available through intelligence reach. Since the products of MASINT are not as well known as products from other intelligence disciplines, the G-2/S-2 must be aware of the types of MASINT products available to support the operation, and then educate the rest of his unit's staff on the use of these MASINT products. Lastly, the G-2/S-2 must also ensure MASINT reporting and dissemination channels and procedures are in place and rehearsals are conducted with all pertinent MASINT elements to ensure interoperability.

COLLECT

10-17. MASINT provides information required to answer PIRs and other intelligence requirements in support of the ISR effort. As stated earlier in this chapter, MASINT collection must not only be synchronized within its own discipline but also be synchronized and integrated into the unit's overall ISR effort in order to be effective. MASINT sensors are employed throughout the full spectrum of operations from a variety of platforms—subsurface, ground, marine, and aerospace.

10-18. Just as in the other intelligence disciplines, MASINT involves dealing with huge volumes of data that have to be processed before beginning analysis and production. The process function regarding MASINT involves converting esoteric data into a form that is suitable for performing analysis and producing intelligence. MASINT processing can include relatively simple actions such as converting a UGS sensor activation into a report, to a complex task such as processing hyperspectral imagery into a report identifying the composition and concentrations of carcinogenic chemicals present in the emissions from a factory upwind from a US forces encampment.

PRODUCE

10-19. Effective and timely MASINT requires personnel with diverse skill sets. The MASINT producer must ensure the MASINT product satisfies the associated intelligence requirements and that the product is in the required format. The quality, fidelity, and timeliness of MASINT products are highly dependent upon the type of target, the collection system, the system's position in relation to the target or NAI, and the weather, as well as the MASINT system operator's ability to identify the appropriate threat activity. The objective of MASINT production is to be used in an all-source analytical approach.

ANALYZE

10-20. The intelligence staff analyzes intelligence and information about the enemy's equipment, doctrine, and TTP. Using this information, along with the knowledge of friendly force MASINT capabilities, the intelligence staff develops and refines a collection strategy to maximize the use of the unit's MASINT systems to answer intelligence gaps.

ASSESS

10-21. The primary goal of the MASINT assess function is to determine whether the results of MASINT collection and production meet the requirements of the unit's ISR effort. MASINT producers must assess all facets of MASINT operations, from receipt of the ISR task to the dissemination of MASINT, in an effort to determine the effectiveness of MASINT. An assessment of the friendly force's capabilities must be conducted to ensure the continued effectiveness of, or to improve upon, MASINT collection. This assessment is not only directed at each MASINT asset individually but also throughout the supporting intelligence communications architecture, to include intelligence reach and the unit's entire ISR effort.

10-22. Additionally, the G-2/S-2 immediately assesses MASINT products upon receipt for accuracy and relevance. He must inform the MASINT producer of the extent to which the product answered the PIR or intelligence requirement. Providing feedback to the MASINT producer—and collector—helps improve the effectiveness and efficiency of MASINT.

PROPAGATE

10-23. MASINT of critical importance to the force, including answers to the PIRs, is disseminated via the most expeditious means possible.

10-24. For intelligence reach operations, MASINT products are available and disseminated in a variety of forms. The requestor must ensure that the MASINT product can be transmitted over the available communications systems, to include verifying the appropriate security level of the communications system.

5398
5399

Chapter 11

Open-Source Intelligence

DEFINITION

11-1. **Open-source intelligence is *information of potential intelligence value that is available to the general public*** *(JP 2-0).* 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,** which 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,** which 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.

ROLE OF OPEN-SOURCE INTELLIGENCE

11-2. OSINT operations are integral to Army intelligence operations. The availability, depth, and range of publicly available information enable intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support other ISR efforts by providing general initial information that supports generate intelligence knowledge and enhances collection and production. As part of a single-source and all-source intelligence effort, the use and integration of OSINT ensures commanders have the benefit of all available information. All OSINT operations conducted by intelligence personnel must be in compliance with the legal restrictions in Executive Order 12333, DOD Directive 5100.20, and AR 381-10.

11-3. The source, the information, and the collection means rather than a specific category of technical or human resources distinguish OSINT from other intelligence disciplines. 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 unintrusive. Other intelligence disciplines use confidential sources or intrusive techniques to collect private information. Confidential sources and private information are—

- **Confidential source,** which is any person, group, or system that provides information with the expectation that the information, relationship, or both, are protected against public disclosure.
- **Private information,** which is data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. There are two subcategories of private information: classified information and controlled unclassified information.
  - ***Classified information*** requires protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.
  - ***Controlled unclassified information*** requires the application of controls and protective measures, for a variety of reasons (that is, sensitive but unclassified, or for official use only), not to include those that qualify for formal classification.

11-4. The following characteristics address the role of publicly available information and OSINT in Army operations.

- **Provides the Foundation.** The US social structures, education system, news services, and entertainment industry shape our world view, awareness of international events, and perceptions of non-US societies. This foundation is an essential part of the generate intelligence knowledge step of the intelligence process.
- **Answers Requirements.** The availability, depth, and range of public information enable intelligence and non-intelligence organizations to satisfy many of the CCIRs (PIRs and FFIRs) 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 planning phase to the production phase of the intelligence process.
- **Enhances Collection.** Open-source research and collection support other surveillance and reconnaissance activities by answering requirements and providing foundational 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 ensures commanders have the benefit of all sources of available information.

FUNDAMENTALS OF OPEN-SOURCE INFORMATION

11-5. The Army does not have a specific MOS, additional skill identifier (ASI), or SQI for OSINT. With the exception of the Asian Studies Detachment, the Army does not have base TOE for OSINT units or staff elements. OSINT missions and tasks are imbedded within existing missions and force structure or accomplished through task organization.

11-6. The focus of Army OSINT operations is the MIB. Each of these INSCOM units conducts sustained, regionally focused intelligence operations in support of their ASCC and combatant command. While their OSINT capabilities may vary, each of these theater-level MI units is the focal point within the combatant command for managing Army open-source requirements and providing OSINT support to Army tactical units deploying to or operating within the combatant command's AOR. When open-source skills and regional knowledge are not present in these deploying tactical units, personnel from the MIB may deploy with and form the core of the tactical unit's OSINT organization as well as provide the control mechanism for synchronization and information exchange between echelons.

OPEN-SOURCE INTELLIGENCE CONSIDERATIONS

11-7. For the most part, the considerations for OSINT are similar to those of other intelligence disciplines.

- OSINT organizations need clearly stated intelligence requirements to effectively focus collection and production.
- OSINT operations must comply with AR 381-10 and Executive Order 12333 on the collection, retention, and dissemination information on US persons.
- OSINT organizations can be overwhelmed by the volume of information to process and analyze.
- OSINT operations require qualified linguists for foreign language-dependent collection and processing tasks.

11-8. Personnel responsible for planning or executing OSINT operations must also consider the concerns discussed below.

COMPLIANCE

11-9. Under AR 381-10, procedure 2, Army intelligence activities may collect publicly available information on US persons only when it is necessary to fulfill an assigned function. There must also be a link between the collection of the US person information and the Army intelligence organization's assigned mission. Army intelligence components must exhaust the least intrusive collection means before requesting a more intrusive collection means. The following are additional considerations for Internet collection:

- Army intelligence components must use Government computers to access the Internet for official Government business unless otherwise authorized.
- Internet protocol addresses, uniform resource locators (URLs), and email addresses that are not self-evidently associated with a US person may be acquired, retained, and processed by Army intelligence components without making an effort to determine whether they are associated with a US person as long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the Army intelligence component must make a reasonable and diligent inquiry to determine whether the data are associated with a US person.

LIMITATIONS

11-10. Intelligence personnel and organizations must comply with applicable DOD Directives and Army Regulations that govern contact with and collection of information from open sources. For example, DOD Directive 5100.20 prohibits SIGINT organizations from collecting and processing information from public broadcasts with exception of processing encrypted or "hidden meaning" passages. AR 380-13 prohibits the assignment of Army personnel, military or civilian, to attend public or private meetings, demonstrations, or other similar activities held off-post to acquire CI investigative information without specific approval by the Secretary or the Under Secretary of the Army.

OPERATIONS SECURITY

11-11. More than any other intelligence discipline, the OSINT discipline could unintentionally provide indicators of US military operations. Information generally available to the public as well as certain detectable activities such as open-source research and collection can reveal the existence of, and sometimes details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit US military operations. Purchasing documents, searching an Internet site, or asking questions at public events are examples of detectable open-source research and collection techniques that could provide indicators of US plans and operations.

11-12. Taking OPSEC into consideration, organizations must determine what level of contact with open sources and which collection techniques might provide indicators that an enemy could piece together in time to affect US military operations. In OSINT operations, countermeasures range from limiting the frequency or duration of contact with a source to prohibiting all contact with a source. If OPSEC so requires, such as to protect a Government computer from hacker retaliation, a direct reporting unit commander may approve nonattributable Internet access.

CLASSIFICATION

11-13. AR 380-5 states that intelligence producers "must be wary of applying so much security that they are unable to provide a useful product to their consumers." This is an appropriate warning for OSINT operations where concern for OPSEC can undermine the ability to disseminate inherently unclassified information. As shown in table 11-1, the classification of source metadata, collector metadata, collected information, and derivative intelligence differs based on the means of collection and the degree of damage to national security that disclosure of this information could reasonably be expected to cause. Since it is already in the public domain, publicly available information and the source metadata are unclassified. AR 380-5, chapter 4, directs that Army personnel will not apply classification or other security markings

"to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium." For reasons of OPSEC, the classification of collector information is controlled unclassified or classified information.

Table 11-1. Open-source intelligence classification considerations

IF		THEN			
Information Source	Collection Means	Source Metadata	Collector Metadata	Collected Information	Intelligence Report
Confidential	Overt	Classified or Controlled Unclassified	Classified or Controlled Unclassified	Classified or Controlled Unclassified Information	Classified or Controlled Unclassified
	Clandestine	Classified	Classified		
Open	Overt	Unclassified	Controlled Unclassified	Unclassified	Classified, Controlled Unclassified, or Unclassified
	Nonattributable		Classified or Controlled Unclassified		
NOTE: This table is prescriptive not directive. Organizations with original classification authority or personnel with derivative classification responsibilities must provide subordinate organizations and personnel with a security classification guide or guidance for information and intelligence derived from open sources in accordance with the policy and procedures in AR 380-5.					

11-14. According to AR 380-5, chapter 2, a compilation of unclassified publicly available information into an intelligence product (estimate, report, or summary) is normally not classified. In unusual circumstances, the combination of individual unclassified items of information into an intelligence product may require classification if the compilation provides an added factor that warrants classification.

11-15. AR 380-5, chapter 6, provides a list of factors or classification considerations which includes but is not limited to the following:

- Intelligence that reveals the identity of a conventional source or method that normally does not require classification.
- Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the particular source or method.
- An intelligence requirement is classified when it reveals what is not known, what is necessary to know, and why.

Note. The intelligence staff creates sanitized, unclassified collection tasks from the intelligence requirements since uncleared US and non-US persons make up a significant portion of open source collectors.

- Information that would divulge intelligence interests, value, or extent of knowledge on a subject.
- Information related to political or economic instabilities in a foreign country threatening American lives and installation there.

DECONFLICTION

11-16. During planning, the G-2/S-2 staff and the G-3/S-3 staff must deconflict OSINT operations with other activities. Specifically, contact or interaction with open sources may compromise the operations of another intelligence discipline. Open-source collection may adversely affect the ability of non-intelligence organizations such as CA, MP, medical, and PA to accomplish their missions. Conversely, CA, MP, medical, PA, or other personnel who overtly contact an OSINT source may inadvertently compromise OSINT operations as well as the safety of the open source or collector. Each of these situations could lead to the loss of access to the open source and information of intelligence value.

DECEPTION AND BIAS

11-17. Deception and bias are of particular concern in OSINT operations. Unlike other disciplines, OSINT operations do not normally collect information by direct observation of activities and conditions within the AO. OSINT operations rely on secondary sources to collect and distribute information that the sources may not have observed themselves. Secondary sources such as government press offices, commercial news organizations, NGO spokespersons, and other information providers can intentionally or unintentionally add, delete, modify, or otherwise filter the information they make available to the general public. These sources may also convey one message in English for US or international consumption and a different non-English message for local or regional consumption. It is important to know the background of open sources and the purpose of the public information in order to distinguish objective, factual information from information that lacks merit, contains bias, or is part of an effort to deceive the reader.

11-18. In addition to determining the reliability and validity of the information obtained during OSINT operations, intelligence analysts must consider the biases and cultural backgrounds of civilian interpreters who may be used to translate or even search for relevant non-English information. These civilian interpreters may be local hires when deployed overseas, and many civilian interpreters do not have security clearances.

INTELLECTUAL PROPERTY

11-19. AR 27-60 prescribes policy and procedures for the acquisition, protection, transfer and use of patents, copyrights, trademarks, and other intellectual property by DA. It is Army policy to recognize the rights of copyright owners consistent with the Army's unique mission and worldwide commitments. As a general rule, Army organizations will not reproduce or distribute copyrighted works without the permission of the copyright owner unless such use is within an exception under US Copyright Law or required to meet an immediate, mission-essential need for which non-infringing alternatives are either unavailable or unsatisfactory.

11-20. According to the US Copyright Office, "fair use" of a copyrighted work for purposes such as criticism, comment, news reporting, teaching, scholarship, or research, is not an infringement of copyright. Implicit with fair use is the documentation and citation of the source of the copyrighted information. The following are four factors in determining fair use:

- Purpose and character of the use. In the context of fair use, intelligence operations are similar in purpose and usage to non-profit news reporting and research organizations.
- Nature of the copyrighted work.
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole. There is no specific number of words, lines, or notes that may safely be taken without permission. Usually, the amount or portion of copyrighted material is limited to quotations of excerpts and short passages, and summary of a speech or article, with brief quotations.
- Effect of the use upon the potential market for or value of the copyrighted work. The effect on the market or value of copyrighted material relates to reproduction and dissemination of products provided by the owner beyond that authorized the owner's "Terms of Use" or described in contracts and licenses with the US Government.

OPEN SOURCES AND INFORMATION

11-21. Open sources and publicly available information may include but are not limited to—

- **Academia.** Courseware, dissertations, lectures, presentations, research papers, and studies in both hardcopy and softcopy on economics, geography (physical, cultural, and political-military), international relations, regional security, science, and technology.
- **Governmental, Intergovernmental, and NGOs.** Databases, posted information, and printed reports on a wide variety of economic, environmental, geographic, humanitarian, security, science, and technology issues.
- **Commercial and Public Information Services.** Broadcasted, posted, and printed news on current international, regional, and local topics.
- **Libraries and Research Centers.** Printed documents and digital databases on a range of topics as well as knowledge and skills in information retrieval.
- **Individuals and Groups.** Handwritten, painted, posted, printed, and broadcasted information (for example, art, graffiti, leaflets, posters, and websites).

OPEN-SOURCE MEDIA

11-22. A simple communications model consists of a sender, a message, a medium, and a receiver. The medium is the access point to publicly available information for open-source research and collection. The primary media that open sources use to communicate information to the general public are shown in table 11-2 and discussed below.

PUBLIC SPEAKING FORUMS

11-23. Public speaking, the oldest medium, is the oral distribution of information to audiences during events that are open to the public or occur in public areas. These events or forums include but are not limited to academic debates, educational lectures, news conferences, political rallies, public government meetings, religious sermons, and S&T exhibitions. Neither the speaker nor the audience has the expectation of privacy when participating in a public speaking forum unless there is an expressed condition of privacy such as the Chatham House Rule. The Chatham House Rule says that:

> *When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.*

11-24. If invoked, privacy conditions such as the Chatham House Rule change the characterization of the source from an open to a confidential source and may necessitate treating the source and collected information in accordance with HUMINT or CI procedures. Unlike the other open-source collection, monitoring public speaking events is done through direct observation and, due to its overt nature, could entail risk to the collector.

PUBLIC DOCUMENTS

11-25. A document is any recorded information regardless of its physical form or characteristics. Like public speaking, public documents have always been a source of intelligence. Documents provide in-depth information about the operational environment that underpin our ability to plan, prepare for, execute, and assess military operations. During operations, documents such as newspapers and magazines provide insights into the effectiveness of information tasks, especially information engagement. Books, leaflets, magazines, maps, manuals, marketing brochures, newspapers, photographs, public property records, and other forms of recorded information continue to yield information of intelligence value about operational environments. Sustained document collection contributes to the development of studies about potential operational environments. Collection of documents on the operational and technical characteristics of foreign materiel aid in the development of improved US tactics, countermeasures, and equipment.

