# MILITARY INTELLIGENCE PUBLICATION 2-0.1 INTELLIGENCE REFERENCE GUIDE


Fort Huachuca
Arizona
"from sabers to satellites..."

## JUNE 2010

**DISTRIBUTION RESTRICTION:** Distribution authorized to U.S. Government agencies and their contractors only because it requires protection in accordance with AR 380-5 and as specified by DCS G-3 Message DTG 091913Z Mar 04. This determination was made on 4 June 2010. Other requests for this document must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ 85613-7017, or via e-mail at ATZS-FDC-D@conus.army.mil.

**DESTRUCTION NOTICE:** Destroy by any method that will prevent disclosure of contents or reconstruction of the document in accordance with AR 380-5.

# Foreword

Currently, the intelligence warfighting function includes a formidable set of capabilities across all echelons from "mud-to-space." This flexible force of personnel, organizations, and equipment collectively provides commanders with the timely, relevant, accurate, predictive, and tailored intelligence they need. We provide the intelligence that continuously supports the commander in visualizing the operational environment, assessing the situation, and directing military actions through ISR synchronization and the other intelligence tasks.

The intelligence warfighting function is comprised of nine powerful intelligence disciplines. Eight of those disciplines essentially feed the discipline of all-source intelligence which in turn is focused on the commanders' requirements. Technological advances have enabled single-discipline analysts to leverage other analysts and information and to conduct multi-discipline analysis to an extent not possible in the past. However, all-source intelligence is still the nexus that integrates information and intelligence from all units and the other intelligence disciplines.

Future operational environments will be greatly impacted by globalization. "Globalization and growing economic interdependence, while creating new levels of wealth and opportunity, also creates a web of interrelated vulnerabilities and spreads risk even further, increasing sensitivity to crises and shocks around the globe and generating more uncertainty regarding their speed and effect" according to the National Defense Strategy, June 2008.

Key aspects of globalization include—

- Non-state groups, organized crime, and cultural and environmental change will stress already fragile social and political structures.
- American science and technology (S&T) communities, both commercial and Department of Defense (DOD), will compete with some growing economies for technical advantage.
- By 2020, organized crime is likely to thrive in resource-rich states now experiencing political and economic transformation.
- By 2025, urban growth will concentrate in coastal areas. The majority of urban populations will live within 60 miles of coastlines.
- By 2030, the world's urban population will be over 4.9 billion fostering—
    - Interdependent economies.
    - The interaction of differing societies and cultures.
    - More powerful non-state actors.
    - Porous international boundaries.
    - The inability of some nation-states to fully control their territory, economy, and to provide security and services.
- By 2030, competition for access to and control of natural resources (energy, water, and food) will dramatically increase areas of potential conflict.
- " … Cyber security risks pose some of the most serious economic and national security challenges of the 21st Century" according to the Presidential Cyberspace Policy Review, May 2009.

The Joint Operational Environment 2010 observes that, "With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains."

In future operational environments as U.S. forces conduct increasingly complex operations Army intelligence will continue to prove even more critical by providing Army warfighting commanders

with predictive, knowledge-based intelligence. As stated in the National Intelligence Strategy, August 2009, the Intelligence Community (IC) must ***"Operate as a single integrated team, employing collaborative teams that leverage the full range of IC capabilities*** to meet the requirements of our users, from the President to deployed tactical military units."

Some current conceptual documents postulate that future operations will be significantly different from past operations in which intelligence was merely viewed as a supporting operation. Today, and in the future, intelligence must not only drive operations but precisely drive operations. Therefore, Army intelligence must be prepared to:

- Operate in complex and urban terrain among the local population. This task requires a combination of existing and new technical means and expanded collection capabilities to exploit previously unexploited signatures.
- Develop a new MI mindset and culture that includes expanded capabilities to conduct political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) collection, analysis, and reporting. This includes the realization that understanding the dynamics of the local population and culture in stability operations can often be as important as maneuver against and targeting of threat cells and organizations. Most operations in the future will continue to center on people, requiring an intelligence force with a firm grasp of the operational variables and civil considerations.
- Develop more detailed and precise intelligence and knowledge against networks and individuals to achieve unparalleled operational success. This requires a flexible intelligence structure armed with the many necessary skill sets and prepared to task organize as required (thus more agile).
- Proactively, rather than reactively, integrate new technology—for example, communications, information processing, sensing, and hand held devices—and effectively tap into global data and information stores. This will assist Army intelligence in efficiently synchronizing the enterprise and managing the vast amounts of classified intelligence and open-source information (which is still growing exponentially). The endstate is to build an overarching federated and networked analytical enterprise.

The challenge we must meet is to develop agile, innovative, critically thinking, and culturally aware Military Intelligence (MI) Soldiers, leaders, and civilians for this future operational environment. These professionals must possess a balance of interpersonal skills and technical competence necessary for an effective military team. Our future success relies upon methodical yet creative and adaptable MI Soldiers and leaders that are not risk-adverse and can find a way to meet the commander's requirements.

To this end we developed this reference guide as a tool for the MI professional. I am confident that the intelligence warfighting function and MI Corps are up to these challenges and we will continue to make very significant contributions to our Army.

***Always Out Front!***

**JOHN M. CUSTER**
**Major General, U.S. Army**
**Commanding**

# MI Publication 2-0.1

## Contents







FOR OFFICIAL USE ONLY

Table of Contents

Table of Contents



FOR OFFICIAL USE ONLY

## Figures

## Tables

# Preface

Military Intelligence Publication 2-0.1 (MI Pub 2-0.1), Intelligence Reference Guide, is an unclassified for official use only (FOUO) resource that captures information relevant to the environments the Army and Army Intelligence are currently experiencing. It is a helpful resource for commanders, intelligence and operations staff officers, warrant officers, NCOs, and analysts at all skill levels and echelons. MI Pub 2-0.1 comprises six chapters that address current topics of value to a full understanding of the field of military intelligence fundamentals, disciplines, operations, training, and systems. Specifics of particular interest or importance are expanded in 13 appendices, including one on cyberspace operations and another one on telecommunications and signal fundamentals.

The proponent of this publication is the United States Army Intelligence Center of Excellence (USAICoE). The views expressed herein are those of the authors and compilers and not of the U.S. Army Training and Doctrine Command. The contents of MI Pub 2-0.1 were provided by program managers responsible for particular systems and subject matter experts proficient in their particular areas.

Any actions taken related to this publication must be in compliance with AR 381-10.

# Chapter 1
# Military Intelligence Modernization

## INTRODUCTION

**1-1.** A campaign-capable expeditionary force is vital to meeting the demands of an environment of persistent conflict. In the near future, the Army will conduct continuous operations in this environment. The Army is modernizing by converting to a modular force and through Army force generation (ARFORGEN). Military intelligence (MI) is modernizing by—

- Increasing MI capacity and skills balance.
- Revitalizing Army human intelligence (HUMINT) capabilities.
- Giving brigade combat teams (BCTs) and battalion-level access to "flat," all-source information networks.
- Improving MI wartime readiness.

## MODULARITY

**1-2.** Modular force conversion, part of the Army's overall modernization effort, reorganizes the Army into modular theater armies, theater support structures, corps and division headquarters, BCTs, and multifunctional and functional support brigades. This is based on standardized organizational designs for both the Regular Army and Reserve Components (Army National Guard and Army Reserve). The process includes changes in almost all aspects of the Army.

**1-3.** MI plays an important role in the modernization of the Army. Modernization changes MI as well, changing the way it is organized to meet the challenges of responding rapidly to current operations.

**1-4.** A key aspect of Army modernization is the shift from division-based to brigade-based organizations. The smaller, modular units are more mobile than division-centered brigades. They are quicker to respond to the needs of joint force commanders. More Soldiers are available at the tactical level, closer to the fight. Connectivity and reachback are more essential than before..

### A Brigade-Based Modular Force

**1-5.** The conversion to a brigade-based modular force is an intellectual approach to force design and is driving a cultural shift in the Army—a key factor in moving to a campaign-capable expeditionary force. Modularity is more than just another organizational change, it is the Army's major force modernization initiative. It involves the redesign of all components of the operational Army into a larger, more powerful, more flexible, and more rapidly deployable force.

### Modularity Equals Growth in Military Intelligence

**1-6.** As the Army transforms into modular brigade-based units, the need for MI Soldiers increases. Besides growing the analyst and collection capability at the brigade staff level, the BCT includes an organic MI company. Divisions are supported by battlefield surveillance brigades (BFSBs). These consolidate capabilities that can be pushed down to the BCT level. The number of MI Soldiers at the BCT level has increased by almost 18 percent compared to the previous design.

**1-7.** Modular units are interchangeable and tailorable organizations. They provide joint force





FOR OFFICIAL USE ONLY

commanders with a strategically responsive force. Modular units improve the capability to deploy quickly to harsh operational environments and defeat a threat. Modular units incorporate capabilities that were previously held at higher headquarters, including support, thus enabling the modular formation to act more autonomously when required. With a modular, brigade-based structure, Army forces—

- Are more responsive to geographic combatant commanders.
- Employ better joint capabilities.
- Facilitate force packaging and rapid deployment.
- Are more capable of independent action than previous organizations.

**1-8.** By using modular units as building blocks, joint force commanders can tailor their forces to changing situations. Over time, commanders can draw from larger force pools available for rotation. Modular units are designed to integrate seamlessly into other Army and joint force units, employing innovative technologies and operational methods. Under the previous design, when a brigade was assigned a mission, it task-organized using other division resources, such as artillery and engineers, to create an ad hoc BCT. Modularity significantly changes that approach by creating standing combined arms BCTs (see FM 3-0, appendix C) containing the capabilities necessary to deploy to a fight—in effect, organizing as they intend to fight. The change includes adding access to joint capabilities at much lower levels with more robust network capabilities, more joint and specialized personnel, and enhanced training and leader development. Creating standing combined arms BCTs that contain the capabilities necessary to deploy to a crisis means these brigades reduce the peace-to-war transition time.

## Redesign

**1-9.** Redesign centers on the BCT. This unit, a stand-alone and standardized tactical force of 3,500 to 4,000 Soldiers, is organized to reflect the way it fights. There are three types of BCTs: heavy, infantry and Stryker. (See figure 1-1, 1-2, and 1-3.)

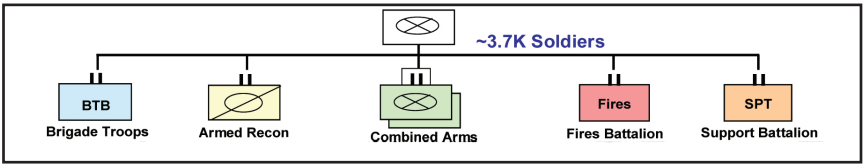



**Figure 1-1. Heavy brigade—two armor-mechanized infantry battalions and an armed reconnaissance battalion**

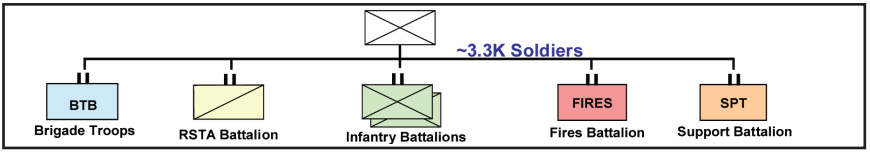



**Figure 1-2. Infantry brigade—two infantry battalions and a reconnaissance and surveillance battalion**

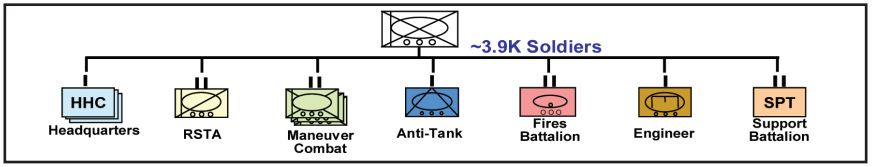



**Figure 1-3. Stryker brigade—three Stryker battalions and a reconnaissance and surveillance battalion**





FOR OFFICIAL USE ONLY

## ARMY FORCE GENERATION

**1-10.** In the era of persistent conflict, combatant commanders and civil authorities need a constant supply of trained and combat-ready land forces. By late 2003, the Army recognized the challenge of providing forces to meet the increased demand. ARFORGEN is the process the Army developed to provide ready forces from across the Army—the Regular Army and Reserve Components—to meet the elevated and sustained level of combatant commanders' requirements.

**1-11.** Intelligence support to force generation is one of the four tasks included in the intelligence warfighting function. Generating knowledge begins in the reset phase of the ARFORGEN cycle and continues throughout the unit's deployment timeline. (See chapter 5.) It requires that units be connected to the Global Information Grid, even in peacetime operations, to mine data and build data files for contingency-based threats, terrain and weather, and civil considerations.

**1-12.** The ARFORGEN three-phase cycle is a structured progression that increases unit readiness over time. The result of the process is predictability for Soldiers and the Army. ARFORGEN provides trained, ready, and cohesive units that meet the requirements of combatant commanders and the Army. The Army uses the ARFORGEN process to allocate resources—equipment, personnel, and training opportunities.

**1-13.** ARFORGEN enhances the Army's ability to maintain an all-volunteer force while deploying units on extended-duration missions. ARFORGEN sustains the all-volunteer force in two ways:

- ARFORGEN provides Soldiers with programmed periods of rest during the reset phase. These periods are needed for Soldiers to maintain relationships with their families, promote physical and mental welfare, and sustain relationships with employers.
- ARFORGEN's reset phase provides Soldiers with the opportunity to participate in professional education opportunities and refurbish their equipment.

**1-14.** Following the reset phase, units transition to the train/ready phase. During this phase, units receive personnel, new equipment, and full spectrum operations (FSO) mission essential task lists (METLs) for the assigned mission. Units develop an FSO METL collective training plan that culminates with a mission rehearsal exercise. Upon certification, units move to the available force pool to support domestic missions or operational deployments. Currently that period may vary, but is usually 12 months. (See figure 1-4.)

**1-15.** In response to ongoing persistent conflict challenges, the Army refined the ARFORGEN process to more effectively account for continuous unit and leader feedback. This continuous feedback occurs during monthly and quarterly training support and resourcing conferences. These conferences focus on verifying the synchronization of unit training timelines with the required resourcing.





FOR OFFICIAL USE ONLY

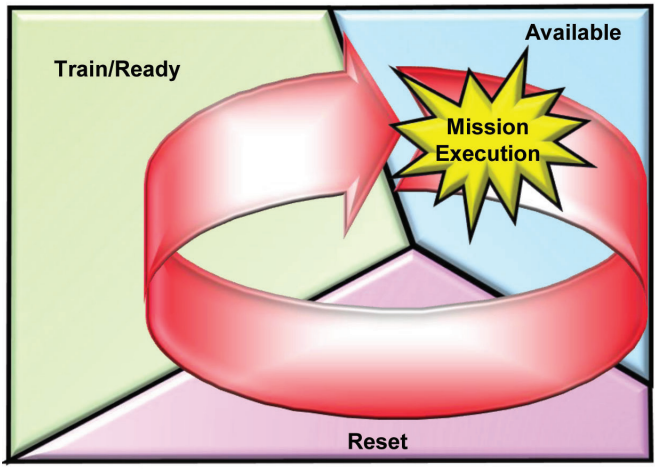



**Figure 1-4. ARFORGEN cycle**

## INTELLIGENCE MODERNIZATION

**1-16.** Combat lessons learned from recent military operations have highlighted the need for increased MI capabilities within BCTs and maneuver battalions. The Army has incorporated hard-won field experience into modular design. This modular design shifts the warfighting focus from division-level to BCT-level operations and equips Soldiers for the fight. MI modernization focuses on four critical areas:

- Increasing MI capacity and skills balance.
- Revitalizing Army HUMINT capabilities.
- Enabling BCT and battalion-level access to flat, all-source information networks.
- Improving MI wartime readiness.

**1-17.** Modular BCTs and battalions perform a broad range of continuous collection and analytical tasks to ensure mission completion. The modular MI structure addresses the increase in responsibility by more than doubling the size of the maneuver battalion S-2 sections and tripling the size of the BCT S-2 sections. Due to the expansion of the brigade and battalion S-2 sections, the expansion of BCT organic MI companies increases capabilities in HUMINT, signals intelligence (SIGINT), unmanned aircraft systems, and analysis.

**1-18.** Battlefield experience shows that BCTs also require additional intelligence support at lower echelons. To accomplish this, the Army is forming MI collection battalions weighted toward HUMINT and interrogator capabilities. These battalions form the core of the new BFSBs. To better support joint interrogation operations at the joint task force level, the Army is also building four joint interrogation and debriefing center battalions to provide strong, expert interrogation capabilities in close coordination with military police detention forces.

**1-19.** Expansion of the Army's HUMINT capability is another important component of MI modernization. HUMINT is especially critical in irregular warfare and stability operations where understanding the human dimension is essential to achieving operational success. Beyond force structure, Army HUMINT modernization is enhancing the training and employment of the HUMINT force at all levels. Increasing Army MI capacity and HUMINT capability are essential but insufficient





FOR OFFICIAL USE ONLY

unless MI Soldiers at all levels are provided access to all sources of information across all classification levels. In addition to such Internet-based tools as Intelligence Knowledge Network (IKN) and MI Space, MI Soldiers also use advanced software tools to rapidly search, visualize, and analyze large quantities of data. Presently, the Army is delivering that capability through accelerated development and fielding of Distributed Common Ground System-Army (DCGS-A) workstations and network access at the battalion level. (See appendix E.)

**1-20.** The flat DCGS-A network gives Soldiers access to more than 200 data sources. It enables—

- Rapid collaboration through shared access to data, regardless of type or classification.
- Rapid mining, fusing, and visualization of data for better understanding.
- Speedy reachback support to forward-deployed analysts from Army Intelligence and Security Command (INSCOM), theater, and national agencies.

**1-21.** DCGS-A access enables MI Soldiers to stay apprised of the threat after returning from combat and performing tactical overwatch to directly support deployed units.

**1-22.** Improved Army intelligence readiness requires that Soldiers be equipped for the asymmetric fight through expansion of continuous, focused intelligence, surveillance, and reconnaissance (ISR) capabilities and by improved training across the MI force. The Army is expanding surveillance capabilities through both manned and unmanned systems. Together these systems, described in appendix I, provide dedicated, downward-focused, and responsive surveillance and targeting capability to warfighting units. The Army is transforming intelligence training through programs, such as the Foundry Program, cultural awareness, and language training. (See chapter 5.)

**1-23.** Modernization demands that the Army train adaptive leaders, sustain readiness, and continue to provide actionable intelligence in an era of persistent conflict. Army G-2, INSCOM, the U.S. Army Intelligence Center of Excellence (USAICoE), and the Military Intelligence Readiness Command (MIRC) focus on MI modernization across the Army:

- Army G-2 provides strategic direction and resources.
- INSCOM performs worldwide missions across all intelligence disciplines to support Army component commanders and forces.
- USAICoE provides foundational training, doctrine, and combat development to prepare leaders and Soldiers for operations.
- MIRC provides trained and ready Soldiers, mission-tailored teams and units, and state-of-the-art intelligence production and training facilities.

## INTELLIGENCE DRIVES OPERATIONS

**1-24.** Intelligence supports commanders and staffs in visualizing the operational environment. Visualization includes more than having knowledge of the physical and manmade characteristics of the area of operations (AO). It requires knowing the current dispositions and activities of the threat forces in that space as well as their current and future capabilities. More importantly, visualization requires commanders and staffs to understand the objectives of the threat forces.

**1-25.** Determining the intent of threat leaders is a significant challenge confronting the intelligence staff. The key factor that makes determining intent so difficult is the process of action and reaction that occurs between a force and its threat. Friendly actions or even preparations, if detected, cause a reaction by the threat. Estimating the outcome of these actions and reactions requires the intelligence staff to know what future friendly actions are planned and to plan multiple courses of action.

**1-26.** During peacetime operations, intelligence helps commanders make acquisition choices, protect technological advances, shape organizations, and design training to ready the force. Intelligence





FOR OFFICIAL USE ONLY

assets monitor foreign states and volatile regions to identify threats to U.S. interests in time for the President and Secretary of Defense to respond effectively, efficiently, and in a manner consistent with U.S. policy. Information shortfalls are identified and eliminated. Intelligence units are employed or deployed as early as directed to support U.S. initiatives and to assist multinational forces.

**1-27.** Intelligence supports commanders as they decide which forces to deploy; when, and where to deploy them; and how to employ them in a manner that accomplishes the mission at the lowest human and political cost. Although supporting the effort to reduce or eliminate sources of conflict, peacetime intelligence constantly prepares for escalation to war.

**1-28.** During wartime, intelligence—

- Informs commanders of the threat's information capabilities, and where and when to exploit intelligence gaps.
- Tells commanders of the threat's centers of gravity and helps the operational planner identify the best means for attacking or exploiting them.
- Enables commanders to focus and leverage combat power and determine acceptable risk.
- Is the key to allowing commanders to achieve powerful, dynamic concentrations of forces. In wartime, it is important that support be anticipatory and precise.
- Maximizes and synchronizes support to commanders while minimizing demands made on commanders and staffs.

## CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

**1-29.** Intelligence effectiveness is measured against the following quality criteria (see FM 2-0):

- **Accuracy.** Intelligence gives commanders an accurate, balanced, complete, and objective picture of the enemy and other aspects of the AO. To the extent possible, intelligence accurately identifies threat intentions, capabilities, limitations, and dispositions. It is derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments are presented, when necessary, to ensure balance and bias-free intelligence.
- **Timeliness.** Intelligence is provided early to support operations and prevent surprise from enemy action. Intelligence flows continuously to commanders before, during, and after an operation. Intelligence organizations, databases, and products are available to develop estimates, make decisions, and plan operations.
- **Usability.** Intelligence is presented in a form that is easily understood, or is displayed in a format that immediately conveys the meaning to the consumer.
- **Completeness.** Intelligence briefings and products convey all the components necessary to be as complete as possible. Completeness is frequently driven by time constraints—the 60 percent answer now may be more useful than the 90 percent answer that comes too late.
- **Precision.** Intelligence briefings and products provide only the required level of detail and complexity to answer the requirements.
- **Reliability.** Intelligence is evaluated to determine the extent to which collected information that is being used in intelligence briefings and products is trustworthy, uncorrupted, and undistorted. Concerns about reliability issues are stated up front.

**1-30.** Effective intelligence meets three additional criteria:

- **Relevant.** Intelligence supports commanders' concept of operations. It is relevant to the capabilities of the units, commanders' information requirements, and commanders' preferences.
- **Predictive.** Intelligence informs commanders about what the threat can do and what the threat is most likely to do. Intelligence staff anticipate commanders' intelligence needs.
- **Tailored.** Intelligence is presented—based on the needs of the commanders, subordinate





FOR OFFICIAL USE ONLY

commanders, and staff—in a specific format that is clear and concise so they can understand it, believe it, and act on it. It supports and satisfies commanders' priorities.

## ACTIONABLE INTELLIGENCE

**1-31.** Actionable intelligence is an example of bringing the characteristics of effective intelligence together with the effective integration of intelligence into ongoing operations. JP 2-0 discusses the concept of critical intelligence. Army personnel have used the concept of actionable intelligence to reflect the joint concept of critical intelligence. In current operations, the concept of actionable intelligence is used by Army personnel to describe information that answers operational requirements. Army personnel also use it to describe specific commanders' guidance to a sufficient degree and with sufficient reliability to support commanders' targeting decisions.

**1-32.** Analysts face the challenge of processing ever-increasing amounts of information with limited resources until a solution to the conundrum is found—either increasing the number of analysts or improving the sophistication of automation.

**1-33.** Ideally, the staff thoroughly integrates intelligence into the operations process to ensure the collection and reporting of accurate, timely, useful, complete, precise, reliable, relevant, predictive, and tailored information and intelligence. This integration is accomplished by integrating the characteristics of effective intelligence with successful ISR operations and ISR synchronization. When that is done, commanders can fight the threat based on knowledge rather than assumptions. (See FM 2-0.)





FOR OFFICIAL USE ONLY

# Chapter 2

# Intelligence Fundamentals

## INTRODUCTION

**2-1.** This chapter discusses the fundamentals of intelligence, the intelligence enterprise, and the intelligence warfighting function. It also gives an overview of the intelligence disciplines and discusses the intelligence community.

## BASICS

**2-2.** *Intelligence* is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity (JP 2-0). Intelligence provides commanders and their staffs with predictive and tailored information supporting the commander's decisionmaking.

**2-3.** The intelligence officer is the commander's primary advisor on all matters relating to intelligence. This includes the intelligence enterprise, the intelligence warfighting function, intelligence support to planning, intelligence support to operations, and the intelligence disciplines. The intelligence sections at each echelon assist in planning operations; synchronizing intelligence, surveillance, and reconnaissance (ISR); and developing intelligence products.

**2-4.** The Army's operational concept requires a firm focus on the enemy. It stresses taking action, avoiding enemy strengths, and exploiting critical vulnerabilities of the enemy. Identification of these strengths and vulnerabilities is crucial. Operations also require decisions and actions based on situational awareness—an understanding of the essential factors that make each condition unique—rather than on preconceived schemes or techniques. Accurate and timely intelligence—knowledge of the enemy and the surrounding environment—can provide this situational awareness. Situational awareness is a prerequisite for the Army's success in war. Intelligence contributes to the exercise of effective command during military operations and helps ensure the successful conduct of those operations.

**2-5.** Because intelligence deals with many unknowns—questions about an unfamiliar area and enemies who actively try to conceal information about their forces and intentions—there will almost always be intelligence gaps. The knowledge provided will lack the desired degree of detail and reliability. Intelligence cannot provide absolute certainty. Instead, it attempts to reduce the uncertainty facing commanders to a reasonable level by collecting relevant information, placing it in context to provide knowledge, and conveying it in a manner to enhance understanding. Furthermore, intelligence possesses both positive—or exploitative—and protective elements. It uncovers conditions that can be exploited and simultaneously provides warning of enemy actions. Intelligence provides the basis for a commander's actions supporting full spectrum operations (offensive, defensive, and stability or civil support operations).

**2-6.** Intelligence is not simply another word for information. It is more than an element of data or a grouping of information. Instead, intelligence is a body of knowledge needed to support decisionmaking. The intelligence fundamentals support decisionmaking. These fundamentals are—

- Maintain relevant knowledge about—





FOR OFFICIAL USE ONLY

- Potential threats.
- The surrounding environment.
- Civil considerations.

- Acquire the required data.
- Analyze and present new intelligence to the commander.

## Maintain Relevant Knowledge

**2-7.** Maintaining relevant knowledge about potential threats, the surrounding environment, and civil considerations includes all of the intelligence activities conducted to develop understanding of the operational environment used to support military planning. This includes—

- Intelligence preparation of the battlefield (IPB).
- ISR synchronization and intelligence support to ISR integration.
- Intelligence reach.

### Intelligence Preparation of the Battlefield

**2-8.** Planning military operations requires the intelligence officer and staff to create and refine a series of products that provide commanders and staffs an understanding of the threat and relevant aspects of the area of operations (AO). *Intelligence preparation of the battlefield* is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain and weather, and civil considerations in a specific area of interest and for a specific mission. By applying IPB, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space (FM 2-01.3). IPB—

- Is a continuous planning activity, undertaken by the entire staff.
- Is designed to support the running estimate and military decisionmaking process (MDMP).
- Is designed to build an extensive database for each potential area where a unit may be required to operate.
- Allows commanders and staffs to gain the information needed to selectively apply and maximize combat power at critical points in time and space.
- Is most effective when it integrates each staff element's expertise into the process.
- Is, along with analysis, the driver of ISR activity.

**2-9.** The database is analyzed to determine the impact of the enemy, terrain and weather, and civil considerations on operations and is presented in graphic form. The Army uses the mission variables of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) as the framework for the analysis. (See FM 2-01.3 for additional information on IPB.)



### Intelligence, Surveillance, and Reconnaissance Synchronization

**2-10.** ISR synchronization accomplishes the following:

- Analyzes information requirements and intelligence gaps.
- Evaluates available assets, both internal and external.
- Determines gaps in the use of those assets.
- Recommends ISR assets controlled by the organization to collect on commander's critical information requirements (CCIRs).
- Submits requests for information (RFIs) for adjacent and higher collection support.

**2-11.** It is crucial that all commanders and staff sections participate in ISR planning—from the identification of information requirements, through the collection and reporting of information to answer the CCIRs, to the assessment of ISR and the updating of ISR plans.
The following characteristics describe successful ISR operations:

- Focus on CCIRs.



FOR OFFICIAL USE ONLY

- Operate continuously.
- Facilitate commanders' visualization and decisionmaking.
- Facilitate the application of combat power.
- Focus on the AO.

**2-12.** ISR centers on the commander's information requirements. The ISR synchronization matrix serves as the baseline for ISR operations and as a guide for preparation of the ISR plan. The staff develops and monitors the ISR tasking matrixes, with input from the commander and other staff members. Operations officers develop the ISR plan. Commanders implement it. The ISR plan must be synchronized with current and future operations. The ISR plan must provide for the rapid shifting and diversion of resources as the situation develops or alters, or as tasks and requirements are satisfied.

### Intelligence Reach

**2-13.** Intelligence reach is a process. The process allows intelligence organizations to proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies—both within and outside the theater of operations. This support and sharing is unconstrained by geographic proximity, echelon, or command. Intelligence obtained through intelligence reach helps planning and preparation for operations. It may provide additional information used in answering CCIRs.

**2-14.** Intelligence reach entails using existing automated information systems, such as the Distributed Common Ground System-Army (DCGS-A), while connected to the Global Information Grid (GIG). (For additional information on DCGS-A, see appendix E.) Intelligence reach includes establishing and providing access to—

- Classified and unclassified programs.
- Databases, networks, systems.
- Other Web-based collaborative environments for—
    - Army forces.
    - Joint forces.
    - National agencies.
    - Multinational organizations.

**2-15.** Intelligence reach facilitates intelligence reporting, production, dissemination, and a multilevel collaborative information environment.

## Acquire the Required Data

**2-16.** Acquire the required data includes all of the intelligence collection activities undertaken to collect information required by commanders and staffs as they accomplish assigned missions. Executive Order 12333 (EO 12333) states that Army intelligence and counterintelligence (CI) shall "collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and CI to support departmental requirements, and, as appropriate, national requirements."

**2-17.** Recent operations show a greater need for persistent surveillance. Persistent surveillance is 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 retargeting in near or real-time. (JP 2-0).

## Analyze and Present New Intelligence to the Commanders

**2-18.** Analyze and present new intelligence to commanders is the activity where information becomes intelligence through processing, exploitation, and analysis. Processing the incoming information





FOR OFFICIAL USE ONLY

involves the intelligence architecture, systems, data management, and the flow of information within the intelligence enterprise. Exploitation is the process of taking the collected data and putting it into a form usable by the analyst.

**2-19.** Analyzing and putting the information into context are goals of all analysts. Achieving these goals requires intelligence analysts to understand capabilities and limitations of intelligence collection assets and reporting. Using multiple sources during intelligence analysis reduces uncertainty and helps solve problems that could not be resolved via a single source.

**2-20.** The analysis process requires critical thinking. The intent behind critical thinking is to increase intelligence accuracy via a thorough and organized process. (See chapter 4.)

**2-21.** The ability to communicate effectively to decisionmakers transforms intelligence into action. This requires an understanding of the way rapidly unfolding events relate to local culture or history and how these events will impact the unit's mission. Understanding the larger picture is essential to focusing the intelligence effort on the commander's priorities while identifying emerging threats in a dynamic operational environment. (For additional information on intelligence analysis, see TC 2-33.4.)

## THE ARMY INTELLIGENCE ENTERPRISE

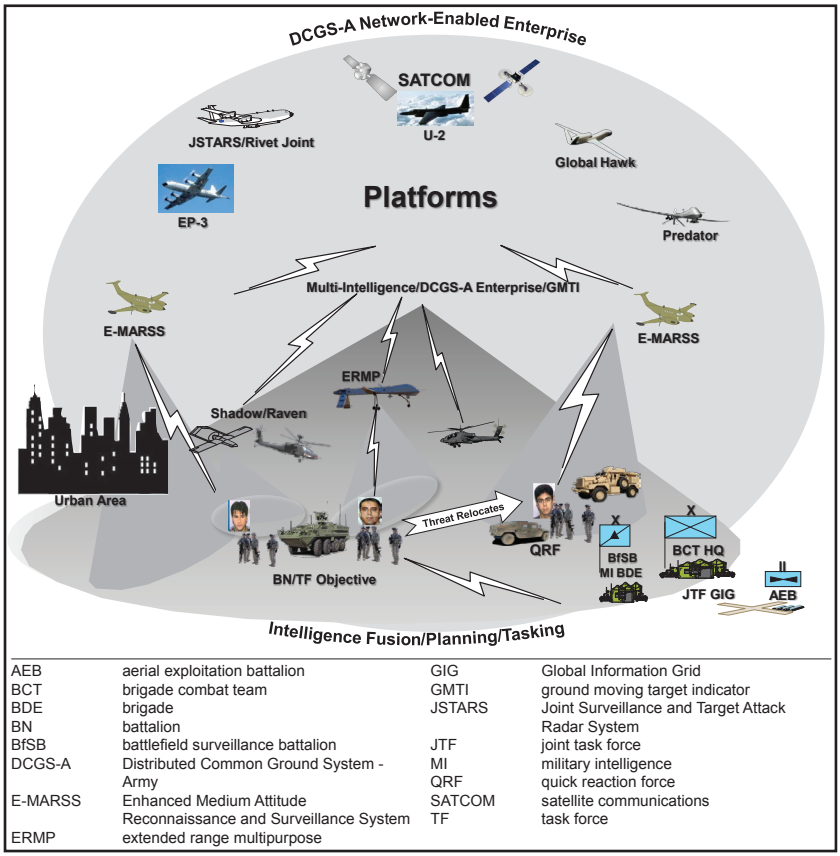
**2-22.** The Army intelligence enterprise is the totality of the networked and federated systems, and efforts of the military intelligence personnel (including collectors and analysts), sensors, organizations, information, and processes that allow the focus necessary to use the power of the entire intelligence community. Information about the U.S. and multinational intelligence community appears later in this chapter.

**2-23.** 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 synchronizes ISR activities and intelligence analysis and production to produce intelligence to support the commander's decisionmaking. Figure 2-1 illustrates the tactical portion of the Army intelligence enterprise.





FOR OFFICIAL USE ONLY




| | | | |
|---|---|---|---|
| AEB | aerial exploitation battalion | GIG | Global Information Grid |
| BCT | brigade combat team | GMTI | ground moving target indicator |
| BDE | brigade | JSTARS | Joint Surveillance and Target Attack Radar System |
| BN | battalion | | |
| BfSB | battlefield surveillance battalion | JTF | joint task force |
| DCGS-A | Distributed Common Ground System - Army | MI | military intelligence |
| | | QRF | quick reaction force |
| E-MARSS | Enhanced Medium Attitude Reconnaissance and Surveillance System | SATCOM | satellite communications |
| | | TF | task force |
| ERMP | extended range multipurpose | | |

**Figure 2-1. Army intelligence enterprise tactical portion**

**2-24.** Within the assigned AO, the commander must understand the critical elements of the operational environment that affect the mission. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). The operational environment includes the battlefield effects of—

- Enemy (including other threats).
- Terrain and weather.
- Mission variables.
- Civil considerations (areas, structures, capabilities, organizations, people, events [ASCOPE]). (For additional information on ASCOPE, see FM 2-01.3.)