Table 11-2. Primary open-source media

SYSTEM	*COMPONENTS*	*ELEMENTS*
PUBLIC SPEAKING	SPEAKER	• Sponsor • Relationship • Message
	FORMAT	• Conference • Debate • Demonstration • Lecture • Rally
	AUDIENCE	• Location • Composition
PUBLIC DOCUMENTS	GRAPHIC	• Drawing • Engraving • Painting • Photograph • Print
	RECORDED	• Compact Data Storage Device • Digital Video Disk • Hard Disk • Tape
	PRINTED	• Book • Brochure • Newspaper • Periodical • Pamphlet • Report
PUBLIC BROADCASTS	RADIO	• Low Frequency AM Radio • Medium Frequency AM Radio • VHF FM Radio • L- and S-Band Satellite Radio
	TELEVISION	• Ku Band Satellite Television • VHF and UHF Terrestrial Television
INTERNET SITES	COMMUNICATIONS	• Chat • Email • News; Newsgroup • Webcam • Webcast • Weblog
	DATABASES	• Commerce • Education • Government • Military Organizations

Table 11-2. Primary open-source media (continued)

SYSTEM	*COMPONENTS*	*ELEMENTS*
INTERNET SITES (continued)	INFORMATION (WEBPAGE CONTENT)	• Commerce • Education • Government • Military Organizations
	SERVICES	• Dictionary • Directory • Downloads • Financial • Geospatial • Search and URL Lookup • Technical Support • Translation

PUBLIC BROADCASTS

11-26. A public broadcast entails the simultaneous transmission of data or information for general public consumption to all receivers or terminals within a computer, radio, or television network. Public broadcasts are important sources of current information about the operational environment. Television news broadcasts often provide the first I&W of situations that may require the use of US forces. Broadcast news and announcements enable personnel to monitor conditions and take appropriate action when conditions change within the AO. News, commentary, and analysis on radio and television also provide windows into how governments, civilians, news organizations, and other elements of society perceive the US and US military operations. Broadcasts also provide information and insights into the effectiveness of information tasks.

INTERNET SITES

11-27. Army intelligence components must use Government computers to access the Internet for official Government business unless otherwise authorized (for example, an Army Reservist participating in the World Basic Information Library Program).

11-28. Internet sites enable users to participate in a publicly accessible communications network that connects computers, computer networks, and organizational computer facilities around the world. The Internet is more than just a research tool. It is an ISR tool that enables intelligence personnel to locate and observe open sources of information. Through the Internet, trained collectors can detect and monitor Internet sites that may provide I&W of enemy intentions, capabilities, and activities.

11-29. Collectors can monitor newspaper, radio, and television websites that support assessments of information tasks, especially information engagement. Collectors can conduct periodic searches of webpages and databases for content on threat characteristics. Collecting webpage content and links can provide useful information about relationships between individuals and organizations. Properly focused, collecting and processing publicly available information from Internet sites can support understanding of the operational environment.

Chapter 12

Signals Intelligence

DEFINITION

12-1. *SIGINT is intelligence produced by exploiting foreign communications systems and noncommunications emitters* (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 activity 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), and foreign instrumentation signals intelligence (FISINT).

- COMINT is intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means. COMINT includes computer network exploitation, which is gathering 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 and/or transmission. The imagery can be static or streaming.
- ELINT is intelligence derived from the interception and analysis of noncommunications emitters (for example, radar). ELINT consists of two subcategories: operational ELINT (OPELINT) and technical ELINT (TECHELINT).
  - OPELINT is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems.
  - TECHELINT is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.
- FISINT involves the technical analysis of data intercepted from foreign equipment and control systems such as telemetry; electronic interrogators; tracking, fusing, arming, firing command systems, and video datalinks.

ROLE

12-2. SIGINT provides intelligence on threat capabilities, disposition, composition, and intentions. In addition, SIGINT provides targeting information for the delivery of lethal and nonlethal fires. Ultimately, the role of SIGINT is to collect, process, and disseminate SIGINT information in support of operations.

FUNDAMENTALS

12-3. It is important that the G-2/S-2 understand how SIGINT assets are organized not only within the Army but also throughout DOD. The majority of SIGINT assets from all the armed services, combined with national SIGINT assets, work together to support commanders from the tactical to the strategic level. Only by understanding the SIGINT structure that transcends traditional service component boundaries can the
G-2/S-2 understand how to use SIGINT effectively.

NATIONAL TACTICAL SIGINT RELATIONSHIPS

12-4. Since September 11, 2001, National Tactical SIGINT integration has grown from concept to reality. Today, tactical Army SIGINT elements rely heavily on NSA for many integrated functions and, conversely, NSA relies on tactical resources for intelligence. These functions and interfaces include NSA network (NSANet) connectivity to conduct analytic and data exchanges and input data into and access raw data from databases, and supporting the Army SIGINT collectors and analysts with specific SIGINT equipment and tools. Intelligence development has increased to the point of truly being integrated within the SIGINT enterprise. The SIGINT technical architecture complements existing C2 relationships; it does not replace the commander's authority or chain of command. The following organizations are the basis for this relationship.

ARMY CRYPTOLOGIC OPERATIONS, INSCOM

12-5. Army Cryptologic Operations (ACO) is an element of INSCOM G-2 located within NSA and acts as the Army's Service cryptologic element (SCE) representative. ACO supports Army cryptologic operations, capabilities, and resourcing for the purpose of providing dominant strategic and operational SIGINT, Information Assurance, and Information Operations for ground component commanders, national agencies, and national decision makers. The ACO is instrumental in providing SIGINT quick reaction capability systems. The ACO works closely with NSA and other SCEs to collaborate and leverage the SIGINT enterprise in improving sensor capabilities and technical and analytical support to Army SIGINT elements.

ARMY TCAE (ATCAE)

12-6. The ATCAE, established at the national level, plays a significant role in TCAE operations by providing technical support oversight and coordinating collaborative issues such as getting approvals for NSA connectivity and access to national databases for US Army tactical SIGINT personnel. The ATCAE is located within the NSA complex at Fort Meade, MD, and represents the Army Deputy Chief of Staff for Intelligence on SIGINT technical matters involving Army ground SIGINT elements.

12-7. The ATCAE works closely with the Army Cryptologic Operations to support the Army's special sensor capabilities by providing SIGINT technical and analytical support. The special sensor capability systems are responsive to the ground force commander's requirements and enable SIGINT personnel to conduct SIGINT operations against modern communications systems.

2-118. The ATCAE provides 24-hour service through its service desk and time-sensitive operations or military support desks. This support includes—

- Comprehensive technical SIGINT information to support collection, processing, analysis, and reporting, as well as collateral support for the unit's SIGINT/EW mission.
- Information on current world situations and friendly and threat military operations, tailored to a given unit's mission.
- Assistance in identifying hardware and software to carry out specific training and operational missions beyond the capability of organic equipment and systems.
- Advising Army tactical SIGINT personnel, at all levels, to reach and maintain an operational readiness posture by using ATCAE mobile training teams MTTs, the TROJAN program, and SIGINT Foundry Garrison Cryptologic Activities assets.
- Electronic quality control of unit reporting and forwarding to national time-sensitive systems.
- Assistance in obtaining SIGINT communications network connectivity and accesses to national assets to include databases.
- Assistance in reviewing and recommending modifications to US SIGINT directives on behalf of the tactical ground units' SIGINT technical issues.

SIGINT FOUNDRY

12-8. Soldiers deploying to operational zones will continue to face new technologies which they must exploit, process, analyze, and report. AIT training will provide foundational training, but Soldiers require more extensive training to ready them for specific deployments. The Army developed SIGINT Foundry to meet new SIGINT requirements and to bring SIGINT Soldiers up to operational readiness prior to deployment. As a result of close coordination between the Army G-2, the ACO/INSCOM, and the 704th MI Bde/742d MI Bn (ATCAE), nine Garrison Cryptologic Activity Centers are being established at the major CONUS Army installations to provide both training and overwatch capabilities to bring Army SIGINT Soldiers to an operational readiness standard.

THEATER TCAE

12-9. The theater TCAE performs SIGINT technical control and analysis and management. It provides SIGINT technical support for assigned, attached, OPCON, and lower echelon SIGINT resources deployed in the AOR. This includes mission tasking, processing, analyzing, and reporting of SIGINT data, information, and intelligence. The TCAE provides direction for the theater C&E battalion's SIGINT mission and for other theater tactical SIGINT assets.

ARMY SIGINT SYSTEMS

12-10. SIGINT elements at echelons corps and below conduct actions to search for, intercept, and identify threat signals for the purpose of immediate recognition. These actions provide information required to answer PIRs and other intelligence requirements in support of the ISR effort.

12-11. There is a varying mixture of SIGINT assets at echelons corps and below that include—

- AN/TSQ-219(V1and V2), Tactical Exploitation System.
- AN/PRD-13(V2), Improved SIGINT Man-pack System.
- AN/MLQ-4X, Prophet and AN/MSW-24 Prophet Control.
- AN/USD-9, Guardrail Common Sensor.
- AN/ASQ-223, Airborne Reconnaissance Low-Multifunction.

12-12. For more information on SIGINT assets, see MIHB 2-50.

SIGNALS INTELLIGENCE IN THE INTELLIGENCE PROCESS

12-13. The SIGINT discipline has several unique considerations throughout the steps of the intelligence process.

GENERATE INTELLIGENCE KNOWLEDGE

12-14. SIGINT personnel conduct intelligence reach; research (for example, databases, academic studies, products, or materials, OSINT or other information sources); and data mining that aid in determining the adversary's use of the electromagnetic spectrum in the supported unit's AOI. SIGINT personnel must follow all applicable policies and regulations on the collection of information and OPSEC. The information and intelligence gathered is the basis for—

- Developing a comprehensive SIGINT baseline database for the AO. What communications means does the threat use and what are their TTP? Do they incorporate civilian systems with military systems?
- Determining key SIGINT collection gaps. Are all the threat's electromagnetic emanations being collected and results databased? If not, why? If they are being collected, how do we receive or pull the reporting?

- Developing an understanding of the information and intelligence that can be collected with unit SIGINT collection assets and, when appropriate, other SIGINT collection assets in the AO. This also includes how and where the threat emanations may best be collected. Does the terrain support line of sight collection and reporting communications systems?
- Determining a method of understanding when changes to the baseline occur that are of intelligence interest. Does the threat go to radio silence prior to an offensive operation?

12-15. This information also can be used to determine predeployment training and develop exercises to provide as realistic and relevant training as possible. For tactical SIGINT personnel the best means to generate intelligence knowledge is by conducting tactical overwatch. While conducting tactical overwatch the SIGINT personnel, for example, will know what the specific types of threats, threat equipment, and threat TTP that they can expect to encounter when deployed.

PLAN

12-16. An important SIGINT planning consideration is that, when possible, SIGINT collection should be employed in conjunction with other intelligence disciplines collection systems. SIGINT is often used to cue, and be cued by, other ISR assets.

12-17. During planning, the SIGINT technical control element retrieves, updates, and develops any required SIGINT databases. This includes coordination with air and ground assets, other SIGINT assets or elements that support the operation, as well SIGINT assets that will operate in other units AO.

PREPARE

12-18. Preparation involves operational direction and control of SIGINT activities, including tasking and the allocation of effort. Operational control of SIGINT assets provides an authoritative prescription for SIGINT activities to include the uniform techniques and standards by which SIGINT information is collected, processed, and reported.

12-19. SIGINT operational tasking encompasses the direct levying of SIGINT information requirements by a military commander on designated SIGINT resources. This includes the authority to deploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated.

12-20. The commander ensures the SIGINT unit and asset leaders have conducted all necessary coordination and rehearsals. This includes establishing or verifying the operation of the SIGINT technical architecture.

12-21. The G-2/S-2 and SIGINT asset commander validate the availability of SIGINT assets and resources. SIGINT reporting and dissemination channels and procedures need to be in place. Deploying personnel require deployment training and a current polygraph in order to qualify for access to resources; appropriate and necessary database access; and connectivity and interoperability with all appropriate SIGINT elements. Courses such as Deployer (DEPL) 2000 help prepare SIGINT Soldiers for deployment.

COLLECT

12-22. SIGINT performs two major collection activities:

- **Signals Intercepts:** These include those SIGINT actions used to search for, intercept, and identify threat electromagnetic signals for the purpose of immediate threat recognition. Signals intercept provides information required to answer PIRs and other intelligence requirements in support of the ISR effort.
- **Direction Finding:**
  - Even when threat radio operators use COMSEC procedures, SIGINT teams can often intercept and approximate the location of the threat's signals. SIGINT teams can use DF to determine the movement of threat personnel or equipment; locations of emitters associated

with weapon systems and units; new and confirmed emitter locations; and possible friendly targets the enemy intends to attack (lethal and nonlethal).

- In addition to using DF to intercept and approximate the location of threat forces, DF operations can assist the (radio-equipped) friendly force by locating and vectoring assets or units during limited visibility; locating downed aircraft and personnel radio beacons; conducting signal security assessments; and locating sources of communication interference and jamming.

12-23. SIGINT processing involves converting intercepts of signals into written and verbal reports, automated message, graphic displays, recordings, and other forms suitable for analysis and intelligence production. Since US forces routinely conduct operations against threats who speak languages other than English, SIGINT processing often also includes translation of these intercepts.

12-24. Due to the complexity of many SIGINT systems, automated processing may occur several times before SIGINT data or information receives any human interaction.

ELECTRONIC WARFARE SUPPORT AND SIGINT

12-25. EW refers to any military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the adversary (JP 3-51). SIGINT is often confused or misrepresented as EW or a subdivision of EW known as electronic warfare support (ES). ES is achieved by **assets tasked or controlled by an operational commander**. These assets are tasked to search for, intercept, identify, and locate or localize sources of intentional or unintentional radiated electromagnetic energy. The purpose of ES tasking is immediate threat recognition, planning and conduct of future operations, and other tactical actions such as threat avoidance, targeting, and homing.

12-26. ES is intended to respond to an immediate operational requirement. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements. That is not to say that data collected for intelligence cannot meet immediate operational requirements. Intelligence collected for ES purposes is normally also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met (JP 3-13.1).

12-27. SIGINT can support and be supported by the components of EW. This means preserving the electromagnetic spectrum for friendly use while denying its use to the adversary. ES data can be used to produce SIGINT; this provides intelligence information for electronic or lethal attack or targeting.

PRODUCE

12-28. The SIGINT analyst provides SIGINT products to satisfy the associated intelligence requirements, in the required format and in a timely manner. The quality and timeliness of SIGINT products are highly dependent upon the type of intercept, the collection system, the system's position in relation to the threat emitter, the weather, as well as the SIGINT operator's ability to identify the appropriate threat signal activity. The objective for SIGINT is to be used in an all-source analytical approach.

12-29. There are a number of products generated from SIGINT. SIGINT reports are time-sensitive in nature and will contain anything from a traditional text formatted report to nontraditional reports comprised of color graphics, sound and/or video clips. SIGINT reports produced have titles such as (although not limited to) klieglights, tactical reports, and tactical ELINT reports and contain caveats that allow or restrict intelligence information to individuals with a need to know.

ANALYZE

12-30. The SIGINT analyst evaluates intelligence and information about the enemy's communications capabilities to determine appropriate SIGINT collection strategies. Conversely, a corresponding analysis of the friendly forces' SIGINT capabilities must be conducted to ensure the continued effectiveness of, or to

improve upon, SIGINT collection. SIGINT analysts also sort through large amounts of SIGINT and information and intelligence to identify and use only that which pertains to the CCIRs (PIRs and FFIRs).

ASSESS

12-31. The primary goal of the assess function when applied to SIGINT is to determine whether the results of SIGINT collection meet the requirements of the unit's ISR effort. SIGINT producers must assess all facets of SIGINT operations, from receipt of the ISR task to the dissemination of SIGINT to determine effectiveness. This assessment is not only directed at SIGINT assets on an individual basis but also throughout the supporting SIGINT architecture and the unit's entire ISR effort.

12-32. The G-2/S-2 immediately assesses SIGINT products upon receipt for timeliness, relevance, and accuracy. They must inform the SIGINT producer of the extent to which the product answered the PIR or intelligence requirement. Feedback is provided to the SIGINT producer and collector; this reinforces the effectiveness and efficiency of SIGINT.