**2-25.** The J-2/G-2/S-2 is the principal staff officer responsible for gathering information and intelligence for the commander. Intelligence staff officers are responsible for helping commanders understand how current and potential enemies organize, equip, recruit, train, employ, and control their forces. The J-2, G-2, or S-2 also aid commanders in understanding the terrain and weather, and their effects on both friendly and enemy operations. This includes the military aspects of the terrain and weather, as well as civil considerations. Additionally, intelligence officers assist commanders in synchronizing ISR during planning and operations.





FOR OFFICIAL USE ONLY

**2-26.** The intelligence staff can leverage the intelligence enterprise to assist in all areas of the intelligence warfighting function. The intelligence enterprise, connected to the GIG through LandWarNet, is distributed throughout the battlefield. It is the core of an integrated effort emphasizing the development of staff situational awareness and the commander's enhanced situational understanding.

**2-27.** DCGS-A is the intelligence component of the Battle Command Mission Command Network. DCGS-A provides a suite of analytical tools, digital mapping capabilities, and collaboration software. DCGS-A is carried on a subscriber network that links analysts using the system. This facilitates the collection, processing, and fusing of sensor data; the distribution of sensor information and fusion products; the storage and retrieval of information and intelligence; and the conduct of ISR operations.

## THE INTELLIGENCE WARFIGHTING FUNCTION

**2-28.** 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). The intelligence warfighting function is one of six warfighting functions—

- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- Mission Command.
- Protection.

**2-29.** 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 ISR operations and is driven by the commander. Intelligence is more than just collection. Developing intelligence is a continuous process that involves analyzing information from all sources and conducting operations to develop the situation.

**2-30.** The intelligence warfighting function is a flexible force of personnel, organizations, and equipment that, individually or collectively, provide commanders with the accurate, timely, usable, complete, precise, reliable, relevant, 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 supporting operations worldwide, from below ground to space.
- Includes the ability to leverage theater and national capabilities.
- Requires cooperation and federation of ISR and analysis efforts internally; with higher, lower, and adjacent organizations; and across Service components and multinational forces.



**2-31.** The intelligence warfighting function not only includes assets within the military intelligence (MI) branch, but also assets of other branches that perform intelligence warfighting function tasks. Each Soldier, as a part of a small unit, is a potential information collector and an essential contributor to the commander's situational understanding. Each Soldier develops a special level of awareness due to exposure to events occurring in the AO and has the opportunity to collect and report information by observation of, and interaction with the population.

**2-32.** Conducting (planning [to include design], preparing, executing, and assessing) military operations requires intelligence regarding the threat and other aspects of the AO. The intelligence warfighting function generates intelligence and intelligence products that describe the enemy and other aspects of the AO. These intelligence products enable commanders to identify potential courses of action (COAs), plan and employ forces effectively, employ effective tactics and techniques, and implement protection.



FOR OFFICIAL USE ONLY

**2-33.** The intelligence warfighting function supports commanders in offensive, defensive, stability, and, when directed, civil support operations. Intelligence supports realistic training thorough planning, meticulous preparation, and aggressive execution. The deployment tempo requires intelligence readiness to support operations at any point. This support reaches across the spectrum to produce the intelligence required to accomplish the mission. During force projection operations the intelligence warfighting function supports commanders from predeployment through redeployment.

**2-34.** The intelligence warfighting function architecture—the components comprising the intelligence warfighting function—provides specific intelligence and communication structures at each echelon from the national level to the tactical level. Effective communications connectivity and automation are essential components of this architecture.

**2-35.** Individual tasks making up the intelligence warfighting function are detailed in FM 2-0. The intelligence warfighting function includes these primary tasks:

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

## Support to Force Generation

**2-36.** Support to force generation is the task of generating knowledge concerning an AO, facilitating future intelligence operations, and force tailoring. It includes establishing intelligence communications architectures and knowledge management to enable intelligence reach, collaborative analysis, data storage, and intelligence production that supports the commander's contingency plans. Support to force generation consists of the following five subtasks:

- Provide intelligence readiness.
- Establish intelligence architecture.
- Provide intelligence overwatch.
- Generate knowledge.
- Tailor the intelligence force.

## Support to Situational Understanding

**2-37.** Support to situational understanding is the task of assisting commanders to clearly understand the force's current state relative to the enemy and the environment. It supports the commander's ability to make sound decisions. (See FM 2-01.3 for additional information.) This task is broken down into the following five subtasks:

- Perform IPB.
- Perform situation development.
- Provide intelligence support to protection.
- Provide tactical intelligence overwatch.
- Provide intelligence support to civil affairs activities.

## Perform Intelligence, Surveillance, and Reconnaissance

**2-38.** Perform ISR is an activity synchronizing and integrating collection assets and processing systems that support current and future operations. This is an integration of the intelligence and movement and maneuver functions. It is also a combined arms operation directed by the operations officer. It is supported by the intelligence officer and the rest of the staff. Through ISR, the unit continuously plans, tasks, and employs collection assets and intelligence processors to collect and disseminate timely and





FOR OFFICIAL USE ONLY

accurate information that satisfies the CCIRs. (See FMI 2-01 for additional information.) The task is broken down into the following subtasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct reconnaissance.
- Conduct surveillance.
- Conduct related missions and operations.

### Support to Targeting Information Superiority

**2-39.** Intelligence support to targeting and information superiority is the task of providing commanders information and intelligence support for targeting for lethal and nonlethal actions. It includes intelligence support to the planning, preparation, execution, and assessment of direct and indirect fires and the Army information tasks of information engagement, information protection, operations security (OPSEC), and military deception, as well as assessing the effects of those operations. (See JP 3-60 and FM 6-20-10 for doctrine on targeting. See FM 3-0, chapter 7, and FM 3-13 for doctrine on information superiority. See FM 3-36 for doctrine on electronic warfare.) Within this task are three subtasks:

- Provide intelligence support to targeting.
- Provide intelligence support to Army information tasks.
- Provide intelligence support to combat assessment.

## THE INTELLIGENCE COMMUNITY

**2-40.** The *intelligence community* consists of all departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role (JP 2-01.2). Many organizations in the intelligence community support military operations by providing specific intelligence products and services. The successful intelligence officer and staff are familiar with these organizations and the methods of obtaining information from them. Figure 2-2 shows the organizations of the U.S. intelligence community.





FOR OFFICIAL USE ONLY

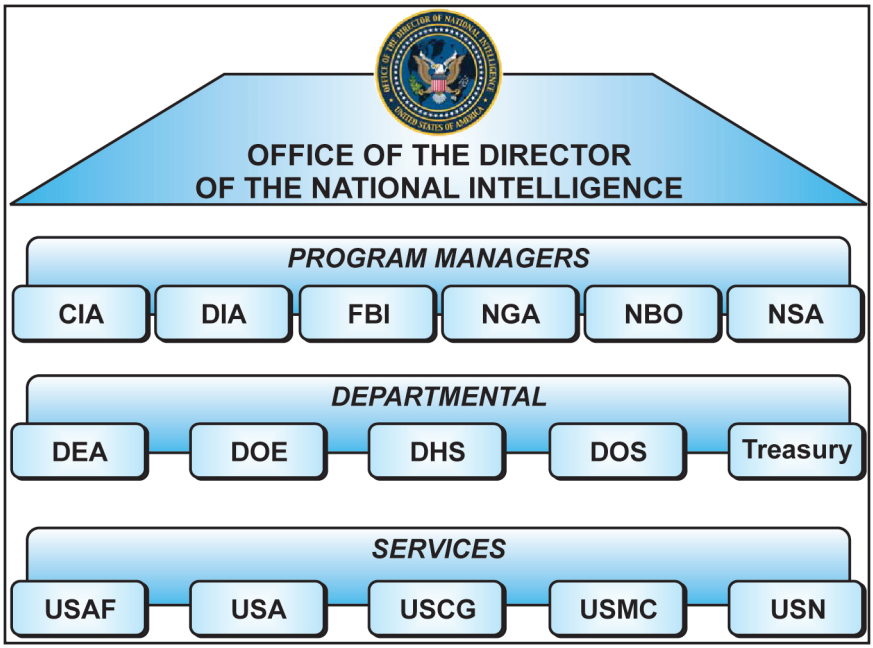



**Figure 2-2. Intelligence community membership**

## Office of the Director of National Intelligence

**2-41.** The Director of National Intelligence (DNI) is the head of the intelligence community, overseeing and directing the implementation of the National Intelligence Program. The DNI acts as the principal intelligence advisor to the President, the National Security Council, and the Homeland Security Council for matters related to national security. Working with the Principal Deputy DNI, the goal of the office of the DNI is to effectively integrate foreign, military, and domestic intelligence in defense of the United States and its interests abroad.

### Central Intelligence Agency

**2-42.** The Central Intelligence Agency's (CIA's) primary areas of expertise are human intelligence (HUMINT) collection, all-source analysis, and the production of political, economic, and biographic intelligence.

### Defense Intelligence Agency

**2-43.** The Defense Intelligence Agency (DIA) provides oversight of the Defense Intelligence Analysis Program and provides intelligence support in such areas as all-source military analysis; human factors analysis; HUMINT; measurement and signature intelligence (MASINT); medical intelligence; CI; counterterrorism; chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) counterproliferation; counterdrug operations; information operations (IO); personnel recovery; peacekeeping and multinational support; noncombatant evacuation operations; indications and warning (I&W); targeting; battle damage assessment; current intelligence; systems analysis of the threat; collection management; intelligence architecture and systems support; intelligence support to operation planning; defense critical infrastructure protection; and document and media exploitation (DOMEX). (For more information on the DIA and its organizations, see DODD 5105.21.)




FOR OFFICIAL USE ONLY

### Federal Bureau of Investigation

**2-44.** The Federal Bureau of Investigation (FBI) has primary responsibility for conducting CI activities, and coordinates CI activities with other agencies in the intelligence community within the United States. (EO 12333 includes international terrorist activities in its definition of CI.) The FBI shares law enforcement and CI information with appropriate Department of Defense (DOD) entities and combatant commands. The FBI is a key component in the Army's biometrics program. The FBI also plays a key role in operations outside the continental United States, including counterthreat finance operations.

### National Geospatial-Intelligence Agency

**2-45.** The National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence (GEOINT) support, including imagery intelligence (IMINT), geospatial information, geospatial data sets, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic data and information. (For more information on the NGA and its organizations, see DODD 5105.60.)

### National Reconnaissance Office

**2-46.** The National Reconnaissance Office (NRO) is responsible for integrating unique and innovative space-based reconnaissance technologies. The NRO also engineers, develops, acquires, and operates space reconnaissance systems and conducts related intelligence activities. (For more information on the NRO and its organizations, see DODD 5105.23.)

### National Security Agency/Central Security Service

**2-47.** The National Security Agency (NSA) is the U.S. Government lead for cryptology. Its mission encompasses both signals intelligence (SIGINT) and information assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS (DIRNSA/CHCSS). NSA/CSS provides SIGINT and IA guidance and assistance to the DOD components, as well as national customers. The DIRNSA/CHCSS serves as the principal SIGINT and IA advisor to the Secretary of Defense, the Under Secretary of Defense (Intelligence), the Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer, the Chairman of the Joint Chiefs of Staff, the combatant commanders, the secretaries of the military departments, and the DNI, as well as other U.S. Government officials. (For more information on the NSA and its organizations, see DODD 5100.20.)

### Drug Enforcement Administration

**2-48.** The Drug Enforcement Administration (DEA) has primary responsibility for enforcing the controlled substances laws and regulations of the United States. This includes illicit substances destined for sale in the United States. Because of this, DEA operates extensively overseas, often in cooperation with the intelligence community. DEA also participates as a non-DOD partner in counterthreat finance operations.

**2-49.** DEA maintains a national drug intelligence network in cooperation with federal, state, local, and foreign officials. It collects, analyzes, and disseminates strategic, investigative, and tactical intelligence information to U.S. law enforcement and intelligence agencies and, when appropriate, to foreign counterparts.

### Department of Energy

**2-50.** The Department of Energy (DOE) analyzes foreign information relevant to U.S. energy policies and nonproliferation issues.





FOR OFFICIAL USE ONLY

### Department of Homeland Security

**2-51.** The Department of Homeland Security (DHS) includes the following subordinate organizations:

- Customs and Border Protection.
- Federal Emergency Management Agency.
- Immigration and Customs Enforcement.
- Transportation Security Administration.
- U.S. Citizenship and Immigration Services.
- U.S. Secret Service.
- Office of Inspector General.

**2-52.** The Directorate for Information Analysis and Infrastructure Protection analyzes the vulnerabilities of U.S. critical infrastructure, assesses the scope of terrorist threats to the U.S. homeland, and provides input to the Homeland Security Advisory System.

### Department of State

**2-53.** The Department of State's (DOS's) Bureau of Intelligence and Research performs intelligence analysis and production on a wide range of political and economic topics essential to foreign policy formulation and execution.

### Department of the Treasury

**2-54.** The Department of the Treasury analyzes foreign intelligence related to economic policy and participates, with the DOS, in the overt collection of general foreign economic information.

### U.S. Air Force

**2-55.** The Air Force Deputy Chief of Staff for ISR 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 ISR Agency. Additionally, the Air Force Office of Special Investigations is the Service's main focal point for CI activities. The Air Force Weather Agency provides meteorological support. (Additional information describing the Air Force approach to operational ISR employment is found in AFDD 2-9.)

### U.S. Army

**2-56.** The U.S. Army Intelligence Department (G-2) is responsible for policy formulation, planning, programming, budgeting, management, staff supervision, evaluation, and oversight of intelligence activities for the Department of the Army. The G-2 is responsible for the overall coordination of the MI disciplines.

### U.S. Coast Guard

**2-57.** The U.S. Coast Guard (USCG) operates as both a military service and a law enforcement organization. It provides general maritime intelligence support to commanders from the strategic to tactical levels in the areas of HUMINT, SIGINT, GEOINT, MASINT, open-source intelligence (OSINT), and CI.

### U.S. Marine Corps

**2-58.** The Director of Intelligence is the Marine Corps (USMC) 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 ISR Enterprise.





FOR OFFICIAL USE ONLY

### U.S. Navy

**2-59.** The Director of Naval Intelligence exercises staff supervision over the Office of Naval Intelligence (ONI), which provides the intelligence necessary to plan, build, train, equip, and maintain U.S. naval forces. The National Maritime Intelligence Center consists of ONI, the USCG Intelligence Coordination Center, the Navy Information Operations Command, and detachments of the Marine Corps Intelligence Activity and Naval Criminal Investigative Service.

### Other Agencies

**2-60.** There are a number of U.S. Government agencies and organizations that are not members of the intelligence community but that collect and maintain 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 U.S. Patent Office are potential sources of specialized information on political, economic, and military topics. The intelligence community may draw on these organizations to support and enhance research and analysis and to provide relevant information and intelligence to commanders and planners.

**2-61.** Many other U.S. Government agencies directly support 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 U.S. Foreign Disaster Assistance.
- U.S. Agency for International Development.

## Multinational Intelligence Organizations

**2-62.** DOD and U.S. Government intelligence organizations often work together with multinational intelligence organizations—both military and civilian—to achieve common goals. *Multinational operations* are military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance (JP 3-16).

**2-63.** Every aspect of the intelligence process is substantially affected in multinational operations. In some international operations or campaigns, joint force commanders will be able to use international standardization agreements as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation is unique, such agreements may have to be modified or amended, based on the situation. The following general principles provide a starting point for creating the necessary policy and procedures (for more information, see JP 3-16, and JP 2-01):

- **Maintain unity of effort.** Each nation's intelligence personnel need to view the threat from multinational as well as national perspectives. A threat to one multinational partner must be considered a threat to all multinational partners.
- **Make adjustments.** There will be differences in intelligence doctrine and procedures among multinational partners. A key to effective multinational intelligence is the readiness to make the adjustments required to resolve significant differences.
- **Plan early and plan concurrently.** National command channels need to determine what intelligence may be shared with the forces of other nations.
- **Share all necessary information.** Multinational partners should share all relevant and pertinent intelligence about the situation and threat, consistent with U.S. and theater guidance.
- **Conduct complementary operations.** Intelligence efforts of the nations must be complementary. Each nation's intelligence system will have strengths and limitations as well as unique and valuable capabilities. All intelligence resources and capabilities should be available to apply to the whole of the intelligence problem. Establishing a multinational collection management element is essential for planning and coordinating multinational collection operations.





FOR OFFICIAL USE ONLY

# Chapter 3
# Intelligence Disciplines

## INTRODUCTION

**3-1.** Intelligence disciplines are categories of intelligence functions. The Army's intelligence disciplines are—

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

## ALL-SOURCE INTELLIGENCE

**3-2.** *All-source intelligence* is the intelligence discipline responsible for all-source products and the processes used to produce them (FM 2-0). *All-source intelligence* also refers to intelligence products and organizations and activities that incorporate all sources of information, most frequently including human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source intelligence data in the production of finished intelligence (JP 2-0). Army forces conduct operations based on the all-source intelligence assessment developed by the intelligence staff. The all-source intelligence assessment is expressed as part of the intelligence estimate.

**3-3.** All-source intelligence operations are performed by the intelligence staff. They 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 (to include design). They are updated as needed, throughout preparation and execution, based on information gathered through continuous assessment.

### Role

**3-4.** The ever-growing volume of data and information from numerous sources helps commanders improve their situational understanding. Situational understanding enables commanders to better—

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

**3-5.** Commanders depend on skilled intelligence Soldiers to—

- Provide sound intelligence preparation of the battlefield (IPB) products.
- Support the intelligence, surveillance, and reconnaissance (ISR) effort.
- Provide all-source intelligence analysis, including conclusions and projections of future conditions or events that are needed to accomplish the mission according to the commander's intent.