PROPAGATE

12-33. SIGINT of critical importance to the force, including answers to the CCIRs (PIRs and FFIRs), is propagated and disseminated via the most expeditious means possible. Due to the highly perishable nature of SIGINT, the most expeditious reporting means is often immediately augmented with a follow-up report or augmented by a report transmitted through additional means, enhancing the probability of receipt. Sometimes the most expeditious means of reporting critical SIGINT information to the commander is face to face.

12-34. For intelligence reach operations, SIGINT products are available and disseminated in a variety of forms: hardcopy, softcopy, direct viewing, or broadcast. Time-sensitive reporting keeps NSA, commanders, and, non-SIGINT organizations advised on the status of current and potential threats. It is imperative to ensure that SIGINT products are only transmitted over communications systems at the appropriate classification level.

Chapter 13

Technical Intelligence

DEFINITION

13-1. TECHINT is 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 any adversary's technological advantages (JP 2-0).

ROLE

13-2. A strength of the US military is the diversity and extent of its technology base. While the US is one of the world leaders in integrating technology, the threat can achieve temporary technological advantage in certain areas by acquiring modern systems or by improvising new weapons. The world arms market is willing to provide advanced systems to countries or individuals with the resources to pay for them. A concerted TECHINT enterprise is vital to providing precise direction and purpose to DOD R&D and exploitation process to ensure quick and efficient neutralization of threat technological advantages and networks.

13-3. The role of TECHINT is to ensure that the warfighter understands the full technological capabilities of the threat. With this understanding, the US forces can adopt appropriate countermeasures, operations, and tactics.

13-4. TECHINT has three goals within its role:

- To ensure the US armed forces maintain technological advantage against any threat.
- To provide timely, relevant, accurate, predictive, and tailored TECHINT support to the warfighter throughout the full spectrum of military operations. This includes providing US forces intelligence, information, and training on foreign weapons systems to an extent that allows their use of CEE.
- To provide analysis of certain design traits of foreign weapons systems as indicators of threat intent.

13-5. TECHINT includes the subset Weapons Technical Intelligence (WTI), which combines forensic science with TECHINT for application against irregular and nontraditional threats. As such, WTI has four goals:

- To forensically examine events and/or devices or weapons to better understand linkages between technical design and tactical use to guide efforts of the protection warfighting function.
- 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 provide forensic analysis of IEDs, improvised weapons, and weapon components to identify the origin of materiel and components.
- To utilize materiel collected during site exploitation activities to further detain and potentially prosecute individuals for criminal activity.

FUNDAMENTALS

13-6. The fundamentals of TECHINT consist of TECHINT/WTI application in the full spectrum of operations and the importance of chain of custody. See FM 2-22.4 for more information.

TECHINT/WTI APPLICATION IN FULL SPECTRUM OPERATIONS

13-7. TECHINT assets are capable of responding to threats throughout the full spectrum of operations. Traditional TECHINT capabilities are best suited to meet the needs of commanders in General war. For example, the equipment used in General war consists of traditional threat weapons systems (for example, tanks, missiles, ATGMs). As such, TECHINT is capable of quickly identifying the visible and other indications of new weapons, improved munitions or modifications that could potentially defeat US equipment.

13-8. The knowledge gained, through TECHINT exploitation and analysis, also provides the necessary intelligence reach capability for operations that include lower levels of violence. Unlike general warfare, threat forces are not easily identified and often nontraditional and/or irregular threats take refuge in plain sight. Though the combination of forensic science and TECHINT, WIT provides commanders the ability to identify threat networks and their members. This is accomplished by linking individuals with events and materials that are intended to do harm to US forces. Indisputably, WTI assumes primacy in operations related to stable peace through insurgency.

13-9. TECHINT and WTI can be used simultaneously when commanders anticipate or encounter a mix set of threats. Also, the unique capabilities of WTI can be scaled to complete missions related to high priority objectives in general war; for example, the detainment of government officials, political party leaders, military commanders, scientists, and engineers. These detainments can significantly shape the operations by informing commanders on threat equipment capabilities and can affect planning in persistent conflicts, when level of violence decreases.

CHAIN OF CUSTODY

13-10. The proper documentation of captured enemy equipment (CEE) and captured enemy materiel (CEM) is a key factor in producing accurate and relevant TECHINT for the commander. For example, the capture location or the employment of material and associated material can link significant point of interest that can yield exploitable information.

13-11. Specifically, the proliferation of weapons from nation states and non-state actors can reveal third-party influences; properly recorded weapons emplacement can identify the effectiveness of weapons against US forces; and DOCEX can identify new tactics of weapon employment thus increasing effectiveness. Additionally, proper chain of custody is necessary in linking individuals and threat networks with weapons and material and/or events. The information gained through exploitation may eventually be used in US or HN legal proceedings.

THE TECHINT ENTERPRISE

13-12. The TECHINT enterprise consists of multiple entities within the Army working in concert with organizations from other Services components, within DOD, other US departments, national laboratories, and US academic institutions as well as international partners. For additional information on the TECHINT enterprise, see FM 2-22.4.

DEFENSE INTELLIGENCE AGENCY

13-13. DIA manages and reviews overall TECHINT activities. The S&TI Directorate within DIA is the action element for TECHINT. This directorate coordinates with external TECHINT agencies on non-policy matters concerning the production of S&TI. The following organizations provide TECHINT support under the control of DIA:

- **National Center for Medical Intelligence (NCMI)** based at Fort Detrick, MD, is a DOD intelligence production center under DIA control. NCMI is responsible for exploiting foreign medical materiel. The director supports the Army Foreign Materiel Program (FMP) and Army medical R&D requirements. The director coordinates planning, programming, and budgeting with the Army DCS, G-2.
- **Missile and Space Intelligence Center (MSIC)** based at Redstone Arsenal, AL, is a DOD intelligence production center under DIA control and supports the FMP. The MSIC acquires, produces, maintains, and disseminates S&TI pertaining to missile and space weapons systems, subsystems, components, and activities. The S&TI produced at MSIC also covers foreign state-of-the-art technology and research applicable to missiles.
- **Defense HUMINT** conducts worldwide HUMINT operations in support of foreign materiel acquisition (FMA) and foreign materiel exploitation (FME).

13-14. The organizations and agencies below constitute the Army TECHINT structure.

HEADQUARTERS, DEPARTMENT OF THE ARMY DCS, G-2

13-15. HQDA DCS, G-2 exercises staff responsibility for all Army TECHINT activities. The Army DCS, G-2 forms policies and procedures for S&TI activities, supervises and carries out the Army S&TI program, coordinates DA staff and MSC requirements for TECHINT, and is responsible for the Army FMP.

US ARMY INTELLIGENCE AND SECURITY COMMAND

13-16. Under the direction of HQDA, INSCOM is responsible for TECHINT. INSCOM fulfills its responsibilities through its TECHINT oversight function and manages the Army's Foreign Materiel for Training (FMT) Program and FMP. It provides the interface with strategic S&TI agencies in support of FME and organizes, trains, and equips TECHINT organizations. TECHINT exploitation within INSCOM is performed by the following elements:

- **National Ground Intelligence Center.** HQ, INSCOM, exercises OPCON over the NGIC. NGIC produces and maintains intelligence on foreign scientific developments, ground force weapons systems, and associated technologies. NGIC analysis includes but is not limited to military communications electronics systems, types of aircraft used by foreign ground forces, CBRNE capabilities, and basic research in civilian technologies with possible military applications. Recent additions to the NGIC mission include biometric intelligence data, databasing, and Counter Improvised Explosive Device Training Program (CITP).
- **203d Military Intelligence Battalion.** The 203d MI Battalion is a multi-component unit headquartered at Aberdeen Proving Ground, MD, and is the Army's only TECHINT battalion. It performs the following functions:
  - Forms the core of the Coalition Joint Captured Material Exploitation Center (CJCMEC). Provides logistics and infrastructure to absorb Joint and interagency TECHINT assets to form the CJCMEC.
  - Conducts multiple CJCMEC missions worldwide.
  - Conducts TECHINT collection and reporting in support of validated S&TI objectives.
  - Conducts TECHINT training for DOD analysts and TECHINT personnel.
  - Supports INSCOM's FMA and FME operations as directed.
  - Analyzes and exploits foreign CEE, weapon systems, and other CEM.
  - Reports on the capabilities and limitations of CEM.
  - Provides recommendations for countermeasures to enemy technical advantages.
  - Provides foreign or enemy equipment familiarization and training.
  - Provides recommendations on the reuse of CEE.
  - Responds to emerging TECHINT missions.

- Provides task-organized battlefield TECHINT teams to support the commander's TECHINT requirements.

US ARMY MATERIEL COMMAND

13-17. The US Army Materiel Command (AMC) plays a significant support role in TECHINT. Among AMC elements are a series of Army research, development, and engineering centers (RDECs), the Army Research Laboratory System, and the US Army Test and Evaluation Command. Each element plays a role in operations by conducting highly technical evaluations of foreign equipment.

13-18. In time of persistent conflict, the AMC conducts FME on equipment purchased by each laboratory and by RDEC for the intelligence community and for DOD. AMC's foreign ordnance exploitation team, located at the Fire Support Armaments Center EOD (Picatinny Arsenal)—

- Exploits foreign ground ordnance.
- Develops render-safe procedures (RSP) for foreign ordnance.
- Prepares detailed intelligence reports to support EOD, intelligence, and US munitions developer communities.

13-19. There are many other agencies with TECHINT responsibilities within the DOD. Refer to FM 2-22.4 for more information on TECHINT.

TECHNICAL INTELLIGENCE IN THE INTELLIGENCE PROCESS

13-20. The TECHINT discipline has several unique considerations throughout the steps of the intelligence process.

GENERATE INTELLIGENCE KNOWLEDGE

13-21. In order to preclude technological surprise on the battlefield, and to plan for countermeasures, US forces must conduct extensive research of joint knowledge databases with relevant intelligence on the threat. This does not only concern weapons the threat may possess but also other equipment, such as frequency hopping and spread spectrum communications, or sonar-elusive mini-submarines. Regardless of the technology, our forces must understand TECHINT characteristics and how the threat will employ technology in the AO long before they deploy into it. Only then can forces continue planning operations in accordance with the MDMP on an informed basis.

13-22. For example, millions of tons of cached munitions from decades of war in locations like North Korea, Iran, Somalia, Afghanistan, and Iraq present a ready store of explosives for use in conventional or irregular warfare. Detailed TECHINT on the types of munitions, associated weapons systems, potential threat employment of munitions, as well as possible friendly use, and munitions locations is a key product of the generate intelligence knowledge task through intelligence reach of national and theater-level database access and data mining will form a key basis for developing a unit's initial intelligence survey. In turn, the intelligence survey will determine key TECHINT gaps, assist in understanding, allocating, and optimizing ISR assets for collection, and how to recognize and understand TECHINT developments which may affect US Soldiers in the AOs.

13-23. Analysis prior to or after deployment into such an area mentioned above may determine that threat forces have access to numerous high explosive and chemical artillery rounds and are capable of detonating IEDs through various electronic means with deadly accuracy most likely resulting in high casualty rates. Counter-IED training in theater and at home station results in Soldier readiness and also prepares units with intelligence and knowledge to understand and attack insurgent networks. Unit and institutional training for TECHINT analysis teams provide a key combat multiplier as well as important links to knowledge centers through intelligence reach and DCGS-A. TECHINT databases serve units in contact as well as follow-on and redeployed units in support of ARFORGEN, particularly in terms of overwatch and lessons learned.

PLAN

13-24. Based on the information or intelligence from the generate knowledge task, the G-2/S-2 refines PIRs and information requirements including TECHINT considerations. Planning must include specialized TECHINT support for both preplanned and contingency operations to ensure these teams are positioned in accordance with operational needs. For example, a BCT commander's PIRs and information requirements may be, "How and where are munitions from other nations entering into the area of operations?" The BCT S-2 coordinates ISR planning with the S-3 for sensitive border surveillance and reconnaissance from air, ground, and water. TECHINT planning considerations include—

- Task-organizing ground reconnaissance units with TECHINT analysis teams or weapons intelligence teams (if available) with biometrics and forensics capabilities.
- Linguists for translation and transliteration.
- Intelligence reach capability to access and query databases and knowledge center analysts.
- IPB analysis indicating NAI and TAI based on an MCOO template.
- Joint capabilities ISR including SOF.

13-25. As other mission requirements changes, TECHINT planning is synchronized with operations according to commander's guidance.

PREPARE

13-26. Training Soldiers is the basis for successful operations. The G-2/S-2 must ensure that required TECHINT analytical assets, resources, and evacuation means are prepared to provide support. This includes verifying coordination effected with the task-organized TECHINT teams from the 203d MI Battalion. The G-2/S-2 must also ensure the means to report and disseminate TECHINT results to the unit and its Soldiers are in place so they can immediately adopt appropriate countermeasures, operations, or tactics in order to enhance their survival and mission accomplishment.

13-27. Once an OPORD, OPLAN, or WARNO related to a TECHINT mission is issued, units may adjust their planning and make further coordination with collaborative analytical and exploitation agencies to augment their forces. In addition, the G-2/S-2 must ensure that required TECHINT analytical assets, resources, and evacuation means are prepared to provide support.

13-28. The G-2/S-2 must also ensure the means, such as DCGS-A, to report and disseminate TECHINT results to the unit and its Soldiers are in place so they can immediately adopt appropriate countermeasures, operations, or tactics in order to enhance their survival and mission accomplishment.

COLLECT

13-29. TECHINT collection includes capturing, reporting, and evacuating CEM. TECHINT collection begins when an organization or individual reports the recovery or acquisition of threat materiel or as ordered by a commander. An item of materiel is exploited at each level, and continues through succeeding higher levels until an appropriate countermeasure to neutralize the item's capabilities is identified or developed.

13-30. US forces safeguard CEM and report it through intelligence channels to the first TECHINT element in the reporting chain. The location of this TECHINT element will be in accordance with the METT-TC factors; however, the TECHINT representative or element will verify if the type of materiel is of intelligence value and determine its further disposition in conjunction with the unit's staff.

PROCESS

13-31. TECHINT processing starts (simultaneously with collection) with the capture of a piece of equipment of TECHINT value. This confirms that the enemy is employing certain materiel of concern to

US forces. In accordance with METT-TC factors, a TECHINT team may move to the location of the item at the capture site or wait until the item is evacuated before conducting initial exploitation.

13-32. After initial exploitation, the team decides if further processing is required. If it is, the items are sent to the JCMEC. If the item is deemed to yield no immediate tactical intelligence value, it may still be evacuated to the S&TI centers in CONUS for further analysis if the systems represent a change in the technological posture of an enemy.

PRODUCE

13-33. TECHINT teams normally report initial and secondary examinations of CEM using either a preliminary technical report or a complementary technical report.

- A preliminary technical report—
  - Includes a general description of the item.
  - Alerts others to information that can be used immediately by tactical units.
- A complementary technical report is more in-depth and—
  - Follows a secondary or an in-depth initial examination.
  - Allows the JCMEC to compare new information with intelligence holdings.

13-34. At each successive echelon of exploitation, TECHINT analysts add to the overall body of information on an item by either adding to previous reports or by preparing new reports. The JCMEC or other national level S&TI activities prepare more advanced technical reports and analyses. These reports include—

- Detailed technical reports.
- Translation reports.
- Special technical reports.

13-35. Other TECHINT products include—

- JCMEC publications such as operator manuals, maintenance manuals, TECHINT bulletins, and tactical user bulletins.
- S&TI analysis bulletins.
- FME reports.
- Weapons intelligence team reports.

ANALYZE

13-36. TECHINT analysts use checklists established by S&TI agencies and the JCMECs to analyze each type of the threat's equipment for which requirements exist. Analysis always begins with what is known, and what is not known, about the piece of equipment. TECHINT units maintain procedures and plans for sampling, analyzing, and handling materiel.

ASSESS

13-37. The primary goal of the TECHINT assess function is to determine whether the results of TECHINT production meet the unit's PIR or intelligence requirements. The G-2/S-2 immediately assesses TECHINT products upon receipt for timeliness, relevance, and accuracy. The G-2/S-2 must inform the TECHINT producer of the extent to which the product answered the PIR or intelligence requirement. Providing feedback to TECHINT analysts helps improve the effectiveness and efficiency of TECHINT.

13-38. The G-2/S-2 also assesses the success of the unit's ISR effort in accomplishing any TECHINT-associated ISR task and shares the assessment with the staff and the pertinent units or personnel.