### Fundamentals

**3-6.** Intelligence results from the collection, processing, integration, evaluation, analysis, and interpretation of available information. Intelligence also refers to activities that result in the product and to the organizations engaged in such activities.




FOR OFFICIAL USE ONLY

**3-7.** Using information drawn from all disciplines and available sources, all-source analysts perform analysis. They produce timely, relevant, accurate, predictive, and tailored intelligence that satisfies the commander's requirements. All-source analysis provides an overall picture of the threat, terrain and weather, and civil considerations, as well as other aspects of the area of operations (AO). All-source analysis reduces the possibility of error, bias, and misinformation by considering multiple sources of information and intelligence.

## Planning

**3-8.** During planning, the intelligence staff is responsible for providing well-defined, specific all-source intelligence products and tools. The commander and staff expect and require the use and availability of these products and tools throughout planning, regardless of the specific process used:

- Threat characteristics.
- Threat templates and models.
- Threat course of action (COA) statements.
- Event template and event matrix.
- High-value target (HVT) list.
- Weather effects matrix.
- Modified combined obstacle overlay (MCOO) and terrain effects matrix.
- Civil considerations IPB overlays.
- Appropriate civil support products.

***Note.*** Only the intelligence staff's initiative and imagination limit possible products.

**3-9.** The military decisionmaking process (MDMP) combines the conceptual and detailed components of planning. Commanders use the MDMP to build plans and orders for extended operations as well as to develop orders for short-term operations within the framework of a long-range plan. (See appendix D for a discussion of intelligence support to MDMP.)

## Types of Intelligence Products



**3-10.** The intelligence staff produces and supports multiple products, including—

- Running estimate.
- Intelligence running estimate.
- Common operational picture (COP).
- Intelligence estimate.
- Intelligence summary (INTSUM).

## Running Estimate

**3-11.** A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (FM 3-0). Running estimates provide information, conclusions, and recommendations from the perspective of each staff section. They are a staff technique to support the commander's visualization and decisionmaking, 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 information.

**3-12.** Each staff section produces a running estimate. The staff continuously updates the conclusions and recommendations while including projections of future conditions in the area of interest.


FOR OFFICIAL USE ONLY

## Intelligence Running Estimate

**3-13.** The intelligence running estimate helps the intelligence staff track and record pertinent information and provide recommendations to the commander. When applied to the COP, it is a continuous flow and presentation of relevant information and predictive intelligence. When this estimate is combined with the other staff running estimates, it enables the commander's visualization and situational understanding of the area of interest in order to achieve information superiority.

**3-14.** The intelligence running estimate 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, one based on current intelligence products and reports and predictive estimates of future threat activity. The intelligence running estimate consists of all the continuously updated and monitored intelligence available. This intelligence is then filtered to provide the specific intelligence supporting current and projected future operations.

**3-15.** G*enerate intelligence knowledge*, one of the continuing activities of the intelligence process, directly supports the development of the intelligence running estimate, which is refined and improved following mission analysis. It is further refined based on the results of ISR activities. The intelligence running estimate is updated, as required, based on changes in the threat situation, terrain and weather, and civil considerations. The intelligence running estimate includes—

- Situation and considerations.
- Mission.
- COAs.
- Analysis (threat-based).
- Comparison (threat-based).
- Recommendations and conclusions.

**3-16.** The successful intelligence officer clearly understands the weather and terrain effects and visualizes the AO to develop and maintain the intelligence running estimate. This understanding facilitates accurate assessments and projections regarding the—

- Threat.
- Threat situation (including strengths and weaknesses).
- Threat capabilities and an analysis of those capabilities (COAs available to the threat).
- Conclusions drawn from that analysis.

**3-17.** The intelligence running estimate transforms threat characteristics into threat capabilities and projections of future threat actions.

## Common Operational Picture

**3-18.** The *common operational picture* is a single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (FM 3-0). The COP is the primary tool for facilitating the commander's situational understanding. All staff sections provide input regarding their areas of expertise to create the COP.

**3-19.** The portion of the COP depicting the threat situation is 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. The Distributed Common Ground System-Army (DCGS-A) is the means for integrating this information into the COP. (See appendix E.)




FOR OFFICIAL USE ONLY

## Intelligence Estimate

**3-20.** An *intelligence estimate* is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the course of action (COA)s open to the enemy or adversary and the order of probability of their adoption (JP 2-0). The intelligence staff develops and maintains the intelligence estimate.

## Intelligence Summary

**3-21.** An INTSUM summarizes the most current threat situation covering a period of time designated by the commander. This period of time varies, based on 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. An INTSUM may be presented in written, graphic, or oral format, as directed by the commander.

**3-22.** The INTSUM helps the commander assess the current situation and updates other intelligence reports. The INTSUM reflects the interpretation and conclusions of the S-2, G-2, or J-2 regarding threat capabilities and probable COAs, as well as civil considerations. The INTSUM is prepared at brigade and higher echelons and disseminated to higher, lower, and adjacent units. The INTSUM has no prescribed format except that INTSUM will be the first item of the report.

**3-23.** For more information on all-source intelligence, see FM 2-0. Associated military occupational specialty (MOS)s areas of concentration (AOC)s are 35F/350F, 35D.

# COUNTERINTELLIGENCE

**3-24.** *Counterintelligence* is information gathered and activities performed to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations performed for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities (Executive Order 12333[EO 12333]).



**3-25.** CI includes actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of adversaries. It is a key intelligence community contributor to protect U.S. interests.

## Mission and Role

**3-26.** Army CI performs aggressive, comprehensive, and coordinated investigations, operations, collection, analysis and production, and technical services. These functions are performed worldwide to detect, identify, assess, counter, exploit, or neutralize collection threats by the foreign intelligence and security services (FISS) and international terrorist organizations (ITO) to the Army and Department of Defense (DOD), in order to protect the lives, property, or security of Army forces. Army CI has four primary mission areas:

- Counterespionage.
- Support to protection of the force.
- Support to research and technology protection.
- Cyber CI.

**3-27.** The role of CI is to deny, degrade, disrupt, or mitigate FISS and ITO ability and capability to successfully execute intelligence collection targeting U.S. or friendly force interests. CI focuses on countering FISS and ITO intelligence collection activities targeting information or material



FOR OFFICIAL USE ONLY

concerning U.S. or friendly force personnel, activities, operations, plans, equipment, facilities, publications, technology, or documents—either classified or unclassified. CI elements contribute to situational awareness of 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 CI technical services.

## Fundamentals

**3-28.** Fundamentals of the CI discipline include—

- CI core competencies.
- CI structure.
- Support to contingency operations.
- Operational considerations.

## Counterintelligence Core Competencies

**3-29.** CI core competencies are interrelated, mutually supporting, and can be derived from one another. No single competency can defeat the FISS and ITO intelligence collection threat targeting U.S. interests in general, and Army interests specifically. The CI core competencies include—

- Operations.
- Investigations.
- Collection.
- Technical services and support.
- Analysis and production.

### Operations

**3-30.** CI operations are broadly executed activities that support a program or specific mission. CI operations use one or more of the core competencies discussed below. CI operations can be offensive or defensive, and they are derived from, transitioned to, or used simultaneously—depending on the scope, objective, or continued possibility for operational exploitation. Operations fall into two categories—support operations and sensitive operations.

### Investigations

**3-31.** CI performs investigations when national security crimes are allegedly committed by anyone under CI authority. The primary objective of any CI investigation is the identification, exploitation, or neutralization of threats directed against the Army. CI also performs investigations to identify systemic security problems that may have damaging repercussions to Army operations and national security interests.

### Collection

**3-32.** CI collection is the systematic acquisition of information concerning the FISS and ITO intelligence collection threat targeting Army interests. CI elements perform collection activities to support the overall CI mission. CI collection is performed using sources, elicitation, official liaison contacts, debriefings, screenings, and OSINT to obtain information that answers the standing CI collection requirements or other collection requirements based on commanders' requirements.

**3-33.** Although CI and HUMINT have a collection mission, there are distinct differences between their collection objectives. HUMINT focuses on answering commander's critical information requirements (CCIRs) concerning the plans, intentions, capabilities, and disposition of the threat. CI performs collection to understand how FISS and ITO target U.S. forces. With this information commanders can protect personnel, mission, resources, and technology.




FOR OFFICIAL USE ONLY

### Technical Services and Support

**3-34.** CI technical services assist the CI core competencies of investigations, collections, and operations or provide specialized technical support to a program or activity. The proliferation of sophisticated collection technology, surveillance, and eavesdropping devices gives any FISS and international terrorist organizations the ability to increase their capability and effectiveness in collecting on Army interests.

**3-35.** Mitigating this increasing threat requires specialized expertise. CI organizations with technically trained CI special agents are chartered to provide this unique technical capability to augment and provide specialized support to the CI mission. This includes CI special agents trained to—

- Perform technical surveillance countermeasures.
- Perform cyber CI activities.
- Perform CI scope polygraph examinations.
- Provide support to Army information tasks.

### Analysis and Production

**3-36.** CI analysis and production satisfy supported commanders' intelligence requirements and provide focus and guidance to CI operations. CI analysis and production can be accomplished at any level at which Army CI assets are assigned.

#### *Intelligence Analysis*

**3-37.** CI analysis provides supported commanders with situational awareness and understanding of the operational environment. CI analysis focuses on predictive assessments of the plans, intentions and capabilities of FISS and international terrorist organizations. This allows commanders to make informed decisions on the protection posture and targeting to neutralize or exploit those threats to the advantage of U.S. forces.

#### *Operational Analysis*

**3-38.** Operational analysis allows the operational management elements to evaluate the effectiveness and success of their subordinate operational CI teams. This is done through assessments of source production (quantity and quality), source vetting (reliability, accuracy, response to control), and requirements coverage. Operational analysis also allows operational managers to deconflict CI operations, provide direction and focus to eliminate redundancy, and increase the efficiency of the CI teams.



## Counterintelligence Structure

**3-39.** 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 (BFSBs), Army Service component commands (ASCCs), and strategic units are capable of operating at all echelons across the spectrum of conflict. The joint 2X organizational and operational concept was 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 counterintelligence coordinating authority (CICA) throughout the Army ensures a trained and experienced cadre of CI professionals capable of filling Army, joint, and combined 2X and CICA positions.

**3-40.** 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


FOR OFFICIAL USE ONLY

three components—CICA, a HUMINT operations cell (HOC), and an operations support cell (OSC). (See TC 2-22.303 for information on the Army 2X and JP 2-01.2 [S] for information on the joint 2X.)

**3-41.** 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 (MICECP) government civilian employee. (See AR 614-115 [S//NF] for more information on MICECP.)

## Support to Contingency Operations

**3-42.** 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 mission command nodes to identify the collection threat to U.S. forces that could be used by adversary elements to plan hostile acts against U.S. activities and locations.

**3-43.** Once security of the operating bases is established, the operational focus of CI teams shifts outside the operating base to continue to detect, identify, and neutralize the collection threat to U.S. forces as well as to provide indications and warning (I&W) of hostile acts targeting U.S. activities. The CI team uses several collection methods, including CI force protection source operations (CFSO), elicitation, and liaison to answer supported commanders' 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.

**3-44.** 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 approachability 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.

**3-45.** 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. In addition, 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.

## Operational Considerations

**3-46.** CI must be represented and integrated into all phases of operational planning. The success of CI teams 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 nondoctrinal solutions to allow them to operate. This may mean the CI team is paired with other combat and noncombat units to facilitate movement in a particular AO.

**3-47.** The mission of the CI team must be integrated into the overall scheme of maneuver to support commanders' requirements. CI teams are often resourced or outfitted with non-table of organization and equipment (TOE), resources, and personnel that serve a specific purpose and provide them




FOR OFFICIAL USE ONLY

a unique capability to support their commanders. 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.

**3-48.** For more information on CI see FM 2-22.2. Associated MOSs/AOCs are 35L, 35Y/351L, 35E.

## HUMAN INTELLIGENCE

**3-49.** *Human intelligence* is the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities (FM 2-0).

### Capabilities

**3-50.** HUMINT has many capabilities:

- HUMINT collects information from an almost endless variety of potential sources. These include friendly forces, civilians, detainees, and source-related and open-source documents.
- HUMINT focuses on collecting detailed information not available by other means. This includes information on threat intentions and the attitudes and morale of local civilians and threat forces.
- HUMINT can corroborate or refute information collected by other ISR assets.
- HUMINT operates with minimal equipment and deploys in all operational environments to support offensive, defensive, or stability operations. Based on solid planning and preparation, HUMINT collection can provide timely information when deployed in support of maneuver elements and provided with mission-focused support.

### Fundamentals

**3-51.** A HUMINT source is a person that can provide information. HUMINT sources may be threat, neutral, or friendly personnel—either military or civilian. HUMINT operations are supported at times by all of other intelligence disciplines. Principal among these is all-source analysis. All-source analysis supports HUMINT in many ways—one of these is "tiger teams."

**3-52.** HUMINT collectors are the only personnel authorized to perform 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, select other specially trained MOSs, 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 the U.S. Army Intelligence Center of Excellence (USAICoE), Ft. Huachuca, AZ.
- Joint Interrogation Certification Course at HUMINT Training-Joint Center of Excellence (HT-JCOE), Ft. Huachuca, AZ.
- Defense Intelligence Agency I-10 Course, Alexandria, VA.

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

**3-53.** HUMINT collection operations must be performed in accordance with all applicable U.S. law and policy, which include U.S. law; the law of war; relevant international law; relevant directives, including DODD 3115.09 and DOD Directive 2310.1E; DOD instructions; and executive orders, including fragmentary orders. Additional policies and regulations apply to the management of contractors engaging in HUMINT collection.





FOR OFFICIAL USE ONLY

**3-54.** Most HUMINT collection consists of five phases: planning and preparation, approach, questioning, termination, and reporting. Phasing in military source operations (MSO) may differ. These five phases are generally sequential; however, reporting may occur at any point within the process when critical, time-sensitive intelligence information is obtained. The approach techniques are reinforced throughout the questioning and termination phases. (See FM 2-22.3.)

## Human Intelligence Operations

**3-55.** A HUMINT operation ties together all the terms discussed above. HUMINT operations are performed to answer commanders' intelligence requirements. The requirements may vary, depending on the source of the intelligence information. Once the type of operation has been determined, leaders use the operations process (plan [including design], prepare, execute, and assess) as they conduct the operation. Different types of HUMINT operations are—

- Detainee interrogation operations.
- Refugee and local civilian debriefing operations.
- MSO.
- Liaison operations.
- Screening operations.
- Friendly force debriefing operations.
- Support to document and media exploitation (DOMEX) operations.
- Support to site exploitation operations.
- Captured enemy materiel exploitation operations.

### Detainee Interrogation Operations

**3-56.** Detainee interrogation operations involve the systematic questioning of detainees, including enemy prisoners of war, in response to collection requirements. This type of HUMINT operation may be performed at point of capture, at a military police (MP) facility, at a multinational-operated facility, or at another governmental agency-operated collection facility.

### Refugee and Local Civilian Debriefing Operations

**3-57.** Refugee and local civilian debriefing operations involve questioning cooperating refugees to satisfy intelligence requirements consistent with applicable laws. The refugee may, or may not be in custody, and a refugee's willingness to cooperate need not be immediate or constant. Refugee debriefings are usually performed at refugee collection points or checkpoints. They may be performed in cooperation with MP or civil affairs (CA) operations. As with refugees, the local civilians being debriefed may, or may not be in custody. The civilians' willingness to cooperate may or may not, be immediate or constant.



### Military Source Operations

**3-58.** MSO are designed to establish a longer term, formal relationship between a HUMINT collector and a HUMINT source for the purpose of obtaining intelligence information. MSO are generally overt, but discreet tactically oriented collection activities using humans to identify attitudes, intentions, composition, strengths, dispositions, tactics, equipment, locations, target development, personnel, and capabilities of threats to U.S. and multinational partner forces. MSO are employed to develop HUMINT sources that can provide early warning of imminent danger to U.S. and multinational partner forces and contribute to the MDMP. HUMINT collectors may task HUMINT sources to collect specific information only under certain conditions. MSO that involve HUMINT source tasking must be carried out in accordance with AR 381-172 (S//NF), DIAM 58-11 (S//NF), and DHE-M 3301.001 (S//NF). (See also TC 2-22.302 [S//NF] and EO 12333.)

### Liaison Operations

**3-59.** Liaison operations coordinate activities and exchange information with host-nation military and


FOR OFFICIAL USE ONLY

civilian governmental organizations, including police and other infrastructure providers, multinational partners, civilian agencies, and nongovernmental organizations (NGOs).

### Screening Operations

**3-60.** Screening operations identify human or media sources to determine their ability to satisfy intelligence requirements and effectively prioritize the sources for exploitation. Human sources are evaluated for their level of knowledge, level of cooperation, and their placement and access to desired information. Media are screened for content answering priority intelligence requirements (PIRs) or other information of intelligence interest. Screening operations also assist in determining which intelligence discipline or agency could best exploit a given source. Screening operations include, but are not limited to—

- Mobile and static checkpoints where screening of refugees and displaced persons can occur.
- Locally employed personnel screening.
- Screening performed in conjunction with a cordon and search operation.
- Detainee screening.
- DOMEX screening.

### Friendly Force Debriefing Operations

**3-61.** Friendly force debriefing operations involve debriefing U.S. forces and multinational partners to answer collection requirements, and to ensure that information collected is entered into the intelligence system for proper analysis and dissemination. These operations must be coordinated with the affected U.S. or multinational partner units.

### Support to DOMEX Operations

**3-62.** Support to DOMEX operations involves the screening and systematic extraction of intelligence information from open, closed, printed, and electronic media. For the purposes of this type of HUMINT operations, documents refers to written materials and data inside electronic communications equipment, such as computers, telephones, personal digital assistants, and Global Positioning System devices. The execution of this type of operation is not exclusively a HUMINT function, but may be conducted by any intelligence person. Captured enemy documents are frequently first screened by HUMINT collectors and subsequently used in conjunction with interrogations. A captured enemy document is any document that has been in possession of the enemy, whether or not the enemy created it.



### Support to Site Exploitation Operations

**3-63.** Support to site exploitation operations consists of activities within a site captured from a threat. Sites include factories with technical data on enemy weapons systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, threat finance materials, and document storage areas for secret police forces. These activities exploit personnel, documents, electronic data, and materiel captured at the site while neutralizing any threat posed by the site or its contents.

### Captured Enemy Materiel Exploitation Operations

**3-64.** Captured enemy materiel exploitation operations focus on obtaining and exploiting all types of foreign and nonforeign materiel from a variety of sources. The materiel may have a military application or answer an intelligence collection requirement.

### Planning

**3-65.** There are a number of planning considerations for HUMINT operations. Among them are—

- Interpersonal skills.
- Availability of trained and certified personnel.
- Time.
- Language limitations.



FOR OFFICIAL USE ONLY

- Understanding of the HUMINT mission.
- Collection capability.
- Risk management.
- Legal obligations.
- Connectivity and bandwidth requirements.
- Reporting and immediate access to sources.

**3-66.** For more information on HUMINT, see FM 2-22.3. Associated MOSs or AOCs are 35M, 35Y/351M, 35F.

## GEOSPATIAL INTELLIGENCE

**3-67.** *Geospatial intelligence* is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. (Title 10, Section 467, U.S. Code, establishes GEOINT.) GEOINT consists of imagery, imagery intelligence, and geospatial information (JP 2-03). The Army has retained IMINT as a sub-discipline of GEOINT.

**3-68.** Imagery is 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 behalf of HUMINT collection organizations. *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03).

**3-69.** Geospatial information is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including statistical data and information derived from, among other things, remote sensing; mapping and surveying technologies; and mapping, charting, geodetic data, and related products.

**3-70.** There are many producers of GEOINT, and the users of GEOINT extend from the national level to the lowest tactical level. The overall GEOINT enterprise supporting 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.

**3-71.** The Army does not perform GEOINT operations in isolation. Many ongoing operations and activities across the DOD involve GEOINT. 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 (including the Services), and combatant commands.
- Partners include civil applications committee members, international partners, industry, academia, defense service providers, and civil community service providers.




FOR OFFICIAL USE ONLY

## Capabilities

**3-72.** GEOINT is an intelligence field that—

- Incorporates intelligence analysis into all aspects of it.
- Uses multiple types of sensors and advanced sensor technology.
- Combines multiple types of geospatial data.
- Uses intelligence and data from other intelligence disciplines to provide context.
- Provides the capability to visualize in three dimensions.
- Integrates the element of time and movement, allowing for realistic motion to create dynamic and interactive visual products.
- Provides the geospatial foundation layer for the COP.

## Fundamentals

**3-73.** GEOINT consists of four basic components:

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

**3-74.** GEOINT encompasses all activities involved in the planning, collection, processing, analysis, exploitation, and dissemination of spatial information in order to gain intelligence about the national security or operational environment, visually depict this knowledge, and fuse the acquired knowledge with other information through analysis and visualization processes.

**3-75.** Technology allows the analyst to use and combine geospatial data in different ways to create customized visual products. It allows the analyst to quickly make complex connections between different types of data and information. Geospatial products can leverage a wider variety of data, including information from other intelligence disciplines, through collaborative processes to provide more accurate, comprehensive, and relevant products.



**3-76.** GEOINT specialties include—

- Aeronautical analysis.
- Cartography.
- Geodetic sciences.
- Geospatial analysis.
- Imagery analysis.
- Imagery sciences.
- Marine analysis.
- Regional analysis.
- Source analysis.

**3-77.** Geospatial data can be derived from multiple classified or unclassified sources. GEOINT comprises imagery, IMINT, and geospatial information.

## Geospatial Intelligence Support to Planning and Operations

**3-78.** During planning, geospatial engineers are responsible for developing a specific set of terrain and imagery products within the confines of well-defined guidance and timelines. The terrain-related products produced by the GEOINT cell in the G-2 or S-2 as part of its continuous analysis of the AO during the IPB process have a significant role in targeting and ISR activities.

**3-79.** With the increasing demand for geospatial support at all echelons, the Army created the Army Geospatial Center (AGC) which replaced the Engineer Research and Development Center's Topographic Engineering Center (TEC). The AGC is a direct reporting unit under the U.S. Army


FOR OFFICIAL USE ONLY

Corps of Engineers and provides the same geospatial support that TEC did—coordinating, integrating, and synchronizing GEOINT standards and requirements for the Army in addition to developing and fielding geospatial enterprise-enabled systems and capabilities to the Army and DOD.

### Support To Planning

**3-80.** To effectively assist in planning, successful imagery analysts and geospatial engineers understand the purpose, environment, and characteristics of the planning process described in FM 5-0, the IPB process as described in FM 2-01.3, IPB tactics, techniques and procedures (TTP) as discussed in FM 2-01.301, and intelligence analysis as discussed in TC 2-33.4. In addition, GEOINT planners understand enemy tactics, enemy operational art, the fundamentals of operations described in FM 3-0, and the art of tactics described in FM 3-90. Finally, imagery and geospatial analysts must be familiar with the operations process (including design), and understand how mission command, the commander's visualization of the situation, and the commander's exercise of mission command influence planning.

**3-81.** During planning, geospatial engineers are responsible for developing a specific set of terrain and imagery products within the confines of well-defined guidance and timelines. Formal planning begins with the receipt of mission from higher headquarters or as directed by the commander. However, prior to formal planning, GEOINT cells have a vast amount of preparation to perform in order to be prepared for mission analysis.

**3-82.** Prior to the start of formal planning, the GEOINT cell must develop an understanding of the terrain aspects of the operational environment. Equally as important, the GEOINT cell must have either constructed or received the digital terrain and imagery products necessary to support terrain analysis during IPB. Once the orders process begins, there may not be enough time to build these products prior to the mission analysis briefing or during the rest of the MDMP. The construction of digital overlays is an example of this. In addition to the amount of time required to build the detailed terrain overlays, the time the staff needs to perform planning is significant. It takes even more time to build the overlays required for urban operations. It is important to note that even if the GEOINT cell receives this information from its higher headquarters, the data may not be in the format needed to perform planning. Text, graphic, and spreadsheet products may have to be transformed into digital products that can be used by all of the staff elements in the headquarters.

**3-83.** One of the five critical subtasks to Army tactical task 2.1 (Force Generation) is generate knowledge.

**3-84.** The end state of the generate knowledge process is the development of four general baseline data sets: threat, terrain, weather, and civil considerations. The GEOINT cell is responsible for the terrain data set and provides support to the all-source/fusion cell for the civil considerations data set.

**3-85.** To accomplish this task, the S-2, G-2, or J-2, based on guidance from the commander, focuses GEOINT operations on specific threat forces, continually gathering and refining data throughout the Army force generation (ARFORGEN) process. This results in the intelligence staff being as prepared as possible to begin planning upon receipt of the mission.

### Support to Operations

**3-86.** The full utility of GEOINT comes from the integration of imagery, IMINT, and geospatial information. This results in a more thorough visualization and analysis, and a tailorable view of the operational environment. Imagery, including full motion video and motion imagery, often enhances the commander's situational understanding of the AO. Imagery is also used to support training and the operational requirements, including navigation, mission planning, mission rehearsal, modeling, simulation, and precise targeting. Detailed mission planning and IPB often require imagery to provide the degree of resolution needed to support specialized planning.




FOR OFFICIAL USE ONLY

### *Offensive Operations*

**3-87.** *Offensive operations* are combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers. They impose the commander's will on the enemy (FM 3-0). Offensive operations at all levels require effective intelligence to help commanders avoid the enemy's main strength and to deceive and surprise the enemy. During offensive operations, GEOINT must provide commanders with updated IPB products and products that support the intelligence running estimate. These products must be provided in a timely manner for commanders to significantly affect the enemy.

**3-88.** GEOINT supports the development of IPB products by the S-2, G-2, or J-2 to assist commanders in identifying all aspects of the AO or area of interest that can affect mission accomplishment. The entire staff, led by their intelligence staff, uses the IPB process to identify any aspect of the AO or area of interest that will affect enemy, friendly, and third-party operations.

**3-89.** Organic imagery collection supports commanders' use of unit ISR assets to analyze the terrain and confirm or deny the enemy's strengths, dispositions, and likely intentions. The S-2, G-2, or J-2 officer and S-3, G-3, or J-3 officer, in coordination with the rest of the staff, develop an integrated ISR plan, utilizing imagery collection to satisfy commanders' maneuver, targeting, and information requirements.

**3-90.** In offensive operations, CCIR tasked to GEOINT often include, but are not limited to—

- Locations, composition, equipment, strengths, and weaknesses of the defending enemy force—including high-payoff targets (HPTs) and enemy ISR capabilities.
- Locations of possible enemy assembly areas.
- Locations of enemy indirect fire weapons 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 displaced civilians.
- Withdrawal routes of enemy forces.
- Locations of enemy command and information systems and ISR systems.
- Locations of potential integrated enemy or civilian assembly areas.
- Locations of friendly force assembly areas.



### *Defensive Operations*

**3-91.** *Defensive operations* are combat operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (FM 3-0). 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.

**3-92.** Intelligence should determine the enemy's strength and COAs, and the 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 AO. Intelligence support affords commanders the time necessary to commit the striking force precisely.

**3-93.** In defensive operations, CCIR tasked to GEOINT often include, but are not limited to—

- Locations, composition, equipment, strengths, and weaknesses of the advancing enemy force.
- Locations of enemy command posts, fire direction control centers, early warning sites, and target acquisition sensors.



FOR OFFICIAL USE ONLY

- Locations of possible enemy assembly areas.
- Locations of enemy indirect fire weapons systems and units.
- Locations of gaps, assailable flanks, and other enemy weaknesses.
- Locations of areas for enemy rotary wing and parachute assaults.
- Locations of artillery and air defense gun and missile units.
- Locations of enemy EW units.
- Location 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 displaced civilians.
- Locations of potential integrated enemy or civilian assembly areas.
- Locations of friendly force assembly areas.
- Weaknesses of defensive structure.
- Enemy force disposition.

### *Stability Operations*

**3-94.** *Stability operations* encompass various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0).

**3-95.** Missions where stability operations predominate are often more complex than those where offensive and defensive operations are dominant. Therefore, obtaining the intelligence required is often more complex. In stability operations, commanders often require more detailed intelligence and IPB products to determine how best to conduct operations and influence the local populace to enhance regional stability. The identification and analysis of the threat, terrain and weather, and civil considerations are critical in determining the most effective missions, tasks, and locations in which stability operations are conducted within the strict guidelines of U.S. law and focused on the specific missions directed by the Secretary of Defense.

**3-96.** Humanitarian assistance operations provide critical supplies and services. GEOINT support consists of locating refugee camps, water resources and their condition, and positions for water treatment assets. Imagery can determine soil permeability for effective field and public sanitation, tree availability for cooking and building needs, land availability, and local agricultural capabilities for food production. Additionally, the condition and location of ports, airfields, highways, and railroads can be obtained from imagery.



### *Civil Support Operations*

**3-97.** *Civil support* is Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities (JP 3-28). The Army National Guard (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 United States 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 (if applicable). The ARNG conducts civil support operations to meet 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. Once placed in Title 10 status, ARNG units must adhere to the same laws governing regular Army and Army Reserve operations.

**3-98.** Imagery collection must be planned during civil support operations to both adhere to the law and answer the CCIR. Careful planning of collection operations, with detailed instructions to the units and Soldiers involved, ensures collection operations do not violate U.S. law. GEOINT uses imagery and full motion video to provide products of the incident location or affected areas for federal agencies,


FOR OFFICIAL USE ONLY

first responders, and local law enforcement to use. Systems that provide real-time data and images can be positioned in incident command posts to provide video or imagery to incident commanders. ISR can be a valuable asset for assessing damage to infrastructure, locating populations at risk, and determining passable routes for first responders.

**3-99.** GEOINT products that support civil support operations include, but are not limited to—

- Detailed terrain analysis that incorporates weather to assist in determining potential COAs.
- Change detection products that track the extent of damage (including environmental damage).
- Updated imagery of the AO, for use by all agencies involved in the support operation, to monitor and assess the situation.
- Topographic surveys and map printing, hydrographic surveys, geomagnetic surveys, gravity surveys, medical facility information, and blue force tracking.
- Analysis of public health infrastructure, such as water, waste management, food provision, and medical treatment facilities.

**3-100.** Units and staff organizations performing intelligence activities may not infringe on, or violate the rights of U.S. persons. Collecting information on specific targets inside the U.S. raises policy and legal concerns that require careful consideration, analysis, and coordination with legal counsel. Collection must be in accordance with EO 12333, the National Security Act of 1947, as amended and DOD 5240.1-R. Acceptable reasons for domestic collection are—

- Natural disasters.
- CI.
- Protection of the force.
- Security-related vulnerability assessments.
- Environmental studies.
- Exercise.
- Training.
- Testing.
- Navigational purposes.

**3-101.** There are special considerations when using the following assets:

- National satellites. The National Geospatial-Intelligence Agency (NGA) is responsible for the legal review and approval of requests for the collection and dissemination of domestic imagery from national satellites.
- Airborne platforms. An approved proper use memorandum must be on file with the appropriate combatant command or military Service before airborne platforms can be tasked to collect domestic imagery.
- Commercial imagery. Intelligence components can obtain domestic commercial imagery without higher level approval for valid mission purposes. These include training or testing on federally owned and operated ranges, calibration-associated systems development activities, and domestic disaster relief operations.
- Unmanned aircraft systems. UASs used for navigational and target training activities may collect imagery during formal and continuation training missions as long as the collected imagery is in compliance with AR 381-10.

## Types of Geospatial Intelligence Products

**3-102.** GEOINT products usually incorporate intelligence analysis to ensure development of the most comprehensive product. However, customers do not always require or want analyzed products. Almost any type of GEOINT product can be produced without using intelligence analysis, for instance, using GEOINT as a base for visualization activities such as a COP. GEOINT products are generally categorized as either standard or specialized.





FOR OFFICIAL USE ONLY

### Standard Products

**3-103.** Standard products include geospatial data-derived products such as maps, charts, imagery, and digital raster or vector information. These products may be used alone or with layers of additional data, such as geographic data (vegetation, culture, languages, and weather) and intelligence information. Standard products are primarily derived from electro-optical sensors and existing geospatial data. They can also be derived from radar and multi-spectral sensors, but standard products do not routinely use these sources. The products are normally two-dimensional but can be processed into anaglyphs, which present a three-dimensional effect. Standard products satisfy a significant portion of GEOINT requirements.

### Specialized Products

**3-104.** Specialized products can provide additional information and enhance standard products, tailoring intelligence for a specific purpose. Specialized products may be developed using sophisticated technology to integrate multiple types of geospatial data, as well as data from other intelligence disciplines. Specialized products are typically derived from collection sources utilizing synthetic aperture radar (SAR), thermal infrared, multispectral imagery (MSI), light detection and ranging (LIDAR), and overhead persistent infrared (ONIR). Other sensor sources—such as EO, moving target indicator, and full-motion video—can contribute to the development of specialized products and data.

**3-105.** For more information on GEOINT see FM 2-0. Associated MOS or AOC are 12Y, 35G, 35H, 350G, 125Y 215D, and 35C.

## Imagery Intelligence

**3-106.** *Imagery intelligence* is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03). Imagery analysis is the science of converting information extracted from imagery into intelligence about activities, issues, objects, installations, and/or areas of interest. IMINT is a subdiscipline to GEOINT.

**3-107.** Imagery exploitation involves the evaluation, manipulation, and analysis of one or more images to extract information related to a list of essential elements of friendly information (EEFI). There are three phases of imagery exploitation: first phase, which is known as time-dominant, and second and third phases, which are non-time-dominant. The purpose of time-dominant exploitation (first phase) is to satisfy priority requirements of immediate significance and/or identify changes or activities of immediate significance. The purpose of second phase exploitation is to provide an organized and comprehensive account of the intelligence derived from validated intelligence requirements tasking. In the third phase, detailed, authoritative reports on specific installations, objects, and activities are prepared by the agencies participating in the exploitation effort (see JP 2-03).



## Role

**3-108.** IMINT assists commanders in applying and protecting their combat power and support operations. Imagery often enhances commanders' situational understanding. Imagery is also used for military planning, training, and operations that include navigation, mission planning, mission rehearsal modeling, simulation, and precise targeting. Imagery assets, particularly unmanned aircraft systems and moving target indicator systems, are useful in cueing other ISR systems. As with direct human observation, IMINT allows commanders to visualize the AO in near real time as the operation progresses. When maps are not available, hardcopy or softcopy versions of imagery can act as substitutes. Imagery can update maps or produce grid-referenced graphics. Detailed mission planning and IPB often require imagery, including three-dimensional stereo images, to provide the degree of resolution necessary to support specialized planning.


FOR OFFICIAL USE ONLY

## Capabilities

**3-109.** There are two general types of imagery collection platforms:
- Satellites comprise national technical means and commercial spaceborne platforms.
- Airborne systems comprise national, commercial, theater, and tactical systems.

### National Technical Means

**3-110.** National systems are developed to specifically support the President of the United States, the Secretary of Defense, other national agencies, and U.S. military forces. These systems respond to the needs of the nation and those of the combatant commands.