PROPAGATE

13-39. TECHINT organizations post intelligence studies and TECHINT reports via secure Internet databases as well as through existing intelligence communication architecture. When possible, the preparing organizations share findings with other fusion and analysis elements for maximum effect. Additionally, TECHINT contributes information about threat weapons and equipment and their effectiveness against US forces, providing key input for the COP.

13-40. Relevant TECHINT findings are shared with higher headquarters for operational and strategic application; with adjacent units for pattern and trend analysis; and to lower echelons for situational awareness and general knowledge. They are often used in the development of TTP. Direct dissemination of information contained in TECHINT databases should be sent to the unit responsible for the capture and/or collection of the material, connecting the technical expert with the operational and tactical commanders as often as possible.

13-41. TECHINT of critical importance to the force, including answers to the PIR, is disseminated via the most expeditious means possible. Routine TECHINT reports and products are usually transmitted through the unit's existing intelligence communications architecture in the format of a preliminary technical report.

13-42. For intelligence reach operations, TECHINT products are available and disseminated in a variety of forms. The requestor must ensure that the TECHINT product can be transmitted over the available communications systems. This includes verifying the appropriate security level of the communications systems.

Appendix A

Example Intelligence Summary, Intelligence Estimate, and Intelligence Running Estimate Formats

INTELLIGENCE SUMMARY

A-1. The intelligence summary (INTSUM) contains a brief summary of the most current enemy situation covering a period of time designated by the commander. This period of time will vary with the desires of the commander and the requirements of the situation. It provides a summary of the enemy situation, enemy operations and capabilities, and the characteristics of the terrain and weather and civil considerations.

A-2. The intelligence summary aids in assessing the current situation and updates other intelligence reports. Negative information is included, but no operational information is excluded. The INTSUM reflects the intelligence officer's interpretation and conclusions regarding threat capabilities and probable COAs. The INTSUM is prepared at brigade and higher echelons and disseminated to higher, lower, and adjacent units. The INTSUM has no prescribed format except the word "INTSUM" will be the first item of the report. Figure A-1 shows an example format of an INTSUM. This is neither an all-inclusive nor directed format.

INTELLIGENCE ESTIMATE

A-3. The primary purpose of the intelligence estimate is to—

- Determine the COAs open to the threat and the probable order of their adoption.
- Disseminate information and intelligence.
- Determine PIRs concerning the threat and the AO.

A-4. The intelligence estimate is a logical and orderly examination of the intelligence factors affecting the accomplishment of a mission. It provides commanders with an analysis of the AO and the threat strength and capabilities that can influence their mission. It is used as a basis for planning and disseminating intelligence.

A-5. An intelligence estimate may be prepared at any level. It may be written or oral, formal or informal, detailed or summarized. It is normally written at division and higher and briefed down to battalion. Figure A-2 shows an example format of an intelligence estimate. This is neither an all-inclusive nor directed format.

INTSUM FORMAT

LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(Unit Making Report)
LINE 3 – SITUATION _____	(General Enemy Situation Since Last Report)
LINE 4 – ENEMY FLOT _____	(Current Enemy Front Line Trace)
LINE 5 – ENEMY UNIT SIZE _____	(Enemy Ground Maneuver Units LOCATION/ACTIVITY/Status by Echelon/Size, Location) Strength (Grid), Activity)
LINE 6 – ENEMY ARTILLERY _____	(Enemy Artillery Activity and Estimated Strength)
LINE 7 – ENEMY CBRNE _____	(Enemy CBRNE Activity (Type, Location, DTG))
LINE 8 – ENEMY AIR _____	(Enemy Air and Air Activity)
LINE 9 – ENEMY ENGINEER _____	(Enemy Engineer Activity)
LINE 10 – FORCE PROTECTION AREA THREAT _____	(Enemy FP Area Threat (Light Forces, SF))
LINE 11 – ENEMY'S EST COA _____	(Enemy's Most Probable Courses of Action)
LINE 12 – PIR _____	(Current PIR in Order of Priority and the Phase of Operation)
LINE 13 – ENEMY SUSTAINMENT _____	(Location and Activity of Enemy Combat Sustainment Units) Combat Service Support Units)
LINE 14 – VULNERABILITIES _____	(Analysis of Enemy's Current or Emerging Vulnerabilities)
LINE 15 – WEATHER AND TERRAIN _____	(Analysis of Effects of Weather and Terrain)
LINE 16 – ENEMY COMBAT ASSESSMENT _____	(Summarize Enemy Combat Assessment During Period)
LINE 17 – NARRATIVE _____	(Free Text for Additional Information Required for Clarification of Report)
LINE 18 – AUTHENTICATION _____	(Report Authentication)

6209 **Figure A-1. Example INTSUM format**

Sample of a Division Intelligence Estimate

(Classification)
Copy No ____ of ____ Copies
G2 Section, 52d Infantry Division (Mech)
Glenville (NF3277), EASTLAND
230830Z June 19__

INTELLIGENCE ESTIMATE NO. 20

Reference: Map series EASTLAND, sheets DELTA through KILO, edition 2, 1:50,000.

1. **MISSION**. 52d Division conducts mobile defense along DRY CREEK, accepts no penetration south of HILLS 333 and 421, and prepares to conduct offensive operations within 12 hours.

2. **BATTLEFIELD AREA**.

a. Weather.

(1) Existing situation. Weather for the period 23 June to 28 June will be rainy, and cool, gradually warming and clearing as a high pressure system moves through the area of operations from the south. Temperatures from 40 degrees F to 65 degree F. Visibility will range from 16 to 25 kilometers, except during precipitation and in morning fog in low drainage areas. Surface winds from the south 8 to 10 knots.

Date	BM-NT	BM-CT	EE-CT	EE-NT	Moon-Rise	Moon-Set
23 Jun	0331	0419	2029	2130	1746	0125
25 Jun	0339	0422	2025	2124	1907	0214
27 Jun	0344	0425	2022	2118	2001	0518
28 Jun	0349	0428	2018	2112	2022	0820

(2) Effects on enemy courses of action:
(a) Precipitation will not hinder cross-country movement except in the low drainage areas of MINERTOWN.
(b) Southerly winds will not affect enemy employment of Nuclear Biological and Chemical.
(c) Low visibility during precipitation and morning fog will favor attack.
(3) Effects on friendly courses of action.
(a) Precipitation will not hinder cross-country movement except in the low drainage areas of MINERTOWN.
(b) Southerly wind direction will not affect friendly use of chemical or nuclear weapons.
(c) Low visibility during precipitation and morning fog will not favor friendly defense.

b. Terrain.

(1) Existing situation.
(a) Concealment and cover. Wooded areas around MIDWAY offer good concealment. Numerous ravines in drainage areas of MINERTOWN offer limited concealment and cover.

Figure A-2. Example format of an intelligence estimate

FOR OFFICIAL USE ONLY

(b) Observation and fire. There are good observation points along bluffs above GRINGO River. Fields of fire are excellent throughout plains area north of MUD CREEK but limited moderately in populated and vegetated areas near GLENVILLE.

(c) Obstacles.

1 SWIFT River (fordable 1 kilometer east of GLENVILLE).

2 Bluffs above GRINGO River.

3 City of GLENVILLE. Routes around city are passable; routes through city are impassable.

(d) Key terrain. Hill mass MUKELROY and HILL 333.

(e) Avenues of approach.

1 Available to the enemy into our sector:

a Avenue of approach 1 is from LARGO through gap around the northeast end of HILL 702, 34 kilometers southwest to MINERTOWN and south to DRY CREEK.

b Avenue of approach 2 is from LARGO southeast through MIDWAY to river-crossing east of GLENVILLE.

2 Avenue of approach available for US movement into enemy area will be generally the same as those listed for enemy into our sector.

(2) Effect on enemy courses of action. Terrain favors the enemy attack using avenue of approach 1.

(3) Effect on friendly courses of action. Terrain favors our defense of the area around DRY CREEK.

c. Other Characteristics.

(1) Existing situation. Local nationals throughout the area favor friendly military operations. Large numbers of refugees can be expected to pass through friendly lines.

(2) Effect on enemy courses of action. The enemy can be expected to insert infiltrators as refugees.

(3) Effect on friendly courses of action. Refugees can be expected to provide valuable intelligence.

3. **ENEMY SITUATION**.

a. Disposition. Annex A, Situation Overlay.

b. Composition. Enemy forces opposing 52d Infantry Division(Mech) consist of elements of the 4th Combined Arms Army.

(1) Identified units are:

(a) 10 MRD consisting of:

27th MRR
30th MRR
31st MRR
121st TK Regt (unlocated)

(b) 19th Mech Div Consisting of:

23d MRR
37th TK Regt

(2) Unidentified units are:2XU/IMRR of 19th MRD

c. Strength.

(1) Committed forces. 52d Infantry Division (Mech) is opposed immediately by 4 motorized rifle battalions and 1 tank battalion. These units are supported by normal divisional and regimental artillery.

(2) Reinforcements. Reinforcements available to the enemy for commitment in our zone are a total of 5 motorized rifle battalions and 4 tank battalions from the 27th MRR, 121st TK Regt, and the second echelon battalions of the 30 and 31st MRRs and the 37 TK Regt. Also, the 23 MRR can totally reinforce within 8 hours from start of movement.

(3) Air. Enemy is supported by the 3d Air Army consisting of unidentified numbers of fighter-bomber aircraft, ground attack aircraft, and reconnaissance aircraft. Air parity currently exists with either force capable of obtaining air superiority for limited periods of time. Up to now enemy has used a maximum of 60 fighter-bomber sorties in a 12-hour period.

Figure A-2. Example format of an intelligence estimate (continued)

(4) Nuclear. No estimate of the enemy's nuclear support for the next 30 days is available. Enemy currently has 152mm Sp How with nuclear rounds and SSM which can deliver rounds of 10-50 KT yield within range of our division.

d. Recent and Present Significant Activities.

(1) Air reconnaissance and photo reports indicate increased enemy movement along axis BRAVO to LIMA. movement indicates reinforcement of forward element of 4th CAA.

(2) Enemy's aerial recon and tactical air flights have increased in the last 36 hours, particularly in the line of contact.

(3) For the past 36 hours, volume of vehicular traffic has increased in southerly direction.

(4) Artillery fire from the enemy has become more intensive in the last 24 hours.

(5) Reliable source reports large tracked, amphibious vehicles moving into area vicinity HILL 805.

(6) Enemy has begun to employ smoke along the forward slope of HILL 702.

e. Peculiarities and Weaknesses.

(1) Personnel. Enemy, units are presently estimated to be at 85% to 90% authorized strength. Morale is high, although replacements may not be highly trained.

(2) Intelligence. Enemy stresses communications security and subordinate units of the 4th CAA have recently initiated intensive radio security and procedures training.

(3) Operations.

(a) Enemy is susceptible to mine warfare and antitank weapons.

(b) Enemy has trained heavily on attack formations and has been told offensive action is the only way to victory.

(c) Enemy is vulnerable to nuclear weapons due to massed forces and canalization by further advancement.

(4) Logistics. Supplies are adequate for the enemy's conduct of either the offense or defense. The enemy had previously stockpiled supplies well forward in division areas.

(5) Personalities. G/D Masonski, CG of the 1Oth MRD, is an advocate of penetration type offense on a narrow front with subsequent widening of the gaps to split enemy forces.

4. **ENEMY CAPABILITIES**.

a. Enumeration:

(1) Attack at any time along sense of approach 1 with 4 motorized rifle battalions and 1 tank battalion supported by normal divisional and regimental artillery.

(2) Attack at any time along avenue of approach 2 with 4 motorized rifle battalions and 1 tank battalion supported by normal divisional and regimental artillery.

(3) Defend at any time with forces in contact supported by all available division and regimental artillery.

(4) Reinforce his attack or defense with all or part of the following units at the places and times indicated:

UNIT	PLACE	TIME
(a) 30th MRR (-)	Avenue of approach 2	immediately
(b) 31st MRR (-)	Avenue of approach 1	immediately
(c) 37th TK Regt (-)	Avenue of approach 1	immediately
(d) 27th MRR (-)	Avenue of approach 1 or 2	2 hr after start of movement
(e) 23 MRR	vic LITTLE	8 hr after start of movement
(f) 121st TK Regt	Unlocated	Unknown
(g) U/I MRR of 19th MRD	vic BRAVO	9 hr after start of movement

(5) Delay in successive positions to the east of LITTLE.

(6) Employ chemical agents within our sector at any time.

(7) Employ nuclear weapons of a 0.5-50 KT yield with delivery by artillery or SSM.

(8) Employ guerrilla forces in our rear area either alone or in conjunction with the capabilities enumerated below.

Figure A-2. Example format of an intelligence estimate (continued)

(9) The enemy can attack our area with an undetermined number of fighter, ground attack, and bomb sorties daily. The maximum number of daily sorties mounted in our area has been 60.

b. Analysis and Discussion.

(1) Attack along avenue of approach 1.

(a) The following indicate adoption of this capability:

1 Uses a good avenue of approach.

2 The enemy is massing motorized rifle elements, tanks, artillery and logistic support along this avenue.

3 Forward elements dispersed on a relatively narrow front.

4 Extensive artillery preparation along approach.

(b) The scant cover presented along this avenue of approach is a limiting factor but does not preclude adoption of this capability.

(2) Attack along avenue of approach 2.

(a) The following indicate adoption of this capability:

1 The enemy is massing mechanized elements, tanks, artillery and logistics support along this avenue.

2 Forward elements disposed on a relatively narrow front.

3 Extensive artillery preparation along this avenue.

(b) The following indicate rejection of this capability:

1 This avenue of approach accommodates only one deployed regiment and offers limited cover and concealment.

2 The limited obstacle presented by GLENVILLE.

(3) Defend. The following indicate rejection of this capability:

(a) The enemy is massing his forces along the line of contact.

(b) Enemy has followed known doctrine for attack.

(c) Terrain favors attack.

(4) Reinforce. The following indicate adoption of this capability:

(a) Movement of additional troops toward the front.

(b) New units identified in the combat zone.

(c) Forward logistical buildup.

(5) Delay. There are no indications of the enemy's adoption of this capability.

(6) Use chemical agents. There is no indication the enemy will employ chemical agents other than smoke.

(7) Use nuclear weapons. There is no indication the enemy will use nuclear weapons.

(8) Use guerrilla forces. The following indicates adoption of this capability:

(a) Doctrine calls for use of guerrilla force.

(b) Use would enhance enemy advance by creating panic and confusion.

(9) Air attack. Indications are the enemy will continue to use this capability as referenced in paragraph (9) above.

5. **CONCLUSIONS**.

a. Intelligence. Available intelligence indicates that the division can accomplish its mission. Intelligence support adoption of the division course of action.

b. Weather and Terrain. The weather and terrain favors our defense. The best defensive area is the high ground east of Dry Creek. The best avenue of approach into our defensive sector is avenue of approach 1.

c. Probable enemy courses of action.

(1) Attack with forces in contact supported by air and artillery with the main attack of one motorized rifle regiment along avenue of approach 1. Will reinforce with elements as indicated in para 4a(4).

(2) Conduct secondary attack with forces in contact supported by air and artillery with one mechanized regiment along avenue of approach 2.

(3) Employ guerrilla or special forces in our rear areas in conjunction with the above courses of action.

d. Enemy Vulnerabilities.

(1) The Enemy is vulnerable to counterattack since he has been slow to exploit potential penetrations.

(2) Vulnerable to nuclear attack due to massing of troops and concentrated logistics depots.

Figure A-2. Example format of an intelligence estimate (continued)

(3) Mine warfare will be effective against mechanized elements.

KROOK
BG

OFFICIAL:
/S/ Bagger
BAGGER
GS

Annex:	A	-	Situation	Overlay	(omitted)

Distribution: A

Figure A-2. Example format of an intelligence estimate (continued)

INTELLIGENCE RUNNING ESTIMATE

(CLASSIFICATION)

Headquarters

Place

Date, time, and zone

INTELLIGENCE RUNNING ESTIMATE NO. ____

References: Maps, charts, or other documents.

1. MISSION.

The unit's mission determined by the commander.

2. AREA OF OPERATION (IPB step 1).

State the unit's area of operation (AO) and established area of interest (AOI). Both physical and human geography must be taken into account. Consider tribal lines, family lines, cultural lines, economic lines, as well as physical lines such as roads and bodies of water. Cross-border ties may allow insurgents safe haven outside their country and aid in smuggling across the border. Information in this paragraph is based upon the facts and conclusions of intelligence preparation of the battlefield (IPB) and the analysis of the AO.

a. Terrain (IPB step 2).

(1) **Existing situation**. Terrain analysis observation and fields of fire, avenue of approach, key terrain, obstacles, concealment and cover [OAKOC]), analyzing the physical geography (natural and manmade features). In counterinsurgency (COIN) operations, emphasize complex terrain, suburban and urban terrain, key infrastructures, and lines of communication (LOCs). Complex terrain is multifaceted, with physical, social (human), and informational dimensions. Include as much information as necessary for an understanding of OAKOC. Geospatial engineer elements conduct a major portion of the terrain analysis. Geospatial overlay products include vegetation (tree spacing and trunk diameter), surface drainage (stream width, depth, velocity, bank slope, and height), surface materials (soil types and conditions that affect mobility), surface configuration (slopes that affect mobility), obstacles (natural and manmade—consider obstacles to flight as well as ground mobility), transportation systems (bridge classifications and road characteristics such as curve radius, slopes, and width), and effects of actual or projected weather such as heavy precipitation or snow cover.

Analyze the military aspects of terrain (OAKOC). **Observation and Fields of Fire:** Evaluating observation and fields of fire allow you to identify fire sacks and kill zones, ambush sites, engagement areas, battle positions, and defensible terrain. Identify specific system or equipment positions, and areas where maneuvering forces are most vulnerable to observation and fires. Include both visual or with the use of surveillance devices, include electronic and optical line of sight. Include friendly and enemy systems such as weapon sights, laser range finders, radars, radios, and jammers. Identify observation posts and listening posts, areas of visual dead space. **Avenues of Approach:** An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Include air and ground routes (and mobility corridors), to assist in development of named areas of interest (NAIs) and target areas of interest (TAIs), infiltration routes, and exfiltration routes; **Key Terrain:** For enemy and friendly units—tall structures, choke points, intersections, bridges, industrial complexes.

6428 **Figure A-3. Example of an intelligence running estimate format**

In COIN, the people of the area are always key terrain. **Obstacles:** Manmade or natural terrain that stop, impede, or divert military movement. Examples include cant and slope, intervening crests, rivers, lakes, forests, deserts, swamps, jungles, built-up areas, densely populated areas, buildings, road craters, minefields, and trenches. Obstacles to air mobility include features that exceed the aircraft's service ceiling restrict nap-of-the-earth flight or that force the aircraft to employ a particular flight profile, and obstacles that affect the aircraft landing zone and drop zone. Examples are tall trees, towers, power lines, buildings, rapidly rising terrain features, mountains, and smoke or other obscurants. **Cover and Concealment:** Cover examples from direct and indirect fires include ditches, caves, river banks, folds in the ground, ridges, fingers, forested and built-up areas, shell craters, buildings, walls, and embankments. Concealment examples include woods, underbrush, snowdrifts, tall grass, and cultivated vegetation. The evaluation of cover and concealment aids in identifying defensible terrain, possible approach routes, assembly areas, deployment and dispersal areas, ambush sites or positions, specific system or equipment locations, and battle positions.

Use graphic representations and overlays. Use annexes for detailed material. Include effects of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) and enhanced conventional weapons fires, and any other pertinent considerations on each of these factors as appropriate.

(2) **Effect on enemy operations and broad COAs**. Describe the effects of terrain on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Include how the terrain affects the threat's use of CBRNE weapons, and any special methods, techniques, equipment, procedures, or forces the threat may have.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

b. Civil Considerations.

(1) **Existing situation.** Civil Considerations (ASCOPE) are analyzed for all types of military operations. Civil considerations of the environment can either help or hinder friendly personnel and mission, as well as the threat's personnel and mission. Understanding the impact on military operations better prepares the commander and staff, and enhances situational awareness and situational understanding. Analyze civil considerations using the acronym ASCOPE: Areas, Structures, Capabilities, Organizations, People, Events. Use templates and overlays to graphically depict civil considerations areas analyzed.

(a) **Areas.** Analyze the localities and aspects of the terrain that are not normally militarily significant to determine key civilian areas. Analyze the key civilian areas to determine how military operations affect these areas, and how these areas affect military operations. Examples of key civilian areas are (1) Boundaries, (for example, political precincts and districts, districts within a city, or municipalities within a region; boundaries for social, religious, or criminal enclaves; (2) Government centers; (3) Commercial zones (for example, agricultural regions, mining regions, trade routes; (4) LOCs (for example, street patterns, urban patterns, subterranean passages and underlying terrain; and (5) Possible sites for military applications (for example, temporary settlement of displaced civilian camps or other civil functions).

(b) **Structures.** Structures include (1) high-value targets (HVTs) or HPTs (for example, bridges, communication towers, power plants, dams; (2) cultural sites protected by international law or other agreement (for example, churches, temples, mosques, national libraries, and hospitals; (3) Structures that have practical applications which can support military operations (for example, jails, warehouses, television and radio stations, and print plants.

6429 **Figure A-3. Example of an intelligence running estimate format (continued)**

(c) **Capabilities.** Host nation (HN), aggressor nation or some other body's ability to provide key functions or services to save, sustain, or enhance life (in that priority). Examples include emergency services, fire and rescue, food, water supply, fuel, electric power stations, communication facilities, health services, public works and utilities, public safety, public health, public administration, economics, commerce, and technology. Also include resources and services that can be contracted to support the military. Examples include interpreters, laundry services, construction materials, and equipment.

(d) **Organizations.** Non-military groups or institutions in the AO that interact and influence with the populace and the force. Indigenous examples include church groups, fraternal organizations, patriotic or service organizations, labor unions, criminal organizations, and community watch groups. Groups from outside the area include corporations, United Nations agencies, US governmental agencies, and NGOs, such as the International Red Cross/Red Crescent. Include information on their activities, capabilities, and limitations, how their activities affect military operations, and vice versa.

(e) **People.** Civilians within or outside the AO whose actions, opinions, or influence can affect the mission, either positively, negatively, or neutrally. Analyze and identify by their capabilities, needs, and intentions. Consider historical, cultural, ethnic, political, economic, humanitarian factors, key communicators, formal and informal influences. Examples to include are history of the area and how it influences the insurgency, events leading or contributing to the insurgency; tribal, clan, or familial groups and their geographic location and their influences; religious groups, their geographic location, and their influences; ethnic groups, their geographic location and their influences; languages spoken; key people who influence the society, their affiliations and loyalties, and their interrelations with other people; public perceptions of the insurgency; points of agreement or disagreement with insurgent ideology or ideologies; major industries and sources of employment; communication links to other regions; and media influence on local populace.

(f) **Events.** Events are routine, cyclical, planned, or spontaneous activities that significantly affect people, organizations, or military operations. Examples include national and religious holidays, agricultural crop or livestock and market cycles, elections, civil disturbances, and celebrations. Examples of spontaneous events include disasters from natural, manmade, or technological sources. These events create civil hardship and require emergency responses. Also include events precipitated by military forces. Examples include combat operations, deployments, redeployments, and paydays. Once significant events are determined, template and analyze the events for their political, economic, psychological, environmental, and legal implications.

(2) **Effect on enemy operations and broad COAs.** Describe the civil considerations effects on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Also include how the threat's use of CBRNE weapons and any special methods, techniques, equipment, procedures, or forces the threat employees affects civil considerations, and vice versa. Use templates and overlays.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

c. Weather.

(1) **Existing situation**. The main portion of weather analysis is conducted by the Air Force Staff Weather Officer (SWO). Using geospatial intelligence (GEOINT) principles and techniques, the engineer detachment works closely with the SWO to ensure the terrain analysis incorporates the effects of current and projected weather, thus enhancing automated support of the terrain analysis process.

6430 **Figure A-3. Example of an intelligence running estimate format (continued)**

Include climate, current weather report, and weather forecasts on the overall environment. Evaluation of the military aspect of weather include visibility, winds, precipitation, cloud cover, temperature, and humidity. The analysis focus is on the effects of weather on military operations rather than on the factors that make up the analysis. Include thermal crossover, a natural phenomenon which normally occurs twice daily when temperature conditions are such that there is a loss of thermal contrast between two adjacent objects. Include light data for the period of time of military operations. Use appendixes for detailed information.

(2) **Effects on METT-TC**. Describe how the weather favors or disfavors mission, enemy, terrain and weather , troops and support available, time available, and civil considerations (METT-TC).

d. Other Characteristics. When applicable, include other characteristics not covered above. Analyze using the same subheadings (existing situation, effect on enemy operations, effect on own operations and COA). Examples of other characteristics may include wildlife or diseases.

3. ENEMY SITUATION.

This paragraph gives information on the enemy, which will permit later development of their capabilities and vulnerabilities, and refinement of these capabilities into specific COAs and their relative probability of adoption.

a. Composition.

In conventional operations: Summary of threat characteristics that can influence accomplishment of the mission. Include state and unit organization. Special mention is made of electronic warfare (EW), special operations forces (SOF), and CBRNE, as appropriate. **In COIN operations:** Key influential people; political cadre, cells, organization; C2 staff (internal and external), intelligence cells, attack teams and operation cells, finance (internal and external), logistic and support cells, external ties; and, as required, religious organization; ethnic organization; tribal organization; and family organization. Special mention is made of EW, SOF, and CBRN, as appropriate. Reference other documents, as required.

b. Disposition.

In conventional operations: Geographic location of threat elements and how they are deployed or employed. Include recent, current, and projected movements. Reference overlays, situation maps (SITMAPs), previously published documents. **In COIN operations:** Areas of control (religious, ethnic, tribal, political, and/or familial demographics and neighborhoods), C2 locations, safe houses, front organizations, training camps, and sustainment and support locations.

c. Strength.

In conventional operations: Committed forces, reinforcements, air, and CBRNE weapons. The preponderance of strength or lack thereof affects the raising or lowering of the analyst's estimate of the enemy capabilities and vulnerabilities in paragraph 5. Information concerning strength provides an indication of threat capabilities and helps determine the enemy probable COAs or options open or closed.

(1) **Committed Forces.** Include ground maneuver units currently in contact and those ground maneuver units with which imminent contact can be expected, regardless of the specific friendly COA, location, controlling headquarters, and doctrine. The intelligence officer usually accounts for committed forces based upon the size of unit doctrinally used to oppose the friendly unit. Generally, enemy units are

6431 **Figure A-3. Example of an intelligence running estimate format (continued)**

6432

counted in terms of units two echelons below the friendly unit's size. (For example, a brigade S-2 normally considers committed forces in terms of companies; a division G-2 in terms of battalions; and a corps G-2 in terms of regiments or brigades.) If there is doubt whether a unit is a committed force or a reinforcement, it is considered a reinforcement. This attributes to the enemy the maximum capability to reinforce forces to oppose a given friendly COA.

(2) **Reinforcements.** Include designation and location. Reinforcements are those enemy maneuver units that may or may not be employed against friendly forces, depending upon our specific choice of a COA and upon enemy plans. Reinforcements are enemy units not committed in or out of the friendly sector, but which can react to the friendly COA, subject to time and distance considerations, in time to influence the accomplishment of the mission. Imminent contact is not expected. Disposition, location, level of control, or other factors at the time of the estimate are considered in determining which enemy forces are reinforcements.

(3) **Air**. List the number of enemy aircraft by type within operational radius; if known, include the number of possible sorties per day by type of aircraft.

(4) **CBRNE Weapons and Agents.** Estimate, as appropriate, the number, type, yield, and the delivery means of enemy CBRNE weapons or agents available to the enemy.

In COIN operations: Generating popular support is the center of gravity of the insurgency. Insurgent strength is measured largely by how much popular support the insurgency has. As the insurgent group gains in support, its capabilities grow, which in turn enable it to gain more support. Popular support results in safe havens, freedom of movement, logistical support, financial support, intelligence, and new personnel for the insurgency. A gain in support for the insurgents is a loss for the government, and a loss of support for the government is a gain for the insurgents. Evaluate and list the following:

(a) Level of popular support to the insurgency relative to the government includes regional, national, international support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving sustainment, or just withholding information. Include information on the areas they control (religious, ethnic, tribal, political organization, demographics, and neighborhoods).

(b) Forms of popular support the insurgents receive may include safe havens, freedom of movement, logistical support, financial support (internal and external), intelligence, and recruitment for the threat.

(c) Sources of popular support by type (active, passive, internal, external).

(d) Segments of populace supporting the insurgency.

(e) Foreign government support may come from a variety of venues; for example, influential figures pronouncing support; training facilities or safe houses; recruitment, financial support; and providing safe passage across national or international borders. The insurgency may also receive sustainment from national and international countries.

(f) NGO support.

(g) Criminal network support.

(h) Other sources of support.

(i) Methods used to generate popular support and their effectiveness.

(j) Grievance (real or perceived) exploited by insurgents.

(k) Capabilities and vulnerabilities in generating popular support.

6433 **Figure A-3. Example of an intelligence running estimate format (continued)**

6434

(l) Attack teams and operation cells.

(m) Recruitment.

d. Tactics and Training. In conventional and COIN operations list strategy, methods of operations, and doctrine, tactics, and training or other information of interest that provide a basis for analysis to determine relative probability of adoption of specific COAs and to determine enemy vulnerabilities. Enemy failure to take expected action is listed, as well as positive information. In COIN operations, tactics also involve political, military, psychological, and economic considerations. Tactics may include assassinations, arson, bombings, hostage taking, kidnapping, hijacking, seizure, raids, sabotage, denial and deception, hoaxes; use technology to destroy key elements of the national infrastructure—transportation, telecommunications, energy, banking, public health, and water supply; and use CBRNE.

e. Sustainment. Analysts can more accurately evaluate the enemy capabilities, strengths, and combat effectiveness. With knowledge of the enemy's sustainment and support structure. The enemy's adoption of a COA depends on the logistical system to support the action. In conventional operations include procurement, maintenance, distribution, and replacement of all types of material including transport of personnel. In COIN operations, sustainment may include weapons and ammunition, IED and bomb-making components, food, water, propaganda equipment and materials, medical, transportation, and finance. Finance is who is providing the threat with financial support, how the money is transferred, and which financial institutions the enemy uses.

f. Operational Effectiveness. Operational effectiveness studies the threat morale, weapons effectiveness, equipment readiness, leadership, and personnel. Strength must be tied to the operational effectiveness, but is important enough to have its own mention earlier in the estimate. Conventional weapons, such as artillery ranges, should be addressed here.

g. Intelligence. Estimate the enemy's intelligence collection capability. Include how threat picks and evaluates a target; method of ISR; ISR success, ISR vulnerabilities, or ISR susceptibility to deception and detection. HUMINT, IMINT (including threat use of commercial software) and EW capabilities must be addressed if known. How the threat passes intelligence information—radio, cell phone, electronic message—and how it can be interdicted.

h. Communications. Evaluate and list enemy's communication modes may include high-frequency short wave, cell phone, Internet, mail, courier, face-to-face, Citizen Band, or Amateur radio sets or the drop system.

i. Other. Use the threat characteristics listed in chapter 3 and include any other factors necessary for creating as thorough a picture of the threat as possible.

4. ENEMY CAPABILITIES.

Based upon all the previous information and analyses, develop and list enemy capabilities and limitations. A capabilities listing provides a basis for analyzing the available information. It shows those capabilities the enemy can adopt as specific COAs and their relative probability of adoption.

In COIN operations: The listing should show the task and purpose.

In conventional operations:

a. State enemy's capabilities. State what, where, when, and in what strength for each capability.

b. State enemy's limitations. Discuss each limitation, the cause and effect.

6435 **Figure A-3. Example of an intelligence running estimate format (continued)**

6436

c. Analysis and Discussion. Discuss each capability (or appropriate combination of capabilities) in a separate subparagraph, and any effects of the terrain, civil considerations, and/or weather may have on each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

In COIN operations. Evaluation of the threat in COIN operations must begin early and cover a wide range of factors in building an accurate threat model. Based upon all the information and analysis, develop and list enemy capabilities. First, evaluate the following characteristics of the insurgency as a basis for evaluating the enemy COA.

a. Insurgent goals. Does the threat desire a different social or political organization than that which exists under current conditions? How will they conduct operations towards that goal?

b. Insurgent motivations. Are they motivated by ideological, religious, or monetary?

c. Popular support. Include regional, national, and international.

d. Key leaders and personalities. Key influential people, political, ideological, religious, military, and key members who bring expertise (demolition special weapons, assassinations, specialized trainers) staff members, family members, and informal leaders.

e. Organization.

f. Morale of the leaders and members.

g. Then, evaluate the enemy's capability to conduct operations. This should tie in with Operational Effectiveness (paragraph 3f above). State each capability as a task and purpose. State what, where, when, and in what strength for each task. State enemy's limitations and vulnerabilities. Include the cause and effect of the limitation. Evaluate the following capabilities of the insurgency as a basis for evaluating the threat COA:

(1) Conduct violent activities (for example, murder, assassination, arson, bombing, hostage taking, kidnapping, hijacking, seizure, and raids).