### Commercial Means

**3-111.** Commercial companies build, launch, and operate satellite and airborne imagery platforms for profit. In times of crisis, license agreements with the U.S. Government obligate U.S. commercial satellite imaging systems to provide data only to the U.S. Government at the market value. This protects information concerning U.S. operations from threat exploitation by commercial systems such as Google Earth. However, the U.S. Government cannot afford to buy all the commercial imagery available for a crisis, and foreign commercial imagery systems are not bound to this arrangement. Therefore, the nation's enemies and adversaries may use these imagery sources. Commercial imagery has become increasingly valuable for many reasons:
- Due to the unclassified nature of civil and commercial imagery, the imagery is useful in an open environment and may be released to other government agencies, intergovernmental organizations, NGOs, and multinational partners. Civil and commercial imagery 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 EO and radar imagery. Some offer large area collection that is useful for broad area coverage purposes, normally at a reduced resolution.

**3-112.** The NGA Source Directorate is responsible for ordering commercial imagery. The Unclassified National Imagery Library is available to research DOD-purchased commercial imagery. Intelligence personnel should consult the NGA Source Directorate when forming commercial imagery requests.



### Theater Means

**3-113.** Theater reconnaissance assets provide medium- to high-resolution imagery coverage to combatant commands, joint task forces, or major component commands. They serve to fill the gaps in coverage from national-level assets. The primary purpose of these assets is to support theater-level operations by providing imagery coverage of those gaps in national-level assets. Theater imagery collection assets generally have more standoff capability than tactical-level assets and therefore are capable of detecting, tracking, and designating targets at a greater distance than tactical assets. This helps ensure greater survivability of these assets. Theater-level assets also support tactical operations when tactical collection assets are unavailable. Theater combined air operations centers hold approval authority for theater assets.

### Tactical Means

**3-114.** Tactical commanders are engaged in the close fight and therefore have unique intelligence requirements. Tactical collection assets are used to designate and collect on tactical level targets within commanders' AOs. These assets are used to answer intelligence requirements such as the enemy's current disposition and the enemy's defensive preparations on or near friendly objectives. Tactical collection assets are organic to tactical commanders and therefore are extremely responsive to their collection requirements.


FOR OFFICIAL USE ONLY

## Types of Imagery Sensors

**3-115.** There are two general types of imagery sensors: Electro-optical (EO) and radar.
EO sensors include—

- Panchromatic (visible).
- Infrared.
- Spectral (multispectral, hyperspectral, and ultraspectral).
- Polarmetric.
- LIDAR.

**3-116.** Radar sensors are synthetic aperture radar systems that collect and display data either as representations of fixed targets or as moving target indicators.

**3-117.** Each sensor and platform has a unique capability, with distinct advantages and disadvantages. Successful intelligence personnel understand the capability of each sensor and platform so as to make the best selection for the mission, enabling users to better understand the intelligence received. Certain sensors are better suited for military operations than others.

## Fundamentals

**3-118.** Some imagery assets are very responsive to individual CCIRs. Some tactical and theater imagery collection platforms can transmit imagery data directly into the command posts. Examples include data from UASs, the Joint Surveillance Target Attack Radar System, and Airborne Reconnaissance Low. This direct downlink enables intelligence personnel to exploit the imagery as soon as possible instead of waiting 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.

**3-119.** Imagery-related equipment has been reduced in size. The modularity and size reduction of imagery analysis, processing, and display systems facilitates transport. This allows commanders to deploy with less equipment while retaining capabilities and systems required to complete the mission. Imagery considerations include communications bandwidth, product classification, releasability, and equipment and software for imagery analysts to perform their mission. Data compression allows faster transmission of imagery products directly to the warfighter.

## Planning

**3-120.** Determining requirements is the first step in planning for IMINT. The staff must clearly articulate the intelligence requirements. This includes communicating what the mission is and how the requested product will aid in mission accomplishment. Intelligence personnel submit the imagery, collection, and production requirements in the Geospatial Intelligence Management System using established procedures, such as those in unit standing operating procedures (SOPs) or as established by the combatant command.

**3-121.** Intelligence personnel must also determine specific imagery requirements to avoid burdening the system with unnecessary requests. The demand for imagery products often exceeds the capabilities of the imaging system. It is imperative that intelligence personnel consider the type of analysis needed and request only what is required. The specifications of the request for IMINT products often affect the timeliness of the response. For example, determining if vehicles are tanks requires less time and resolution than determining the make, model, and tank capabilities.




FOR OFFICIAL USE ONLY

## Types of Products

**3-122.** IMINT products include—

- Imagery that detects and/or identifies and locates specific unit types, equipment, obstacles, and potential field fortifications—imagery from which intelligence analysts can assess enemy capabilities and develop possible COAs.
- Imagery that updates maps and enhances the interpretation of information from maps. Detailed mission planning uses imagery, including draping imagery over digital terrain elevation for three-dimensional viewing of the terrain.
- Full-motion video displays or products that often provide a real-time picture of an object's movement by indicating its speed, location, and direction of travel. These systems do not differentiate friendly from enemy forces.
- Imagery that supports protection of the force by helping commanders visualize how their forces look—including their disposition, composition, and vulnerabilities—as seen by enemy IMINT systems.
- Target packets with imagery of HVTs and HPTs that include critical elements of the targets and potential collateral damage.
- Imagery that supports combat assessment to confirm damage, determine the percentage of damage, or establish whether the target was unaffected.
- Advanced GEOINT products that can determine change detection, specific weapon system identifications, chemical compositions and material content, and a threat's ability to employ these weapons.

**3-123.** For more information on IMINT see FM 2-0. Associated MOSs/AOCs are 35G, 35H/350G, and 35C.

# MEASUREMENT AND SIGNATURE INTELLIGENCE

**3-124.** *Measurement and signature intelligence* (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 reflected or emitted (JP 2-0).



## Role

**3-125.** MASINT provides intelligence to commanders 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.

**3-126.** By applying near real-time analysis and dissemination, MASINT has a potential to provide timely situational awareness and targeting that is not necessarily available through other disciplines. MASINT sensors have unique capabilities to detect missile launch; detect and track aircraft, ships, and vehicles; perform noncooperative target identification and combat assessment; and detect and track fallout from nuclear detonations. Often, these are the first indicators of hostile activities.

**3-127.** The most familiar MASINT systems used today are employed by ground surveillance and chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) reconnaissance elements. MASINT spans the entire electromagnetic spectrum. Its capabilities complement the other intelligence disciplines. MASINT provides, to varying degrees, the capability to—



FOR OFFICIAL USE ONLY

- Use automatic target recognition and aided target recognition.
- Penetrate manmade and natural camouflage.
- Penetrate manmade and natural cover, including the ability to detect subterranean anomalies or targets.
- Counter stealth technology.
- Detect recently placed mines.
- Detect natural or manmade environmental disturbances on 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 before, during, or after employment.

**3-128.** Detect signature anomalies that may affect target-sensing systems.

## Capabilities

**3-129.** MASINT collection systems include but are not limited to radar, spectroradiometric, EO, acoustic, radio frequency, nuclear detection, and seismic sensors. The systems are also able to collect CBRNE signatures and other materiel samples.

**3-130.** MASINT requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communications, data, and display processing technologies now provide MASINT to support operations.

**3-131.** 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.
- **Radio frequency.** The collection, processing, and exploitation of electromagnetic emissions from a radio frequency emitter, radio frequency weapon, radio frequency weapon precursor, or a radio frequency 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.
- **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 EO capabilities provide detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the material composition of a target. EO data collection has broad application to a variety of military, civil, economic, and environmental targets. EO sensor devices include radiometers, spectrometers, nonliteral imaging systems, lasers, or laser detection and ranging systems.
- **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.
- **Nuclear radiation.** 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 on site inspections of nuclear facilities. Data exploitation results in the characterization of nuclear weapons, reactors, and materials. A number of systems detect and monitor the world for nuclear explosions, as well as for nuclear materials production.
- **Materials.** The collection, processing, and analysis of gas, liquid, or solid samples is a MASINT




FOR OFFICIAL USE ONLY

subdiscipline. Intelligence derived from materials is critical to collection against CBRNE threats. It is also important to analyzing military and civil manufacturing activities, public health concerns, and environmental problems. Samples are collected by automatic equipment, such as air samplers, and directly by humans. Samples, once collected, may be rapidly characterized or they may undergo extensive forensic laboratory analysis to determine the identity and characteristics of the sources of the samples.

## Fundamentals

**3-132.** Within DOD, the Defense Intelligence Agency (DIA) provides policy and guidance for MASINT. While DIA provides policy and guidance for MASINT, the policy and guidance do not interfere with Service component operations. Each Service has a primary command or staff activity that develops requirements and coordinates MASINT efforts. 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 U.S. Army Intelligence and Security Command (INSCOM) channels for data collection and processing.

**3-133.** The scientific and technical intelligence community also performs MASINT collection and processing, primarily to support research programs and signature development. Service research and development centers such as the Communications-Electronics Command Research, Development, and Engineering Center; the Army Research Laboratory; and the Night Vision and Electronic Systems Laboratory are involved in developing sensor systems for collecting and processing MASINT.

**3-134.** In addition to supporting the scientific and technical intelligence mission, INSCOM units also execute limited ground-based operational collection to support ASCCs and subordinate units.

## Planning

**3-135.** 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. These varying capabilities require synchronization in the employment of MASINT sensors, both within the MASINT discipline and within the ISR effort as a whole.

**3-136.** Depending on the type of sensor employed, a given MASINT collection target or named area of interest 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, commanders may decide to have continuous surveillance of certain targets by using available MASINT assets. Another consideration when planning MASINT missions is whether to use active, passive, or a combination of sensors when planning MASINT coverage—decisions that are all 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 to monitor sensor reports.

## Products

**3-137.** Effective and timely MASINT requires personnel with diverse skill sets. The successful MASINT producer ensures 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 depend upon the type of target, the collection system, the system's position in relation to the target,





FOR OFFICIAL USE ONLY

the weather, and the system operator's ability. The objective of MASINT production is to develop products useable in all-source intelligence.

**3-138.** For more information on MASINT see FM 2-0. The Army does not have a specific MOS, AOC, additional skill identifier, or special qualification identifier for MASINT.

## OPEN-SOURCE INTELLIGENCE

**3-139.** *Open-source intelligence* is the discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (FM 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 and publicly available information:

- Open source is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.
- Publicly available information is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

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

### Role

**3-140.** 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 the generate intelligence knowledge continuing activity of the intelligence process 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.

### Capabilities

**3-141.** The Army does not have a specific MOS, additional skill identifier, or special qualification identifier for OSINT. The Army does not have a table of organization and equipment for OSINT units or staff elements. OSINT missions and tasks are contained within existing missions and force structures or are accomplished through task organization.

**3-142.** The collectors of Army OSINT are the MI brigades. Each of these INSCOM units performs sustained, regionally focused intelligence operations to support 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 area of responsibility. When open-source skills and regional knowledge are not present in these deploying tactical units, personnel from the MI brigade 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.

**3-143.** For the most part, the considerations for OSINT are similar to those of other intelligence




FOR OFFICIAL USE ONLY

disciplines:

- OSINT organizations need clearly stated intelligence requirements to effectively focus collection and production.
- OSINT operations must comply with AR 381-10 and EO 12333 on the collection, retention, and dissemination information on U.S. 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.

## Fundamentals

**3-144.** OSINT differs 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 nonintrusive. Other intelligence disciplines use confidential sources or intrusive techniques to collect private information. Key concepts associated with OSINT include confidential sources and private information:

- A confidential source 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 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:
  - Controlled unclassified information requires the application of controls and protective measures, for a variety of reasons.
  - Classified information requires protection against unauthorized disclosure and is marked to indicate its classified status when in written or viewable form.

**3-145.** The following characteristics describe the role of publicly available information and OSINT in Army operations:

- Provides the foundation.
- Answers requirements.
- Enhances collection.
- Enhances production.



### Provides the Foundation

**3-146.** The U.S. social structures, education system, news services, and entertainment industry shape worldview, awareness of international events, and perceptions of non-U.S. societies. This foundation can be an essential part of the generate intelligence knowledge continuing activity of the intelligence process.

### Answers Requirements

**3-147.** The availability, depth, and range of public information enable intelligence and nonintelligence organizations to satisfy many of the CCIRs, PIRs, friendly force information requirements (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 often proceed directly from the planning step to the production step of the intelligence process.

### Enhances Collection

**3-148.** Open-source research and collection support other surveillance and reconnaissance activities by answering requirements and providing foundational information such as biographies, cultural information, geospatial information, and technical data. This optimizes the employment and performance of sensitive human and technical means of collection.

### Enhances Production

**3-149.** As part of single-source and all-source intelligence production, the use and integration of OSINT ensures commanders have the benefit of all available information.



FOR OFFICIAL USE ONLY

## Planning

**3-150.** Personnel responsible for conducting (planning, including design; preparing; executing; and assessing) OSINT operations must also consider the following concerns:

- Compliance.
- Limitations.
- OPSEC.
- Classification.
- Deconfliction.
- Deception and Biass.
- Intellectual property.

### Compliance

**3-151.** Under AR 381-10, procedure 2, Army intelligence activities may collect publicly available information on U.S. persons only when it is necessary to fulfill an assigned function. There must also be a link between the collection of the U.S. 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, Web addresses, and e-mail addresses that are not self-evidently associated with a U.S. person may be acquired, retained, and processed by Army intelligence components without making an effort to determine whether they are associated with a U.S. 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 is associated with a U.S. person.

### Limitations

**3-152.** 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, DODD 5100.20 prohibits SIGINT organizations from collecting and processing information from public broadcasts, with the exception of processing encrypted or "hidden meaning" passages. AR 380-13 prohibits the assignment of Army, military, or civilian personnel 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 of Defense or the Undersecretary of the Army.

### Operations Security

**3-153.** More than any other intelligence discipline, the OSINT discipline could unintentionally provide indicators of U.S. 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 U.S. 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 U.S. plans and operations.

**3-154.** 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 U.S. 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.




FOR OFFICIAL USE ONLY

### Classification

**3-155.** 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 3-1, 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 3-1. Open-source intelligence classification considerations**

| *If:* | | *Then:* | | | |
|---|---|---|---|---|---|
| *Information source is:* & | *Collection means is:* | *Source metadata are:* & | *Collector metadata are:* & | *Collected information is:* & | *Intelligence report is:* |
| Confidential | Overt | Classified or controlled unclassified & | Classified or controlled unclassified & | Classified or controlled unclassified & | 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 source in accordance with the policy and procedures in AR 380-5.



### Deconfliction

**3-156.** During planning, both the intelligence and operations staffs 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 nonintelligence organizations such as civil affairs, MP, medical, and public affairs to accomplish their missions. Conversely, those 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 inability to obtain information of intelligence value.

### Deception and Bias

**3-157.** Deception and Biass 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 U.S. 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 to distinguish objective, factual information from information that lacks merit, contains bias, or is part of an effort to deceive the reader.



FOR OFFICIAL USE ONLY

**3-158.** 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 locally hired when deployed overseas, and many civilian interpreters do not have security clearances.

### Intellectual Property

**3-159.** AR 27-60 prescribes policy and procedures for the acquisition, protection, transfer, and use of patents, copyrights, trademarks, and other intellectual property by the Department of the Army. 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 U.S. Copyright Law or is required to meet an immediate, mission-essential need for which noninfringing alternatives are either unavailable or unsatisfactory.

**3-160.** According to the U.S. 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 nonprofit 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 a 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 by the owner's terms of use or described in contracts and licenses with the U.S. Government.

## Open Sources and Information

**3-161.** 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 nongovernmental organizations.** 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.** Broadcast, 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 broadcast information, including art, graffiti, leaflets, posters, and Web sites.

## Open-Source Media

**3-162.** 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 3-2 and discussed below.




FOR OFFICIAL USE ONLY

**Table 3-2. Primary open-source media**

| System | Components | Elements | |
|---|---|---|---|
| **Public speaking** | Speaker | • Sponsor<br>• Relationship | • Message |
| | Format | • Conference<br>• Debate<br>• Demonstration | • Lecture<br>• Rally |
| | Audience | • Location | • Composition |
| **Public documents** | Graphic | • Drawing<br>• Engraving<br>• Painting | • Photograph<br>• Print |
| | Recorded | • Compact data storage device<br>• Digital video disk | • Hard disk<br>• Tape |
| | Printed | • Book<br>• Brochure<br>• Newspaper | • Periodical<br>• Pamphlet<br>• Report |
| **Public broadcasts** | Radio | • Low frequency AM radio<br>• Medium frequency AM radio | • VHF FM radio<br>• L- and S-band satellite radio |
| | Television | • Ku-band satellite television<br>• VHF and UHF terrestrial television | |
| **Internet sites** | Communications | • Chat<br>• E-mail<br>• News; newsgroup | • Web cam<br>• Web cast<br>• Web log |
| | Databases | • Commerce<br>• Education | • Government<br>• Military organizations |
| | Information (Web page content) | • Commerce<br>• Education | • Government<br>• Military organizations |
| | Services | • Dictionary<br>• Directory<br>• Downloads<br>• Financial | • Geospatial<br>• Search and URL lookup<br>• Technical support<br>• Translation |

| | | | |
|---|---|---|---|
| AM | amplitude modulation | S-Band | 2 to 4 gigahertz |
| FM | frequency modulation | UHF | ultrahigh frequency |
| Ku-band | 11.7 through 14.5 gigahertz | URL | uniform resource locator |
| L-Band | 40 and 60 gigahertz | VHF | very high frequency |



## Public Speaking Forums

**3-163.** 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 scientific and technical 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 states:

> *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.*

**3-164.** If invoked, privacy conditions such as the Chatham House Rule change the characterization of



FOR OFFICIAL USE ONLY

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, public speaking events are monitored through direct observation and, due to the overt nature, could entail risk to the collector.