(2) Conduct other operations (for example, sabotage, denial and deception, hoaxes, and use of technology).

(3) Conduct intelligence operations.

(4) Conduct training.

(5) Conduct sustainment and supply activities.

(6) Conduct information activities.

(7) Conduct political activities.

(8) Conduct recruitment.

h. Analysis and Discussion. Discuss each capability (or appropriate combination of capabilities). In a separate subparagraph, include any effects of the terrain, civil considerations, and/or weather may have on

6437 **Figure A-3. Example of an intelligence running estimate format (continued)**

6438

each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

5. CONCLUSIONS.

Based upon all the previous information and analysis, state conclusions concerning the total effects of the AO on threat operations. List all the possible threat COAs in the order of probability of adoption. Include threat vulnerabilities that can be exploited. State which COAs are considered most likely and those that are the most dangerous COAs. This will assists the commander and staff in selecting friendly COA during wargaming.

a. Probable threat COAs. List COAs in order of relative probability of adoption. A listed COA may include several subordinate COAs that can be executed concurrently. Usually, no more than two or three COAs, in order of probability of adoption, can be justified by the available evidence. The G-2/S-2 should identify which COA is most likely and which is most dangerous at a minimum.

b. Threat vulnerabilities. List the threat peculiarities and weaknesses that result in vulnerabilities which are exploitable at own, higher, or lower levels of command.

c. Intelligence consideration on operations. Indicate whether the mission set forth in paragraph 1 above can be supported from the intelligence standpoint. Indicate which COAs can best be supported.

/s/_____

(Designation of staff officer)

(CLASSIFICATION)

6439 **Figure A-3. Example of an intelligence running estimate format (continued)**

Appendix B

Language Support

ROLE OF LINGUISTS

B-1. Military operations are highly dependent on military and contractor-provided foreign language support. The requirement to communicate with and serve on multinational staffs, communicate with local populations, and exploit enemy forces necessitates the use of linguists. The growing focus on multinational operations increases the competition for limited linguist resources that are vital for mission success. This appendix establishes the framework and process to access, prioritize, and employ the Army's limited organic linguist resources.

LINGUISTIC SUPPORT CATEGORIES

B-2. Foreign language support requirements of US Armed Forces typically fall into one of four broad categories:

- **Intelligence and Information Collection.** This category includes the traditional SIGINT and HUMINT disciplines, as well as foreign language support to protection and exploitation of open-source information.
- **Operations and Multinational Liaison.** This category includes the coordination of military operations and liaison with multinational partners, previously unaffiliated nations, and at times adversary or former adversary nations. Multinational operations are becoming more common and increasingly important.
- **Civil Affairs Activities.** CA activities enhance the relationship between civil authorities in areas with military forces. They involve applying CA functional specialty skills to areas normally under the responsibility of civil government. These operations involve establishing, maintaining, influencing, or exploiting relations between military forces and all levels of HN government agencies. These activities are fundamental to executing stability tasks. CA personnel, other Army forces, other government agencies, or a combination of all three perform these tasks. Foreign language support is critical to CA in areas such as government liaison, legal agreements, medical support and operations, law enforcement, engineering projects, public safety, security and population control, and PSYOP.
- **Sustainment.** This category consists of foreign language support to sustainment functions. These functions include logistical contracting, port, railhead, airhead, or transshipment operations and convoy operations.

DETERMINING LINGUIST REQUIREMENTS

B-3. To identify linguist requirements, the staff conducts mission analysis and identifies specified or implied tasks requiring foreign language support. Other critical factors are the organization or echelon of command and the location of the mission. The staff uses these criteria to determine the allocation of linguists, such as one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed. The staff then applies METT-TC to determine the number of linguists needed for an operation.

B-4. The staff must analyze each linguist assignment to determine the minimum level of foreign language proficiency needed. While interpretation for a peace negotiation requires not only outstanding linguistic capability but also cultural acumen, the translation of routine documents (with the aid of a dictionary)

requires a much different skill set. Poor identification of linguist proficiency requirements can tie up the best linguists in less effective roles, creating linguist shortfalls in other areas.

B-5. The relative importance of each of the four linguist support categories is mission dependent. For example, during a noncombatant evacuation operation civil and military coordination would probably not be as critical as intelligence and information collection. However, the situation is reversed for stability missions. Identifying these "dynamics" helps the commander and staff prioritize linguist requirements.

B-6. Determining linguist requirements for any operation can be difficult because each operation is unique. However, commanders and staffs with a basic knowledge of organic Army linguistic assets, foreign language resource alternatives, and MI skills can successfully assess, prioritize, and employ linguists in support of their military operations.

PLANNING AND MANAGING LINGUIST SUPPORT

B-7. Commanders must consider the linguist requirements as part of their MDMP for every contingency plan and OPLAN assigned to their commands. Prior staff planning and identification of linguist requirements should prompt commanders to initiate linguist support requests and identify command relationships prior to actual operations.

B-8. If the mission analysis reveals requirements for linguistic support, the commander must identify what foreign languages are needed, the foreign language proficiency levels needed for each assignment, and the best source of linguists. In addition, if the mission includes intelligence and information collection, the commander must identify MI collection skills required. During mission analysis, commanders should consider linguist requirements for every contingency plan and OPLAN assigned to their command.

LINGUIST CATEGORIES

B-9. The commander and staff must identify linguist requirements by category:

- **Category I** – Have native proficiency in the target language (level 4-5) and an advanced working proficiency (Interagency Language Round Table [ILRT] level 2+) in English. They may be locally hired or from a region outside the AO. They do not require a security clearance. They must be screened by the Army CI support team.
- **Category II** – Are US citizens screened by Army CI personnel and are granted access to SECRET by the designated US Government personnel security authority. Have native proficiency in the target language (level 4-5) and an advanced working proficiency (ILRT 2+) in English.
- **Category III** – Are US citizens screened by Army CI personnel and are granted either TS/SCI clearance or an interim TS/SCI clearance by the designated US government personnel security authority. Meet a minimum requirement of ILRT 3. They are capable of understanding the essentials of all speech in a standard dialect. They must be able to follow accurately the essentials of conversation, make and answer phone calls, understand radio broadcasts and news stories, and oral reports (both of a technical and non-technical nature).

PRIMARY STAFF RESPONSIBILITIES

B-10. Primary staff at each echelon has responsibilities for evaluating requirements and managing linguist support. The responsibilities include but are not limited to those discussed below. In addition, each staff section is responsible for determining its linguist support required to meet its operational missions.

ASSISTANT CHIEF OF STAFF, G-1 (S-1):

- Identify linguist requirements needed to support G-1/S-1 functions in all contingency areas. G-1/S-1 requirements for linguist support include but are not limited to the following:

- Coordinate with local authorities on matters of civilian hire, financial management, and recordkeeping.
- Coordinate for local morale support and community activities.
- Coordinate with local authorities for postal operations.
- Support for administration, counseling, personal affairs, and leave for local national and third-country national personnel.
- Liaison with multinational counterparts.

- Linguist staffing and linguist replacement management.
- Identify foreign language skill identifiers for all assigned, attached, or OPCON Army linguists.
- Identify all Army foreign language skilled Soldiers not identified on electronic Military Personnel Office System or the Defense Integrated Military Human Resource System (DIMHRS).
- Deploy and provide human resource support to DA and DOD civilian linguists.
- Provide human resource support for LN linguists.
- Procure Army foreign language support personnel for screening local labor resources.

ASSISTANT CHIEF OF STAFF, G-2 (S-2):

- Identify linguist requirements needed to support G-2/S-2 functions in all contingency areas. G-2/S-2 requirements for linguist support include but are not limited to—
  - Identifying Category II and Category III linguist requirements.
  - Evaluating and/or using local maps and terrain products in operations.
  - Processing for MI purposes material taken from detainees or civilian internees.
  - At lower echelons, conducting Soldier surveillance and reconnaissance.
  - Assessing local open-source information for intelligence value.
  - Coordinating intelligence and liaison with multinational and HN counterpart.
- Determine, during the initial IPB, all foreign languages (spoken and written) and dialects needed for mission accomplishment.
- Collect, process, produce, and disseminate information derived from linguist sources.
- Provide intelligence training for MI linguists employed in AOs.
- Coordinate for security investigations, as necessary, for local hire linguists.
- Provide support to CI screening of contracted linguists and LN labor force.

ASSISTANT CHIEF OF STAFF, G-3 (S-3):

- Identify linguist requirements needed to support G-3/S-3 functions in all contingency areas. G-3/S-3 requirements for linguist support include but are not limited to—
  - Identify CAT II and CAT III linguist requirements.
  - Operational coordination and liaison with multinational and HN counterparts.
  - Translate OPORDs and OPLANs for use by multinational counterparts.
- Consolidate unit linguistic requirements and establish priorities.
- Develop linguist deployment and employment plans.
- Develop plans to train linguists and to use linguists for training the force in AO's foreign language survival skills. In addition to global language skills, linguists must have training in specific vocabulary used in the AO; for example, terms used for military, paramilitary, civilian or terrorist organizations, and ethnic groups within the area, nomenclatures of equipment used, and other military or technical vocabulary. Training in the specific dialect used in the AO would also be beneficial.
- Assign, attach, and detach linguists and linguist teams.

- Integrate additional or replacement linguists through operational channels.
- Recommend modernization and development of linguist systems and methods.
- Coordinate mobilization and demobilization of USAR and USARNG linguist support.
- Plan linguist usage for deception operations.
- Plan linguist support for movement of EPWs, detainees, and displaced civilians.
- Coordinate evaluation of linguist support by all staff elements.

ASSISTANT CHIEF OF STAFF, G-4 (S-4):

- Identify linguist requirements needed to support G-4/S-4 functions in all contingency areas. G-4/S-4 linguist requirements for linguist support include but are not limited to—
  - Procure local supply, maintenance, transportation, and services.
  - Coordinate logistics at air and seaports of debarkation.
  - Contract with local governments, agencies, and individuals for sites and storage.
  - Contract for and hire local personnel.
- Provide logistical, supply, maintenance, and transportation support to attached linguists.

ASSISTANT CHIEF OF STAFF, G-6 (S-6):

- Identify linguist requirements needed to support G-6/S-6 functions in all contingency areas. G-6/S-6 linguist requirements for linguist support include but are not limited to—
  - Coordinate suitable commercial information systems and services.
  - Coordinate with multinational forces on command frequency lists.
  - Coordinate signal support interfaces with HN and multinational forces.
- Manage RF assignments for supporting linguist elements.
- Support linguist operations with internal document reproduction, distribution, and message services.
- Integrate automation management systems of linguist units.

ASSISTANT CHIEF OF STAFF, G-7 (S-7):

- Foster and support mutually planned and synchronized PSYOP and information operations efforts.

ASSISTANT CHIEF OF STAFF, G-9 (S-9):

- Identify linguist requirements needed to support G-9/S-9 functions in all contingency areas. G-9/S-9 linguist requirements for linguist support include but are not limited to—
  - Determine civilian impact on military operations.
  - Minimize civilian interference with operations.
  - Recommend curfews, movement restrictions, and relocations if applicable.
  - Provide assistance to liaison with HN and multinational agencies, dignitaries, and authorities.
  - Promote positive community programs to win over support.
  - Determine if multinational operations PSYOP efforts are mutually planned and synchronized.
  - Support, as necessary (to include interpreters) resolution of civilian claims against the US Government.
  - Protect culturally significant sites through command recommendations.
  - Use linguistic and cultural support to identify cultural and religious customs.

- Assist the G-1 in the administrative support to identify linguists and G-4 in the contracting of local hires (especially linguists).
- Identify foreign language requirements to support stability operations.
- Identify and adjust use of HN and other resources (such as linguists and labor) available from civil authorities.

SPECIAL STAFF OFFICER RESPONSIBILITIES

B-11. Linguist requirements for special staff officers include but are not limited to the staff officers shown in table B-1.

6619

Table B-1. Special staff officer responsibilities

SPECIAL STAFF OFFICER	*RESPONSIBILITIES*
Liaison Officers	• Should speak the required foreign language. If not, they require a translator or interpreter for all aspects of their duties. • Request interpreters to assist when representing the multinational operations. • Translate orders, maps, traces, overlays, and documents into multinational foreign languages.
Civilian Personnel Officers	• Recruit, interview for suitability, and hire civilian local labor force if required. • Negotiate host country on labor agreements.
Dental Surgeon	• Administers dental care to support humanitarian mission requirements. • Rehabilitates, constructs, and gains access to existing dental facilities as required.
Financial Management Officer	• Supports the procurement process of local goods and services not readily available through normal logistical channels. • Ensures limited non-US and US pay functions to foreign national, HN, civilian internees, and detainees are provided. • Ensures all necessary banking functions are performed in theater.
Surgeon	• Supports medical humanitarian assistance and disaster relief operations. • Provides medical care of detainees and civilians within the command's AO. • Coordinates medical laboratory access in AO. • Determines the nature of local health threats to the force through populace interviews. • Determines the identity of local or captured medical supplies.
Veterinary Officer	• Determines source and suitability of local foods. • Assists the local population with veterinary service needs.
Chemical Officer	• Identifies enemy force chemical weapons and equipment. • Communicates CBRNE risks to supported populations.
Engineer Coordinator	• Procures proper local materials to support engineering missions. • Communicates engineering project requirements to contracted local work force. • Communicates engineering project impact on local landowners and other affected parties. • Determines, in coordination with G-2/S-2, suitability of local topographic maps and terrain products. • Assesses environmental concerns of HN and local populations in combined operations.
Provost Marshal	• Supports displaced civilian control activities. • Supports internment and resettlement operations, to include displaced civilians. • Supports weapons buy-back programs, as required, and works closely with civil-military liaisons for payments to local officials. • Supports counter-drug and customs activities. • When authorized, helps foreign civil authorities maintain control. • Conducts liaison with local LEAs.
PSYOP Officer	• Produces approved PSYOP propaganda and counter-propaganda media. • Evaluates PSYOP impact on target audience.

6620

Table B-1. Special staff officer responsibilities (continued)

SPECIAL STAFF OFFICER	*RESPONSIBILITIES*
Air Defense Coordinator	• Supports identification of enemy air defense artillery. • Communicates air defense warnings to supported populations. • Communicates air defense project requirements to contracted local work force.
Safety Officer	• Provides safety training to local labor force. • Communicates warnings of dangerous military operations and other hazards to local populace.
Transportation Officer	• Coordinates commercial and local transportation needs. • Coordinates movement scheduling and routes with multinational forces and/or HN.
Surgeon	• Determines the nature of local environmental health threat to the force through populace interviews.

6621 # PERSONAL STAFF OFFICER RESPONSIBILITIES

6622 B-12. Linguist requirements for special staff officers include but are not limited to the staff officers shown
6623 in table B-2.

Table B-2. Personal staff officer responsibilities

PERSONAL STAFF OFFICER	*RESPONSIBILITIES*
Chaplain	• Coordinates religious support with multinational partners. • Determines the impact of local population religious group faiths and practices on military operations. • Provides religious support to the community to include hospital patients, detainees, displaced civilians, and civilian detainees. • Conducts liaison with local population religious leaders in close coordination with the G-9.
Public Affairs Officer	• Acts as the commander's spokesman for all communication with external media. • Assesses the accuracy of foreign media interpretation of Public Affairs Office (PAO) releases. • Assesses and recommends news, entertainment, and other information (assisting G-9) for contracted services foreign nationals.
Staff Judge Advocate	• Translate and interpret foreign legal codes, SOFAs, and international laws. • Determines local environmental laws and treaties through translation services. • Assesses the treatment of detainees and civilian internees. • Translates documents to support G-4 in local contracts.

6624 # SOURCES OF LINGUISTS

6625 B-13. There are various sources that a commander can use to obtain the linguists necessary to support
6626 operations. It is vital to know the advantages and disadvantages of each type of linguist and to carefully
6627 match the available linguists to the various aspects of the operation.

ARMY LANGUAGE-QUALIFIED MOS/AOCS

B-14. The MI language-dependent enlisted MOSs are 35P with an SQI of L (Cryptologic Communications Interceptor/Locator) and 35M (HUMINT Collector) and their related WO AOC of 352P and 351M. Some Soldiers in MOS 35F (All-Source Intelligence Analyst), MOS 35L (CI Agent), and MOS 35N (SIGINT Analyst), and their related WO AOCs 350F, 351L, and 352N are trained in foreign languages.

B-15. Utilizing Soldiers in the MOSs and AOCs mentioned above has many advantages. They are already trained in the military system, are not subject to deployment restrictions (a limiting factor with civilian linguists), have a security clearance and, as US personnel, support the command's interests. The major disadvantage to utilizing these individuals for general foreign language support is that in doing so, they are removed from their primary MI functions. They should be used only in linguistic duties that include intelligence potential.

B-16. Non-MI Army language-qualified enlisted MOSs and officer AOCs are in career management fields/branch codes 18 (Special Forces [enlisted and officers]), 37 (PSYOP), 38 (CA), 180A (Special Forces WO); and functional area 48 (Foreign Area Officer). Particular attention must be paid to the recorded language proficiency and test date of these individuals since the standards vary by field. The same advantages and disadvantages apply as with the MI linguists.

B-17. The Army also includes linguists in MOS 09L (translator/interpreter). The 09Ls are specifically trained to be a translator and interpreter. They have the same advantages as listed above for language-dependent MOS/AOCs. An added advantage is that since their sole job is translation and interpretation, they do not have to be removed from another job in order to be used as a linguist. Their major disadvantage is that they have no additional skill that gives them dual functionality as do the 18, 37, 38, 180A MOSs/AOCs.

ARMY LINGUISTS NOT DOD TRAINED

B-18. The Army also includes numerous Soldiers of all grades who are proficient in a foreign language and are receiving a Foreign Language Proficiency Bonus (FLPB) in accordance with AR 11-6 but whose primary duties do not require foreign language proficiency. They may have attended a civilian school to learn a foreign language, or they may have acquired proficiency through their heritage. They have the advantage of being trained Soldiers and are therefore readily deployable throughout the AO.

B-19. These Soldiers may have the specific vocabulary and military skill knowledge for certain linguist support missions. For example, a supply sergeant who speaks the local language would be an invaluable asset to the G-4. There are disadvantages in that they already have another job and units are reluctant to give up personnel especially if they are in key positions. Their capabilities are difficult to assess. Since they are not required to take the Defense Language Proficiency Test (DLPT) if they are not receiving FLPB, it is often difficult for the G-1/S-1 to identify them as a linguist or for a non-linguist to judge the level of their foreign language capability.

OTHER SERVICE LINGUISTS

B-20. Other service linguists have the advantage of deployability, loyalty, and in most cases a security clearance, but must often learn the Army system and specific Army vocabulary. They are also difficult to obtain since their parent service probably also lacks a sufficient number of trained linguists. Other service linguists, however, will be valuable in joint operation centers and joint activities. When serving a JTF headquarters, Army commanders and staffs must be aware of the linguists in the other services in order to plan for the participation and optimize their employment.

US CONTRACT LINGUISTS

B-21. US civilians can be contracted to provide linguist support. They have an advantage over LN hires in that their loyalty to the US is more readily evaluated, and it is easier for them to be granted the necessary

security clearance. However, there are usually severe limitations on the deployment and use of civilians. A careful assessment of their language ability is important because, in many cases, they use "old fashioned" terms or interject US idioms. If the linguists are recent émigrés, the use of the language in their country of origin could be dangerous to them, or their loyalty may reside with their own country, religious group, tribal affiliations or other close connections when at odds with US interests.

MULTINATIONAL LINGUISTS

B-22. Multinational linguists have their own set of advantages and disadvantages. These linguists may be unfamiliar with the US military system unless they have previously participated in a multinational operation with US forces. They may have a security clearance, but clearances are not necessarily equal or reciprocal, automatically guaranteeing access to classified or sensitive information between nations. They support the command's interest but may have differing priorities or responsibilities within their assigned AOs. These linguists also are already fulfilling specific duties for their own nation, which may also have a shortage of linguists. The major disadvantage to acquiring and maintaining multinational linguist support is that they are outside the military authority of US forces and not under US military contract. These linguists will be valuable in multinational operations centers and activities.

LOCAL NATIONAL CONTRACT LINGUISTS

B-23. LN hires will provide the bulk of linguist support. They are usually less expensive to hire than US civilians and will know the local dialect, idioms, and culture. The expertise of these linguists in particular areas or subject matters can be an asset. However, there are several potential problems with using LN hires, to include limited English skills and loyalty considerations. Therefore, a screening interview or test is necessary to determine their proficiency in English. These individuals also must be carefully selected and screened by CI personnel (with US linguist support) initially and periodically throughout their employment. Their loyalty is always questionable. Local prejudices may influence them, and they may place their own interests above those of the US.

EVALUATING LINGUIST PROFICIENCY

B-24. Commanders and staffs must understand the Army linguist proficiency evaluation system in order to effectively plan for and employ linguists. Evaluation and reevaluation of linguist proficiency is covered in detail in AR 11-6, chapter 5. Language testing is required for all Army personnel in a language-dependent MOS/AOC, who have received foreign language training at government expense, who are receiving FLPB, or who are in a language-required position regardless of MOS/AOC. Other Army personnel who have knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

B-25. The Army uses the DLPT to determine foreign language proficiency levels. DLPTs are listed by foreign language in DA Pam 611-16. In foreign languages where no printed or recorded test exists, oral proficiency interview tests are arranged. The DLPT is an indication of foreign language capability, but it is not the definitive evaluation of an individual's ability to perform linguist support.

B-26. The Army subscribes to the Interagency Language Roundtable's descriptions of the proficiency levels for the skills of speaking, listening, reading, and writing a foreign language, which are available at www.govtilr.org. The plus-level designators, shown as a "+" symbol, are used to designate when a linguist is above a base level, but not yet to the capability of the next level. For example, 2+ would indicate a better than limited working proficiency in the foreign language. The six "base levels" of proficiency, as established by DLPT and/or oral exam, are—

- **Level 0 (No proficiency).** The Soldier has no functional foreign language ability. Level 0+. The minimum standard for Special Forces personnel indicates a memorized proficiency only.
- **Level 1 (Elementary proficiency).** The Soldier has limited control of the foreign language skill area to meet limited practical needs and elementary foreign language requirements.

- **Level 2 (Limited working proficiency).** The linguist is sufficiently skilled to be able to satisfy routine foreign language demands and limited work requirements.
- **Level 3 (General professional proficiency).** The linguist is capable of performing most general, technical, formal, and informal foreign language tasks on a practical, social, and professional level.
- **Level 4 (Advanced professional proficiency).** The linguist is capable of performing advanced professional foreign language tasks fluently and accurately on all levels.
- **Level 5 (Functionally native proficiency).** The linguist is functionally equivalent to an articulate and well-educated native in all foreign language skills; and reflects the cultural standards of the country where the foreign language is natively spoken.

B-27. The above proficiency base levels designate proficiency in any of the four language skills: listening, reading, speaking, and writing. The DLPT only evaluates reading and listening skills. These tests currently do not evaluate linguists above the 3 proficiency level. Oral proficiency interviews evaluate speaking proficiency and also may be used to provide a listening score. These interviews may provide an evaluation all the way up to the 5 proficiency level. Most Army linguist DLPT scores show only two skill levels: listening and reading (for example, 2+/3, or 3/1+). The current Army standard to be considered a qualified linguist is a level 2.

ARMY LANGUAGE PROGRAM CHALLENGES

B-28. Implementation of the Army language program results in several major challenges:

- Acquiring sufficient numbers of linguists in the appropriate languages.
- Anticipating future Army missions and deployments.
- Accurately forecasting the nature and extent of the Army's future linguist needs.
- Defining the special aptitude needed to learn foreign languages.
- The amount of training time required to produce a qualified linguist.
- The high perishability of foreign language skills.
- The constant maintenance required to maintain language skills.
- Linguist retention; foreign languages are a very marketable skill in the civilian sector.
- Army leadership understanding of Linguist issues.

LINGUIST SUPPORT FOR INTELLIGENCE AND INFORMATION COLLECTION

B-29. **Signal Intelligence-Cryptologic Communications Interceptor/Locator 35P:** A cryptologic communications interceptor/locator analyzes and reports information obtained through intercept of foreign language communications. Communications intelligence (COMINT) and monitoring for CI purposes, together with intelligence research and analysis missions, demand highly skilled listening and reading language capability.

B-30. Linguist:

- **Interpreter 09L.** Interpretation is the transfer of meaning from one spoken language into another spoken language. Units may require interpretation capabilities to support commanders in communicating with multinational and threat forces. CA and PSYOP units, law enforcement, medical, logistic, transportation, training, legal, LNOs, and engineer units may also require interpreter support. Most Services do not currently have an interpreter specialty.
- **Translator 09L.** Translation is the rendering by writing of meaning from one written language into another language. Units may require translation of documents to support commanders in communicating with multinational and threat forces. CA and PSYOP units, law enforcement, medical, logistic, transportation, training, legal, LNOs, and engineer units may also require translator support. Most Services do not currently have a pure translator specialty.

B-31. Human Intelligence: HUMINT collectors specifically include enlisted personnel in MOS 97E, WOs in MOS 35M, WOs in MOS 351M and MOS 351Y, commissioned officers in MOS 35E and MOS 35F, select other specially trained MOSs, and their Federal civilian employee and civilian contractor counterparts.

Note. These specially trained and certified individuals are the **only** personnel authorized to conduct HUMINT collection operations.

B-32. HUMINT collection operations that require foreign language capability include the following:

- **Interrogation.** Foreign language requirements for interrogation operations include the ability to read foreign language documents for planning and preparation, and support to DOMEX; and listening and speaking abilities for conduct of the interrogation itself. Even if the interrogation is going to be accomplished using an interpreter, it is beneficial for the interrogator to have proficiency in the target language for more complete understanding, and quality control of the interpreter.
- **Debriefing.** Debriefers require foreign language reading, listening, and speaking capability in order to prepare for an carry out debriefings,
- **Liaison.** HUMINT collectors rely heavily on language ability to conduct effective liaison with host country and some officials.
- **MSO.** All foreign language capabilities are required for effective conduct of MSO.
- **Tactical questioning.** Tactical questioning is expedient initial questioning for information of immediate tactical value. HUMINT collectors involved in tactical questioning require foreign language speaking and listening capabilities.
- **Support to DOMEX.** HUMINT collectors require a foreign language reading ability because may CEDs are associated with detainees and other human sources, and a HUMINT collector is often the first person to screen them. HUMINT collectors will screen the documents associated with human sources and will extract information of use to them in their immediate collection operation.
- **Screening.** HUMINT collectors conducting screening must have a foreign language capability in reading, speaking, and listening.

B-33. **Counterintelligence:** A CI agent is a Soldier in MOS 35L, a WO in MOS 351L, or a commissioned officer in MOS 35E. A CI agent obtains information by direct questioning of a person or persons that may or may not be under the agents' control. Language requirements for CI roles require skill comparable to those being performed by HUMINT specialists. A skilled interpreter can often assist a debriefer. The debriefer skill set is often treated as an ASI, added to either the interrogator or CI specialties.

SUSTAINING MILITARY LINGUIST PROFICIENCY

B-34. Language proficiency is a very perishable skill and diminishes rapidly with lack of use and absence of exposure to the foreign language. In fact, language is quite similar to physical training in that it should be done regularly, if not daily, to maintain capability. Soldiers become a more valuable military asset as they increase their foreign language proficiency. To maintain combat readiness, commanders need to ensure Soldiers have the training time and tools to improve their foreign language skills—as they do for physical training, warrior task training, and other Soldier skills.

B-35. Language labs, on-line foreign newspapers, and foreign radio broadcasts are all examples of language training resources that may be used for this regular training. Additionally, commanders should require all military linguists participate in periodic significant language training events. In-country language immersion training, in-garrison contracted language instructors, and intermediate and advanced language courses taught at the Defense Language Institute Foreign Language Center are some of the

options which can be used to meet this training mandate. Funding for language training is available through language training program funds.

Note. Linguists are a critical resource within the military. Linguists will be employed in MOS-assigned positions or critical linguistic mission tasks and missions and will not be assigned to or employed in duties as drivers, radio operators, or clerks.

B-36. Developments in technology and the Internet now allow Soldiers to use their foreign language as often as they can find time. The following are resources that commanders may use to support their Soldiers' foreign language capabilities:

- In-Country Immersion (Commercial). Several commercial companies provide the opportunity to send Soldiers to countries where the Soldier may attend language courses and live among the local residents. For example:
  - International Center at the University of Utah (www.international.utah.edu).
  - Worldwide Language Resources (www.wwlr.com).
  - National Registration for Language Abroad (NRCSA) (www.nrcsa.com).
- International Standards Organization (ISO)-Immersion. There are commercial and federal programs that provide foreign country environment within CONUS. For example:
  - Language Enrichment Activities Program, the Foreign Language Training Center, Fort Lewis, WA.
  - Global Language Systems, Bountiful, UT (www.glsnet.globtra.com/).
- Joint Language Centers. Each of the regional operation centers of the NSA has a language support organization that provides formal language training opportunities. For example:
  - Fort Gordon, GA (NSA-G).
  - Schofield Barracks, HI (NSA-H).
  - Medina, Lackland Air Force Base, TX (NSA-T).
- Local College or University Language Courses. Check with local universities and colleges for language courses. Some institutions provide the opportunity for custom designed courses for specific language needs.
- Military Language Refresher Programs. All the four military branches conduct language enhancement and language refreshes courses at several locations through the Command Language Program. Many of these programs are conducted in foreign countries as part of the military in-country immersion program.
- Television Programs. Some of the best and more fun ways of learning a foreign language are through movies and television programs. Both foreign and US programs (with foreign subtitle or foreign dubbed) provide the linguist with enjoyable learning environments.
- Computer and Software Language Programs. There are many commercial software programs currently on the market. Rosetta Stone is available to the military through Army Knowledge Online (AKO). For example:
  - Transparent Language (http://www.transparent.com/).
  - Rosetta Stone (www.rosettastone.com).
  - Tell Me More (www.tellmemorestore.com).
- National Security Agency.
- Military Cryptologic Continuing Education Program (MCCEP). The MCCEP was established to provide a structure for the professional development of Cryptologic military language analysts. MCCEP provides career guidance to assist language analysts in broadening and deepening their target knowledge and job abilities. For example:
  - https://www.mccep.org.

- SCOLA. A non-profit educational organization that receives and retransmits television programming from around the world in many languages. These programs are available via Internet to students of language study, ethnic communities, and anyone seeking a global perspective. SCOLA's website is www.SCOLA.org; www.podcastdirectory.com.

- Mobile Training Teams. Contact Defense Language Institute for more information on its mobile training team language courses (http://www.dliflc.edu).
- On-the-Job Training. One of the best, if not the best, methods to help Soldiers increase their language capabilities is through on-the-job training. There are many Federal programs that need linguists. The Reach Language Support Program provides meaningful and challenging translation opportunities to member of the military while providing translation of foreign documents. (rlsp.inbox@us.army.mil). Deployments also provide language proficiency training opportunities.
- Unit Command Language Program. Almost all Army MI battalions have a Command Language Program Manager (CLPM) who supports military linguists in a personal language program development. The CLPM is the best first step in any Army linguist's career.
- Joint Language University. The Joint Language University is a cooperative effort between agencies of the Federal Government, DOD, and Academic institutions (http://jlu.wbtrain.com/).
- Internet. There are several language resources available on the internet. For example:
  - Podcasts (www.itunes.com, http://www.word2word.com/podad.html).
  - Google. A wealth of language opportunities: music, podcasts, videos, programs, and all sorts of great new technology to support foreign language development (www.google.com).
  - Lingnet. An on-line information service, accessible through the Internet or through direct connection, devoted to meeting the needs of the linguist community (http://www.lingnet.org).
  - Langnet. A language learning support system with interactive materials designed for those who want to practice and maintain their target language reading and listening skills (www.langnet.org).
  - Foreign Language Portal. Lists, by foreign language, on the For Official Use Only Army server of foreign language materials (https://www.us.army.mil/suite/doc/5987514).