## Public Documents

**3-165.** 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 underpins the ability to plan, prepare, 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. Documents detailing the operational and technical characteristics of foreign materiel aid in development of improved U.S. tactics, countermeasures, and equipment.

## Public Broadcasts

**3-166.** 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 or radio broadcasts often provide the first I&W of situations that may require the use of U.S. 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 United States and its military operations. Broadcasts also provide information and insights into the effectiveness of information tasks.

## Internet Sites

**3-167.** 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).

**3-168.** 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 a 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.

**3-169.** Collectors can monitor newspaper, radio, and television Web sites that support assessments of information tasks, especially information engagement. Collectors can perform periodic searches of Web pages and databases for content on threat characteristics. Collecting Web page content and links can provide useful information about relationships between individuals and organizations. Properly focused, collecting and processing publicly available information from Internet sites supports understanding of the operational environment.

### Types of Intelligence and Products

**3-170.** 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.

**3-171.** AR 380-5, chapter 6, provides a list of factors or classification considerations that include, but is not limited to the following:

- Intelligence that reveals the identity of a conventional source or method 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.
- Intelligence requirements that reveal what is not known, what is necessary to know, and why.
- 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 installations there.

> ***Note.*** The intelligence staff creates sanitized, unclassified collection tasks from the intelligence requirements, since uncleared U.S. and non-U.S. persons makeup a significant portion of open-source collectors.

**3-172.** For more information on OSINT see FMI 2-22.9. The Army does not have a specific MOS, AOC, additional skill identifier, or special qualification identifier for OSINT.

## SIGNALS INTELLIGENCE

**3-173.** *Signals intelligence* is intelligence derived from communications, electronic, and foreign instrumentation signals (JP 2-0). SIGINT provides unique intelligence information, complements intelligence derived from other sources, and is often used for cueing other sensors to potential targets of interest. For example, SIGINT that 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).
- Foreign instrumentation signals intelligence (FISINT).



### Communications Intelligence

**3-174.** *Communications intelligence* is technical information and intelligence derived from foreign communications by other than the intended recipients (JP 2-0). COMINT includes cyber operations, 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.

### Electronic Intelligence

**3-175.** *Electronic intelligence* is technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 3-13.1). ELINT consists of two subcategories—operational ELINT (OPELINT) and technical ELINT (TECHELINT).



FOR OFFICIAL USE ONLY

- 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.

## Foreign Instrumentation Signals Intelligence

**3-176.** *Foreign instrumentation* signals intelligence is technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links (JP 2-01).

## Role

**3-177.** SIGINT provides intelligence on threat capabilities, disposition, composition, and intentions. In addition, SIGINT provides targeting information for the delivery of lethal and nonlethal fires.

## Capabilities and Fundamentals

**3-178.** The successful intelligence professional understands how SIGINT assets are organized, not only within the Army but also throughout the 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.

## National to Tactical Signals Intelligence Relationships

**3-179.** Tactical Army SIGINT elements rely heavily on the National Security Agency (NSA) for many integrated functions and, conversely, NSA relies on tactical resources for intelligence. These functions and interfaces include NSA network connectivity to perform analytic and data exchanges, as well as connect with databases. NSA supports Army SIGINT collectors and analysts with specific SIGINT equipment and tools.

**3-180.** The SIGINT technical architecture complements existing command 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 (ACO).
- Army Technical Control and Analysis Element (ATCAE).
- Theater technical control and analysis element (TCAE).
- Army SIGINT systems.

### Army Cryptologic Operations

**3-181.** ACO, an element of INSCOM G-3, is located within NSA and acts as the Army's Service cryptologic element representative. ACO supports Army cryptologic operations, capabilities, and resourcing to provide dominant strategic and operational SIGINT, information assurance, and the Army information tasks. ACO supports ground component commanders, national agencies, and national decisionmakers. The ACO provides SIGINT quick reaction capability systems. ACO works closely with NSA and other Service cryptologic elements to leverage the SIGINT enterprise, improve sensor capabilities, and provide technical and analytical support to Army SIGINT elements.




FOR OFFICIAL USE ONLY

### Army Technical Control and Analysis Element

**3-182.** ATCAE, established at national level, plays a significant role in TCAE operations by providing technical support oversight and coordinating issues, such as obtaining approvals for NSA connectivity and access to national databases for U.S. Army tactical SIGINT personnel. The ATCAE is located within the NSA complex at Fort Meade, Maryland, and represents the Army Deputy Chief of Staff for Intelligence on SIGINT technical matters involving Army SIGINT elements.

**3-183.** ATCAE works closely with ACO, providing SIGINT technical and analytical support of the Army's special sensor capabilities. The special sensor capability systems respond to the ground force commander's requirements and enable SIGINT personnel to perform SIGINT operations.

**3-184.** ATCAE provides 24-hour service through its 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, the TROJAN program, and SIGINT Foundry assets.
- Electronic quality control of unit reporting and forwarding to national time-sensitive systems.
- Assistance in obtaining SIGINT communications network connectivity and access to national assets, including databases.
- Assistance in reviewing and recommending modifications to U.S. SIGINT directives on behalf of the tactical ground units' SIGINT technical issues.

### Theater Technical Control and Analysis Element

**3-185.** The theater TCAE performs SIGINT technical control and analysis and management. It provides SIGINT technical support for assigned, attached, operational control, and lower echelon SIGINT resources deployed in the area of responsibility. This support includes mission tasking, processing, analysis, and reporting of SIGINT data, information, and intelligence. The TCAE provides direction for the theater collection and exploitation battalion's SIGINT mission and for other theater tactical SIGINT assets.



### Army Signals Intelligence Systems

**3-186.** SIGINT elements at echelons corps and below perform actions to search for, intercept, and identify threat signals for the purpose of immediate recognition. This provides information required to answer PIRs and other intelligence requirements to support the ISR effort. For more information on SIGINT assets, see chapter 6.

## Electronic Warfare Support

**3-187.** *Electronic warfare* refers to any military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the adversary (JP 3-13.1). 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 ground force commanders. These assets 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, preparation, execution and assessment of future operations, and other tactical actions such as threat avoidance, targeting, and homing. (See JP 3-13.1.)



FOR OFFICIAL USE ONLY

**3-188.** ES is intended to respond to immediate commanders' requirements. 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 requirements. Intelligence collected for ES purposes is normally also processed by the appropriate parts of the intelligence community for further exploitation after the commander's ES requirements are met. (See JP 3-13.1.)

**3-189.** 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. For example, ES data can be used to produce SIGINT; this provides intelligence information for electronic or lethal attack or targeting.

### Planning

**3-190.** Intelligence officers should plan to employ SIGINT assets in conjunction with the collection systems of other intelligence disciplines. SIGINT assets often cue, and are cued by, other ISR assets. During planning, the SIGINT TCAE 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 as SIGINT assets that will operate in another unit's AO.

**3-191.** Associated MOS/AOC are 35N, 35P, 35S, 35Z/352N, 100 352P, 352S, and 35G.

## TECHNICAL INTELLIGENCE

**3-192.** *Technical intelligence* 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).

**3-193.** TECHINT ensures that Soldiers understand the full technological capabilities of the threat. With this understanding, U.S. forces can adopt appropriate countermeasures, operations, and tactics.



**3-194.** TECHINT has three goals:
- Ensure U.S. armed forces maintain technological advantage against any threat.
- Provide timely, relevant, accurate, predictive, and tailored TECHINT support to the Soldier throughout the spectrum of conflict, including using captured enemy materiel (CEM) to provide U.S. forces intelligence, information, and training on foreign weapons systems.
- Analyze certain design traits of foreign weapons systems to develop, confirm, or deny indicators of threat intent.

**3-195.** TECHINT includes the subset of weapons technical intelligence (WTI), which is intelligence derived from the forensic and technical collection and exploitation of improvised explosive devices (IEDs), associated components, improvised weapons, and other weapons system. WTI has four goals:
- 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.
- Enable targeting by identifying, selecting, prioritizing, and tracking individuals and matching them with groups, weapons materiel, financiers, suppliers, insurgent leaders, and other related elements.
- Provide limited forensic analysis of IEDs, improvised weapons, and weapon components to identify the origin of materiel and components.
- Use information from CEM collected during site exploitation to further detain, and potentially support prosecution of, individuals for criminal activity.


FOR OFFICIAL USE ONLY

## Fundamentals

**3-196.** The fundamentals of TECHINT consist of TECHINT application in operations and the importance of the chain of custody.

### TECHINT Application

**3-197.** TECHINT assets can respond to threats across the spectrum of conflict. Their capabilities are best suited to meet the needs of commanders during offensive and defensive operations. For example, the equipment used in these operations consists of traditional threat weapons systems. TECHINT assets are capable of identifying indicators of new weapons, improved munitions, or modifications that could potentially defeat U.S. equipment.

**3-198.** Knowledge gained through TECHINT exploitation and analysis also supports stability operations—often through intelligence reach. Unlike conventional warfare, threat forces are not easily identified, and often nontraditional threats take refuge in plain sight. TECHINT 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 attack U.S. forces.

**3-199.** TECHINT and WTI can be used simultaneously when commanders anticipate or encounter a mixed set of threats. The unique WTI capabilities can be scaled to complete missions during offensive and defensive operations. (See TC 2-22.4.)

### Chain of Custody

**3-200.** Proper documentation of CEM is a key factor in producing accurate and relevant TECHINT for commanders. For example, linking the capture location, details of employment, and the list of associated CEM can yield significant exploitable information.

**3-201.** Specifically, the proliferation of weapons from nation states and nonstate actors can reveal third-party influences. Properly recorded weapons emplacement can identify the effectiveness of weapons against U.S. forces. Additionally, proper chain of custody is necessary in linking individuals and threat networks with weapons and materiel and events. The information gained through exploitation may eventually be used in U.S. or host-nation legal proceedings.



## Planning

**3-202.** Based on the information or intelligence from the generate intelligence knowledge continuing activity, the intelligence officer 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. TECHINT planning considerations include—

- Task-organizing ground reconnaissance units with TECHINT teams or weapons intelligence teams to employ forensics capabilities.
- Linguists for translation and transliteration.
- Intelligence reach capability to access and query databases and knowledge center analysts.
- IPB, including identification of named areas of interest and target areas of interest.
- Joint capabilities ISR, including special operations forces.

**3-203.** As mission requirements change, TECHINT planning is synchronized with operations.



FOR OFFICIAL USE ONLY

## Types of Intelligence and Products

**3-204.** TECHINT teams normally report initial and secondary examinations of CEM using either a preliminary technical report or a complementary technical report.

**3-205.** A preliminary technical report—
- Includes a general description of the item.
- Alerts others to information that can be used immediately by tactical units.

**3-206.** A complementary technical report is more detailed and—
- Follows a secondary or an in-depth initial examination.
- Allows comparison of new information to current intelligence holdings.

**3-207.** At each successive echelon of exploitation, TECHINT analysts contribute to the overall body of information on an item by either adding to previous reports or by preparing new reports. National-level scientific and TECHINT activities prepare more advanced technical reports and analyses. These reports include—
- Detailed technical reports.
- TECHINT update report.
- TECHINT summary.
- Translation reports.
- Special technical reports.

**3-208.** Other TECHINT products include—
- Publications such as operator manuals, maintenance manuals, TECHINT bulletins, and tactical user bulletins.
- Scientific and technical intelligence analysis bulletins.
- Foreign materiel exploitation reports.
- Weapons intelligence team reports.

**3-209.** For more information on TECHINT see TC 2-22.4. The Army does not have a specific MOS, AOC, additional skill identifier, or special qualification identifier for TECHINT.




FOR OFFICIAL USE ONLY

# Chapter 4
# Intelligence Operations

## INTRODUCTION

**4-1.** This chapter introduces the following fundamentals: intelligence and the operations processes; how intelligence drives operations; the tenets of intelligence; the intelligence process; intelligence preparation of the battlefield (IPB); intelligence, surveillance, and reconnaissance (ISR) planning considerations, and intelligence support to targeting and operations security.

## INTELLIGENCE AND THE OPERATIONS PROCESS

**4-2.** Commanders use the operations process of plan (including design), prepare, execute, and assess to continuously design and conduct operations. Commanders cannot successfully accomplish activities involved in the operations process without information and intelligence. The design and structure of intelligence operations support commanders' operations process by providing them with the intelligence needed in order to drive operations.

**4-3.** Soldiers should be able to operate effectively in the uncertain, chaotic, complex, and fluid environment of modern conflicts. The Army philosophy for winning under these conditions is based on rapid, flexible, and opportune maneuver. The concepts central to executing operations are—

- **Orienting on the enemy.** Maneuver warfare attacks the enemy system, the combination of physical, moral, and mental components that make up an enemy or an opposition force. This means focusing on the particular characteristics of the enemy.
- **Commander's intent.** Commander's intent describes the purpose behind the task assigned in a mission. (See FM 6-0.) When the tactical situation changes, the commander's intent provides continuing guidance and permits subordinates to exercise initiative in harmony with the commander's desires.
- **Mission command.** Mission command assigns subordinates a task without specifying how that task must be accomplished. Mission tactics permit subordinates to exercise initiative in adapting to changing situations.
- **Tempo.** Tempo keeps the enemy off balance, increasing friction. Speed, initiative, and flexibility generate and maintain a tempo that the enemy cannot match.

**4-4.** The operations process and the intelligence process are mutually dependent. The commander provides the guidance and focus through commander's critical information requirements (CCIRs), priority intelligence requirements (PIRs), and friendly force information requirements (FFIRs) that drive the operations and intelligence processes. The intelligence process operates throughout the operations process, providing the continuous intelligence essential to the operations process. Intelligence about the area of operations (AO) and area of interest 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 of the operations processes and will be discussed later in this chapter. (See FM 3-0 for a further discussion of the integrating processes.)

## INTELLIGENCE DRIVES OPERATIONS

**4-5.** The role intelligence plays in operations cannot be overstated. Intelligence provides insights concerning exploitable opportunities to defeat the adversary and helps the commander clearly define





FOR OFFICIAL USE ONLY

the desired end state and when that end state has been achieved.

**4-6.** The most important role intelligence plays is assisting commanders and their staffs in visualizing the AO. Visualization includes more than having knowledge of the physical and manmade characteristics of the AO. It requires knowing the current dispositions and activities of adversary forces in that space as well as their current and future capabilities. More importantly, visualization requires an understanding of the objectives of threat forces.

**4-7.** Determining the intent of adversary leaders is one of the most difficult challenges confronting intelligence. The key factor that makes determining intent so difficult is the process of action and reaction that will occur between a joint force and its adversary. Friendly actions or even preparations may, if detected, cause a reaction by the adversary. This has been referred to as the "process of interaction." Estimating the outcome of the process of interaction requires the S-2, G-2, or J-2 to know what future friendly actions are planned and to simultaneously forecast many different scenarios involved in the actions.

**4-8.** During peacetime operations, intelligence helps commanders make acquisition choices, protect technological advances, shape organizations, and design training to ready the joint force. Intelligence assets monitor foreign states and volatile regions to identify threats to U.S. interests in time for the President to respond effectively, efficiently, and in a manner consistent with U.S. values. Information shortfalls are identified and eliminated. Intelligence units are employed or deployed as early as directed to support U.S. initiatives and assist multinational partners.



**4-9.** Intelligence helps the commander decide which forces to deploy; when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission at the lowest human and political cost. Although peacetime intelligence supports the effort to reduce or eliminate sources of conflict, it constantly prepares for escalation to war.

**4-10.** During wartime, intelligence can inform the commander of what the adversary's information capabilities are and where and when the information differential can be exploited. Intelligence tells the commander what the adversary's centers of gravity are. Intelligence assists the operational planner in identifying the best means for attacking or exploiting the enemy centers of gravity (courses of action [COAs]). Intelligence enables the commander to focus and leverage combat power and to determine acceptable risk. Intelligence is the key to allowing the commander to achieve powerful, dynamic concentrations where the adversary is vulnerable. In wartime, it is important that support be anticipatory and precise. Intelligence must maximize and synchronize its support to the commander while minimizing the demands made on the commander and staff.

## TENETS OF INTELLIGENCE

**4-11.** Effective intelligence is the fundamental standard against which the performance of intelligence personnel and organizations are judged. A failure to achieve any of these fundamental attributes may contribute to a failure of operations. The bottom line is whether the PIRs are being satisfied. See figure 4-1.



FOR OFFICIAL USE ONLY

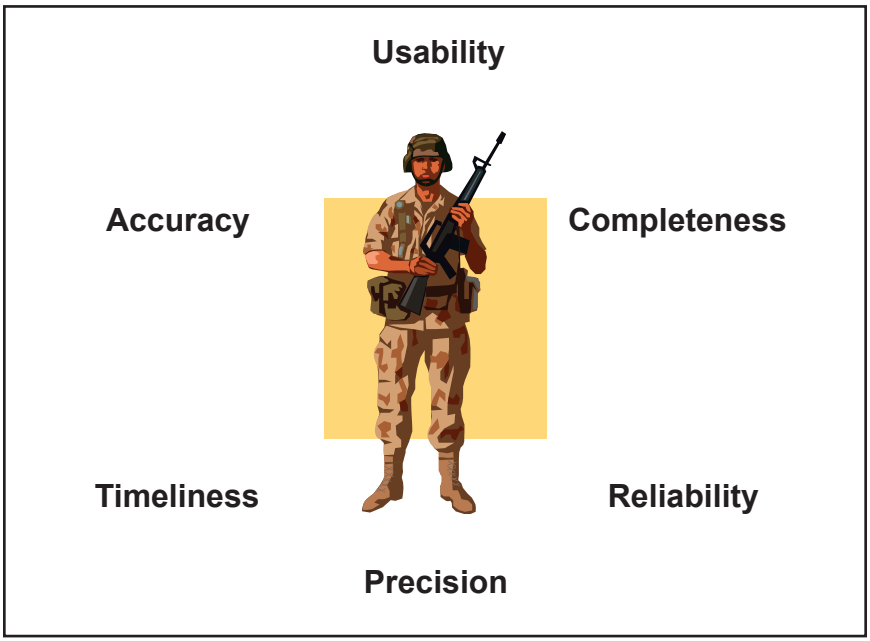



Figure 4-1. Tenets of intelligence



4-12. 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 other aspects of the AO. To the extent possible, intelligence accurately identifies threat intentions, capabilities, limitations, and dispositions. It is derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Intelligence is presented in alternative or contradictory assessments, when necessary, to ensure balance and bias-free intelligence.
- **Timeliness.** Intelligence must be provided early 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.** Present intelligence 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. Completeness is frequently driven by time constraints—the 60 percent answer now may be more useful than the 90 percent answer that comes too late.
- **Precision.** Intelligence briefings and products must provide only the required level of detail and complexity to answer the requirements.
- **Reliability.** Intelligence is 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. Any concerns with these must be stated up front.