LANGUAGE TECHNOLOGY

B-37. DOD and the Army have limited human foreign language translation capability to meet requirements. The Sequoyah Foreign Language Translation System mitigates linguistic shortfalls by expanding the number of language translation points of presence to meet the speech and text translation requirements for current and future operations. Sequoyah is a suite of existing and developing language software modules that are integrated, scaleable, tailorable, interoperable, user-friendly, easily deployable, and available at all echelons. Sequoyah meets the foreign language translation requirements when human linguists are unavailable. It includes web-enabled, mobile, and portable configurations.

TERMS

B-38. ***Machine language translation*** is the use of an electronic device to communicate between English and one or more foreign languages.

B-39. A ***Machine Foreign Language Translation System*** is a system used to communicate between English and one or more foreign languages.

B-40. A ***one-way device*** is a device that contains pre-recorded phrases in a desired target language. Phrases are selected that best support a situation and are then played as a recording for the target audience. Methods for selecting and playing a phrase can be touch (using a stylus or buttons) or speech recognition

of a user reciting an English phrase. It is important to note that speech recognition in a one-way device will search for pre-recorded phrases versus actual spontaneous speech translation.

B-41. A ***one-way*** *"**plus**"* or *"**1.5 way**"* device is a machine foreign language translation system that utilizes commonly used pre-recorded phrases combined with speech.

B-42. A ***two-way device*** is a machine foreign language translation system that translates a user's free speech into a desired target language and allows the targeted language to be translated back into English from the intended recipient. This type of device replicates a two-way spoken conversation at the basic level.

CAPABILITIES

B-43. Machine language translation capabilities include simple pre-recorded speech phrase translations (phrase-based), full two-way free speech translations (free form), and text translations. Various systems have different capabilities which the user should fully understand before utilizing the devices.

B-44. There are four modes of machine language translation: speech to speech, speech to text, text to text, and text to speech. Devices may operate in one mode exclusively or in a combination of modes. Speech to text and text to text devices can be used to monitor foreign broadcast media.

B-45. One-way devices can be loaded with a series of relevant questions and/or commands or instructions based on the situation. This will ensure that the same questions or commands or instructions are being used each time. These devices can be used for checkpoint operations, for example, during which a specific sequence of events occurs repetitively for each person or vehicle passing through the checkpoint.

B-46. Some machine language translation devices can record long portions of speech for later translation by an interpreter. For example, anti-coalition mosques in Iraq have disseminated tactical information and anti-coalition messages during operations in the call to prayer. A recording of the call to prayer can later be analyzed for its content.

LIMITATIONS

B-47. All translation devices are limited to the content of their programs. One-way devices depend on the intended recipient acknowledging the pre-programmed phrases with simple yes or no responses or an indication that the recipient understands by their actions.

B-48. Sophisticated two-way devices interpret cultural and linguistic nuances as well as simple word for word translation. Regardless of the accuracy of the device, machines can still only translate words. They cannot include the unspoken social and cultural subtexts that are also a component of any conversation. Additionally, local dialects may dictate the meanings of specific words or phrases which may not be taken into account by the device. Users must always be aware of the possibility of misunderstandings due to improperly translated words, phrases, or concepts.

.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	Human Intelligence Operations Officer
ABCS	Army Battle Command System
ACC	Army component command
ACE	analysis and control element
ACICA	Army Counterintelligence Coordinating Authority
ADCON	administrative control
AFIST	adversarial, foreign intelligence services, and terrorists
AFMIC	Armed forces Medical Intelligence Center
AKO	Army Knowledge Online
AMC	US Army Materiel Command
AO	area of operation
AOC	area of concentration
AOI	area of interest
ARISC	Army Reserve Intelligence Support Center
ARFOR	Army Forces
ASCC	Army Service Component Command
ASCOPE	areas, structures, capabilities, organizations, people, and events
ASI	additional skill identifier
ASPO	Army Space Program Office
ATCAE	Army Technical Control and Analysis Element
ATCICA	Army Theater Counterintelligence Coordinating Authority
BCT	brigade combat team
BDA	battle damage assessment
BFSB	battlefield surveillance brigade
C&E	collection and exploitation
C2	command and control
CA	Civil Affairs
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CCDR	combatant commander
CCIR	commander's critical information requirement
CEE	captured enemy equipment
CEM	captured enemy materiel
CFSO	counterintelligence force protection source operations
CI	counterintelligence
CIA	Central Intelligence Agency

CICA	counterintelligence coordinating authority
CJCMEC	Coalition Joint Captured Material Exploitation Center
CJCS	Chairman of the Joint Chiefs of Staff
CMO	civil-military operations
CNO	computer network operations
CNN	Cable News Network
COA	course of action
COG	center of gravity
COMINT	communications intelligence
COMSEC	communications security
CONOP	contingency operation
CONUS	continental United States
COP	common operational picture
DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DCS	Deputy Chief of Staff
DEA	Drug Enforcement Administration
DH	Defense HUMINT
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIO	Defence Intelligence Organization, Australia
DIS	Defence Intelligence Staff, United Kingdom
DJIOC	Defense Joint Intelligence Operations Center
DLPT	Defense Language Proficiency Test
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOMEX	document and media exploitation
DOS	Department of State
DOT	Department of Transortation
DS	direct support
DSO	defense source operation
DVD	digital video disk
EA	electronic attack
ELINT	electronic intelligence
ES	electronic support
EW	electronic warfare
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FFIR	friendly force information requirement
FISINT	foreign instrumentation signals intelligence

FLPB	foreign language proficiency bonus
FMA	foreign materiel acquisition
FME	foreign materiel exploitation
FMP	Foreign Materiel Program
FMT	foreign materiel training
FP	force protection
G-2	Corps or Division Intelligence Officer
GEOINT	geospatial intelligence
GMI	general military intelligence
GS	general support
GSR	General support-reinforcing
HCT	human intelligence collection team
HN	host nation
HOC	human intelligence operations cell
HPT	high-payoff target
HQ	headquarters
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
HVI	high-value individual
HVT	high-value target
I&W	indications and warnings
ILRT	Interagency Language Round Table
IMINT	imagery intelligence
INR	Bureau of Intelligence and Research (State Department)
INS	Immigration and Naturalization Service
INSCOM	US Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
ISE	intelligence support element
ISR	intelligence, surveillance, and reconnaissance
J-2	Joint Intelligence Officer
JCMEC	Joint Captured Materiel Exploitation Center
JFC	joint force commander
JIDC	Joint Interrogation Debriefing Center
JIIM	joint, interagency, intergovernmental, and multinational
JIOC	Joint Intelligence Operations Center
JISE	Joint Intelligence Support Center
JRIC	Joint Intelligence Reserve Center
JTF	joint task force
LEA	law enforcement agency
LEP	locally employed personnel
LNO	liaison officer

LTIOV	latest time information is of value
MASINT	measurement and signature intelligence
MCCEP	Military Cryptologic Continuing Education Program
MCIA	Marine Corps Intelligence Agency
MCOO	modified combined obstacle overlay
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MI	military intelligence
MIB	military intelligence brigade
MOS	military occupational specialty
MP	military police
MSC	major subordinate command
MSIC	Missile and Space Intelligence Center
MTI	moving target indicator
NAI	named area of interest
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Cener
NGA	National Geospatial-Intelligence Agency
NDHQ	National Defence Headquarters, Canada
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIC	National Intelligence Council
NIST	National Intelligence Support Team
NMIC	National Military Intelligence Agency
NRO	National Reconnaissance Office
NRT	near-real time
NSA	National Security Agency
NSG	National System for Geospatial-Intelligence
NST	National Support Team
OCONUS	outside continental United States
OFCO	offensive counterintelligence operations
OMT	operational management team
ONI	Office of Naval Intelligence
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security

OSC	operations support cell
OSINT	open-source intelligenve
PA	Public Affairs
PAO	Public Affairs Office
PD/DNI	Principal Deputy/Director of National Intelligence
PIO	police intelligence operations
PIR	priority intelligence requirement
PMESII	political, military, economic, social, information, infrastructure
PMESII-PT	political, military, economic, social, information, infrastructure, with the addition of physical environment and time
POC	point of contact
PSYOP	psychological operation
R&D	research and development
RDEC	research, development, and engineering center
REMBASS	Remotely Monitored Battlefield Sensor System
RF	radio frequency
RFI	request for information
ROE	rules of engagement
RSOC	Regional Security Operations Center
RSP	render-safe procedure
RSTA	reconnaissance, surveillance, and target acquisition
RTCAE	regional technical control and analysis element
S-2	Intelligence Officer
S&TI	scientific and technical intelligence
SAEDA	Subversion and Espionage Directed Against the Army
SALUTE	size, activity, location, unit, time, equipment
SAP	special access program
SAR	synthetic aperture radar
SBCT	Stryker Brigade Combat Team
SCI	sensitive compartmented information
SCID	Strategic Counterintelligence Detachment
SCIF	sensitive compartmented information facility
SECDEF	Secretary of Defense
SIGINT	signals intelligence
SIR	specific information requirement
SOFA	Status of Forces Agreement
SOP	standing operating procedure
SQI	special qualification identifier
SSE	sensitive-site exploitation
TACON	tactical control
TCAE	technical control and analysis element

TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities Program
TFCICA	Task Force Counterintelligence Coordinating Authority
THREATCON	threat condition
TOE	table of organization and equipment
TPFDD	time-phased force and deployment data
TSCM	technical surveillance countermeasures
TTP	tactices, techniques, and procedures
URL	uniform resource locator
USACAC	United States Army Combined Arms Center
USAES	United States Engineer School
USAF	United States Air Force
USCENTCOM JIC	United States Central Command Joint Intelligene Center
USCG	United States Coast Guard
USD(I)	Under Secretary of Defense (Intelligence)
USEUCOM JAC	United States European Command Joint Analysis Center
USMC	United States Marine Corps
USJFCOM AIC	United States Joint Forces Command Air Intelligence Center
USNORTHCOM JIC	United States Northern Command Joint Intelligence Center
USPACOM JIC	United States Pacific Command Joint Intelligence Center
USSOCOM JIC	United States Special Operations Command Joint Intelligence Center
USSOUTHCOM JIC	United States Southern Command Joint Intelligence Center
USSPACECOM CIC	United States Space Command Combat Information Center
USSTRATCOM	United States Strategic Command
USTRANSCOM JIC	United States Transportation Command Joint Intelligene Center
V	version
WARNO	warning order
www	world wide web

SECTION II – TERMS

This section to be completed during Final Approved Draft phase.

term
definition.

term
definition.

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

AR 11-6, *Army Foreign language Program,* 14 December 2007

AR 27-60, *Intellectual Property,* 1 June 1993

AR 380-5, *Department of the Army Information Security Program,* 29 September 2000

AR 380-13, *Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations,* 13 September 1974

AR 381-10, *U.S. Army Intelligence Activities,* 3 May 2007

AR 381-20, *(U) US Army Counterintelligence Activities (S),* 15 November 1993

AR 381-172, *Counterintelligence Force Protection Source Operations and Low-Level Source Operations,* 30 December 1994

DOD Directive 3115.09, *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning,* 3 November 2005

FM 2-22.3, *Human Intelligence Collector Operations,* September 2006

FM 2-22.9

FM 2-91.6, *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection,* 10 October 2007

FM 3-0, *Operations,* 27 February 2008

FM 3-05.102, *Army Special Operations Forces Intelligence,* 31 August 2001

FM 3-19.1, *Military Police Operations, Change 1,* 31 January 2002

FM 3-90, *Tactics, 4 July 2001*

FM 5-0, *Army Planning and Orders Production,* 20January 2005

FM 6-0, *Mission Command: Command and Control of Army Forces,* 11 August 2003

FMI 2-01, *Intelligence, Surveillance, and Reconnaissance Synchronization* (at CADD)

FMI 2-22.9, *Open-Source Intelligence,* with Change 1 dated 7 May 2008

FMI 5-01.1, *The Operations Process,* 16 March 2008

TC 2-22.303, *The 2X Handbook,* 31 July 2006

DIAM 58-11, *DOD HUMINT Policies and Procedures (S)*

DIAM 58-12, *The DOD HUMINT Management System (S)*

CJCS Instruction 1301.01, *Policy and Procedures to Assign Individuals to Meet Combatant Command Mission-Related Temporary Duty Requirements,* 1 July 2001

CJCS Instruction 5120.02A, *Joint Doctrine Development System,* 31 March 2007

CJCSM 3500.04C, *Universal Joint Task List (UJTL),* 1 July 2002

NGA Publication 1-0

JOINT PUBLICATIONS

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

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

JP 3-0, *Joint Operations, with Change 1,* 13 February 2008

JP 3-33, *Joint Task Force Headquarters,* 16 February 2007
JP 5-0, *Joint Operation Planning,* 26 December 2006
JP 5-00.2, *Joint Task Force Planning Guidance and Procedures,* 13 January 1999

DOCUMENTS NEEDED

These Documents must be available to the intended users of this publication.

DA Form 2028, Recommended Changes to Publications and Blank Forms

READINGS RECOMMENDED

These sources contain relevant supplemental information.

AR 350-1, *Army Training and Education,* 9 April 2003
AR 380-5, *Department of the Army Information Security Program,* September 2000
AR 380-10, *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives,* 15 February 2001
AR 380-15. *(C) Safeguarding NATO Classified Information,* 1 March 1984
AR 380-28, Department of the Army Special Security System, 12 December 1991
AR 380-40, *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material,* 22 October 1990
AR 380-49, *Industrial Security,* 15 April 1982
AR 380-53, *Telecommunications Security Monitoring,* 29 April 1998
AR 380-67, *Personnel Security Program,* 9 September 1988
AR 381-1, *Security Controls on Dissemination of Intelligence Information,* 12 February 1990
AR 381-12, *Subversion and Espionage Directed Against the US Army (SAEDA),* 15 January 1993
AR 381-14, *Technical Counterintelligence (TCI),* 30 September 2002
AR 381-45, *Investigative Records Repository,* 25 August 1989
AR 381-47, *(U) US Army Offensive Counterespionage Activities (S),* 30 July 1990
AR 381-100, *(U) Army Human Intelligence Collection Program (S),* 15 May 1988
AR 381-102, *(U) US Army Cover Support Program (S),* 10 January 1991
AR 381-143, *Military Intelligence Nonstandard Material Policies and Procedures,* 1 December 1986
AR 614-115, *Military Intelligence Excepted Career Program,* 12 April 2004
AR 614-200, *Military Intelligence Civilian Excepted Career Program,* 30 September 2004
DA Pam 381-15, *Foreign Military Intelligence Collection Activities Program,* 1 June 1988
DA Pam 611-16, *Handbook of Army Personnel Test,* 1 April 1985
Executive Order 12333, *United States Intelligence Activities,* 4 December 1981
DOD Directive 2310.1, *DOD Program for Enemy Prisoners of War (EPOW) and Detainees (Short Title: DOD Enemy POW Detainee Program),* 18 August 1994
DOD Directive 2310.1E, *The Department of Defense Detainee Program,* 5 September 2006
DOD Directive 5100.20, *The National Security Agency and the Central Security Service,* 23 December 1971
DOD Directive 5100.77, *DOD Law of War Program,* 9 December 1998
DOD Directive 5240.1, *DOD Intelligence Activities,* 3 December 1982
DOD Regulation 5240.0-R, *Procedures Governing the Activities of DOD Intelligence Component That Affect United States Persons,* December 1982
FM 27-10, *The Law of Land Warfare,* July 1956
NGA GEOINT Basic Document Publication 1, September 2006
Title 32, *United States Code* (available online)
Further information and links to many of the above publications can be found at: http://www.dami.army.pentagon.mil/offices/dami-cd/

ARTEPS, MTPs and other intelligence training products are available at the Reimer Digital Library http://www.adtdl.army.mil

DOCUMENTS TO BE PUBLISHED

FM 2-01.3, *Intelligence Preparation of the Battlefield*
FM 2-01.301, *Tactics, Techniques, and Procedures of Intelligence Preparation of the Battlefield*
FM 2-22.2, *Counterintelligence*
FM 2-22.4, *Technical Intelligence*
FM 7-15, *The Army Universal Task List*
FM 2-33.4, *Intelligence Analysis*
FMI 2-91.501, *Intelligence Support to Civil Support Operations*
TC 2-22.201, *Counterintelligence Operations and Collection Activities (S//NF,*
TC 2-22.302, *Controlled Military Source Operations (S//NF)*
TC 2-22.101, *Biometric Enabled Intelligence*

7052

Index

W