4-13. Effective intelligence meets three additional criteria:

- **Relevant.** Intelligence must support the commander's concept of operations. It must be relevant



FOR OFFICIAL USE ONLY

to the capabilities of the unit, the CCIRs, and the commander's preferences.

- **Predictive.** Intelligence should inform the commander about what the threat can do (threat capabilities, emphasizing the most dangerous threat COA) and is most likely to do (the most likely threat COA). The intelligence staff should anticipate the commander's intelligence needs.
- **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 commander's priorities.

## LEVELS OF INTELLIGENCE

**4-14.** Levels of intelligence must be taken into account. There are three levels of war: strategic, operational, and tactical. The levels are a doctrinal construct that explains the links between strategic objectives and tactical actions. The levels of war assist commanders in visualizing a logical flow of operations, allocating resources, and assigning tasks. The levels of intelligence mirror the levels of war.

### Strategic Intelligence

**4-15.** Strategic intelligence is produced for the President, senior military leaders, and the combatant commanders. It is used to create national strategy and policy, monitor the international situation, prepare military plans, determine the need for major weapon systems and force structure requirements, and to conduct strategic operations.



### Operational Intelligence

**4-16.** Operational intelligence is primarily used by combatant and subordinate commanders and their component commanders. Operational intelligence focuses on the military capabilities and intentions of adversaries and potential adversaries. It keeps commanders abreast of events within their areas of responsibility and determines when, where, and in what strength the adversary will stage and conduct campaigns and major operations. Within the area of responsibility, operational intelligence addresses all operational themes, including peace operations and irregular warfare.

### Tactical Intelligence

**4-17.** Tactical intelligence is used by tactical-level commanders in battles and engagements. Tactical intelligence locates the adversary's forces and weapons systems, enhancing the tactical commander's ability to shape the AO using maneuver, fires, and obstacles. Accurate, timely intelligence allows tactical units to achieve positional advantage over their adversaries. Tactical intelligence addresses the adversary across the spectrum of conflict.

## THE INTELLIGENCE PROCESS

**4-18.** The intelligence process consists of four steps 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 continuing activities occur continuously throughout the intelligence process, which is continuously guided by the commander's input. Figure 4-2 shows the intelligence process.



FOR OFFICIAL USE ONLY

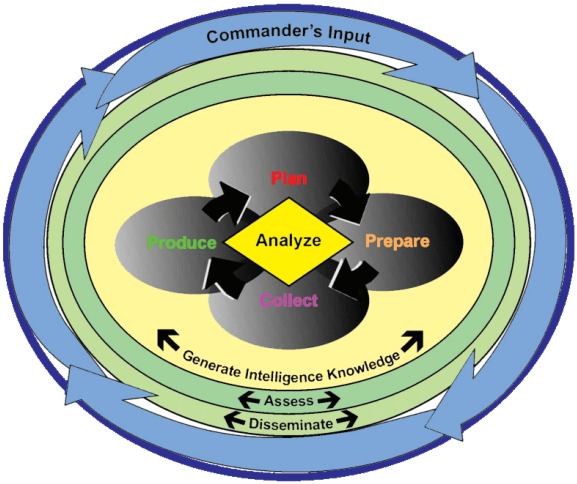



Figure 4-2. The intelligence process

**4-19.** For the intelligence staff, the intelligence process is a model that guides their collective actions in support of intelligence production.

**4-20.** As part of a combined arms staff, the intelligence staff at joint task force, corps, and division—

- Assists the commander in planning military operations.
- Assists the commander in executing those staff and leader activities directed by higher headquarters orders and preparing operation orders that direct the staff and leader activities of subordinate units.
- Facilitates the collection of information and intelligence by performing ISR synchronization and assisting in ISR integration.
- Produces intelligence in support of military operations.

**4-21.** To produce effective intelligence the intelligence staff requires more than just the information and intelligence collected by collection systems and reconnaissance and surveillance assets. The staff must generate intelligence knowledge throughout the intelligence process to ensure they have the data that is necessary to perform effective IPB. The intelligence staff generates this knowledge by data mining open-source, secure Department of Defense (DOD), and secure intelligence community databases and data files.

**4-22.** The intelligence staff continually assesses the intelligence it produces and the status of ongoing ISR operations to ensure the commander's information requirements are being met. The commander provides input to the staff to ensure it remains focused on the commander's intent.

## Commander's Input

**4-23.** Commanders are responsible for driving the intelligence process. They do this by providing commander's input. While it is not a part of the intelligence process itself, commander's input is the primary mechanism commanders use to focus the intelligence warfighting function. Commanders provide input at their discretion. Information gained through the assess continuing activity triggers the intelligence staff to request commander's input.





FOR OFFICIAL USE ONLY

**4-24.** The commander's input directly influences a unit's ISR effort. Each commander determines which intelligence products to develop as well as the format of those products. Commanders may provide input at any point during the intelligence process. The staff then adjusts the ISR effort accordingly.

## Intelligence Process Continuing Activities

**4-25.** Four continuing activities shape the intelligence process. They occur throughout the process and can affect any step at any time:

- Generate intelligence knowledge.
- Analyze.
- Assess.
- Disseminate.

### Generate Intelligence Knowledge

**4-26.** Generate intelligence knowledge is a continuous, user-defined step driven by the commander. It begins prior to mission receipt and provides the relevant knowledge required about the environment for the conduct of 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. It continues throughout the operations process. The unit determines what information it will need—based on the commander's guidance—as well as what information it already has, and what information it needs to collect. When performing the generate intelligence knowledge activity, units and personnel must follow all applicable policies and regulations on the collection of information and operations security (OPSEC). Generate intelligence knowledge is an integral part of the intelligence process. For Army units, the initial action to locate the information they need to collect is establishing an intelligence architecture. This architecture provides access to relevant intelligence community and other Department of Defense (DOD) databases and data files.



**4-27.** Three important aspects of generating intelligence knowledge are initial data-file development, operational and mission variables analysis, and intelligence survey development.

#### *Initial Data-file Development*

**4-28.** The initial result of the generate intelligence knowledge activity is the creation and population of data files, as directed by the commander, that are compatible with the unit's mission command information systems. When generating intelligence knowledge, unit intelligence personnel begin by determining what information they need to collect. The determination is based on the primary variables of the operational environment for which the intelligence staff is responsible. These are needed to support the command, IPB, and to answer the CCIRs.

#### *Operational and Mission Variables Analysis*

**4-29.** As units begin to collect data on the projected AO, the data should be organized into baseline data files based on 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 systems perspective—political, military, economic, social, infrastructure, and information (PMESII) as well as the operational variables (PMESII-PT, where PT refers to physical environment and time)—to populate the baseline data files.

**4-30.** All-source analysts ensure that relevant information is incorporated into the common database and the unit Web page. This information becomes the basis for intelligence support of predeployment readiness training that is based on the operational environment. It can incorporate simulations or replications of items such as threat vehicles, weapons, and uniforms, as well as threat tactics,



FOR OFFICIAL USE ONLY

techniques, and procedures (TTP)—along with civil considerations in the AO.

**4-31.** 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.

**4-32.** 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 performing IPB and mission analysis. Generate intelligence knowledge is also the basis for developing a unit's initial intelligence survey. The generate intelligence knowledge activity continues to gather, categorize, and analyze information on relevant aspects of the projected AO. The generate intelligence knowledge activity continually adds new information. It updates and refines understanding of the AO throughout the operations process.

**4-33.** During a deployment, a unit's databases become a resource for the generate intelligence knowledge activity of follow-on units that may replace them (in support of Army force generation [ARFORGEN]). During and after deployment, the generate intelligence knowledge activity also supports tactical overwatch and the collection of lessons learned.

### *Intelligence Survey*

**4-34.** The intelligence survey is a process that assists the S-2, G-2, or J-2 in identifying ISR asset collection capabilities and limitations within the projected AO. 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 capability.
- Develop an understanding of the information and intelligence that can be collected with unit intelligence assets.
- Determine a method of understanding when changes that are of intelligence interest occur to the information baseline, collection capability baseline, or analytical baseline.

**4-35.** The intelligence survey, which is developed over time and is continuously updated, provides the S-2, G-2, or J-2 with an initial assessment for recommending intelligence asset apportionment within the projected AO. The intelligence survey suggests the best use of 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 signals intelligence (SIGINT) asset collection due to terrain or lack of threat transmitters, but it may be well-suited for human intelligence (HUMINT) collection teams. The S-2, G-2, or J-2 may recommend that unit SIGINT collection assets not be deployed to that area, but that additional HUMINT collection teams would be a valuable source of intelligence collection in the same area.

**4-36.** This assessment includes a determination of what nonstandard ISR assets—including quick reaction capabilities and off-the-shelf capabilities and systems—are available to support the commander. Additionally, when reviewing contingency plans and operation plans (OPLANs), the S-2, G-2 or J-2 should use the intelligence survey to update the plan based on new technologies, capabilities, or sources of information and intelligence.

**4-37.** The intelligence survey also helps determine what communications capabilities will be required





FOR OFFICIAL USE ONLY

for deployed intelligence operations. The survey 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 to accomplish its mission.

### Analyze

**4-38.** *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 2-0). The intelligence staff analyzes intelligence and information about the threat's capabilities, friendly vulnerabilities, and the AO to determine how these can impact operations. The intelligence staff must also analyze and identify issues and problems that occur while performing the unit's intelligence process. Examples of this could be focusing on the wrong priority or the location of assets that are inadequate to collect required information.

**4-39.** This analysis enables the commander and staff to determine the appropriate action or reaction. It also allows the commander and staff to focus or redirect assets and resources to fill information gaps, mitigate collection limitations, or alleviate pitfalls. (For more information on intelligence analysis, see TC 2-33.4.)

### *Critical Thinking*

**4-40.** Critical thinking is an essential element of the analytical thought process. Critical thinking is necessary for adaptation to new developments in the ever-changing operational 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



**4-41.** 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 (For more information on critical thinking, see TC 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.

**4-42.** Critical thinking involves improving the quality of thought 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. Critical thinking is a self-directed, self-disciplined, self-monitored, and self-corrective thought process. It requires effective communication, problem-solving abilities, and continuous evaluation.

**4-43.** Critical thinking entails the examination of those structures or elements of thought implicit in all reasoning: purpose, problem, 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 are scientific thinking, mathematical thinking, historical thinking, anthropological thinking, economic thinking, moral thinking, and philosophical thinking. The critical thinker is—

- **Fair-minded**—remains neutral in appraising or applying countertheories to opinions of others.
- **Honest**—knows and acknowledges 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**—does not stop at the obvious; digs deeper to overcome initial conclusions; is satisfied



FOR OFFICIAL USE ONLY

only when the hypothesis is fully developed.

- **Focused—**is not easily swayed or distracted by emotions; maintains a point of concentration.
- **Questioning—**is not satisfied with the obvious; eager to seek additional information and data when none is immediately apparent.
- **Open-minded—**is 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*

**4-44.** Civil considerations are an important part of analysis. Civil considerations comprise six characteristics expressed in the memory aid ASCOPE (areas, structures, capabilities, organizations, people, and events). Depending on the echelon conducting operations, these factors may be expressed using the joint systems perspective, the operational variables, or the mission variables. Additionally, the human terrain analysis team can provide detailed information and analysis pertaining to the socio-cultural factors involved in an operation.

---

***Note.*** For additional information on ASCOPE and the IPB process, see FM 2-01.3

---

**4-45.** The ASCOPE factor 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.

**4-46.** 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 identifies the circumstances under which rules shift and change. Culture influences how people make judgments about what is right and wrong, assesses what is important and unimportant, categorizes things, and deals with matters 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.

**4-47.** Understanding other cultures applies across the spectrum of conflict, not just to operations dominated by stability concerns. For example, tactics used against a threat who considers surrender a dishonor worse than death may be different from those used against a foe 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 host nation. To operate successfully in multinational settings, Army leaders must recognize 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

**4-48.** Assess plays a critical role in evaluating the information collected during the intelligence process. Continual assessment of ISR operations, available information and intelligence, and various aspects of the mission variables (mission, enemy, terrain and weather, troops and support available—time available and civil considerations [METT-TC]) is 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.
- Effectively uses information and intelligence.

### Disseminate

**4-49.** 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





FOR OFFICIAL USE ONLY

commander. Determining the product format and selecting the means to deliver the information are key aspects of dissemination.

**4-50.** As required by unit SOPs, new or updated intelligence information must be regularly inputted in the common operational picture (COP) to provide the most current picture. The *common operational picture* is a single display of all relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (FM 3-0). It is conveyed through reports, automatic updates, and overlays common to all echelons and digitally stored in a common database. The COP facilitates mission command through collaborative interaction and real-time sharing of information between commanders and staffs. The intelligence portions of the COP are those messages and overlays relating to the 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 S-2, G-2, or J-2 monitors the common database to ensure it reflects the most current information and intelligence available. The intelligence staff must regularly provide updated intelligence to the COP in accordance with unit SOPs to support the commander's and staff's situational awareness.

**4-51.** Information presentation may be in oral, written, interactive, or graphic formats. The type of information, the time allocated, and the individual preferences of the commander all influence the information format. The (Distributed Common Ground System–Army) enterprise provides a common backbone for the dissemination of intelligence. It answers CCIRs for the commander, subordinate commanders, and staffs requiring direct dissemination.



### *Granting Access*

**4-52.** Granting access to databases, information, or intelligence ensures that personnel, units, or organizations are able to acquire and use what they need. This information may be found in classified and unclassified databases, programs, networks, systems, and other Web-based collaborative environments. The concepts of "push" and "pull" come into play regarding access. "Pushing" information and products to personnel, units, and organizations is actually dissemination, whereby the originating entity intentionally sends the products to designated addressees. "Pulling" information and products is accomplished by personnel, units, and organizations who are aware of sites with relevant information holdings and, on their initiative, "pull" information.

### *Sharing*

**4-53.** Sharing is primarily the result of establishing a collaborative environment. Collaboration takes many forms. Collaborative tools are often computer-based tools (groupware) that help individuals work together and share information. The tools allow virtual online meetings and data sharing. Sharing allows analysts, other intelligence personnel, and other subject matter experts to freely exchange information and intelligence that answers their commander's requirements. Sharing implies "pushing" relevant information to applicable parties.

### *Postings*

**4-54.** 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 but not part of the normal dissemination group for a specific unit or organization. When posting information to the Web or updating information on a Web site, units or organizations should inform higher, subordinate, and lateral units or organizations that may require this information. Units rarely have enough personnel to dedicate a Soldier to continuously search Web sites for new or updated information that may be of use to that unit or organization. The acquisition of posted information implies "pulling" relevant information by interested parties from relevant databases and information sources.



FOR OFFICIAL USE ONLY

## The Intelligence Process Steps

**4-55.** There are four steps in the intelligence process. They are the core of the intelligence process and recur continuously throughout the operations process:

- Plan.
- Prepare.
- Collect.
- Produce.

### Plan

**4-56.** 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 S-2, G-2, or J-2 synchronizes ISR and supports the S-3, G-3, or J-3 in ISR integration. Planning activities include, but are not limited to—

- Performing IPB and preparing IPB products and overlays.
- Developing initial PIRs.
- Developing the ISR synchronization tools.
- Developing the initial running intelligence estimates or briefings (usually as part of the mission analysis briefing). This should include initial PIRs as well as threat strengths and vulnerabilities that friendly forces should avoid or exploit.
- Managing requirements.
- Submitting requests for information (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 tools.
- Supporting the preparation of Annex B (Intelligence), and assisting the S-3, G-3 or J-3 in completing Annex L (ISR).

**4-57.** Commanders should be aware that intelligence collection is enabled by and subject to laws, regulations, and policies to ensure intelligence operations are properly conducted. Categories of legal considerations include the United States Code, executive orders, National Security Council intelligence directives, Army regulations, U.S. SIGINT directives, rules of engagement, status-of-forces agreements, and other international laws and directives.

### Prepare

**4-58.** 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 to use as they produce orders and conduct operations. Failure to properly prepare for intelligence collection and the publication of finished intelligence products can cause an operation to focus on an entirely wrong location, force, or objective. Thorough staff preparation allows the commander to focus the unit's combat power and achieve mission success. The prepare step includes those staff and leader activities that take place upon receiving the operation order (OPORD), OPLAN, warning order (WARNO), or commander's intent.

### Collect

**4-59.** 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 area of interest. A successful ISR effort results in the timely collection and reporting of relevant and accurate information. This helps assure the commander's situational understanding.

**4-60.** This collected information forms the foundation of intelligence databases, intelligence production, and the situational awareness of the S-2, G-2, or J-2. The requirements manager evaluates





FOR OFFICIAL USE ONLY

the reported information for its responsiveness to the CCIRs, PIRs, and FFIRs. The collect task can be broken into two subtasks—process and report.

***Process***

**4-61.** Once information has been collected, it is processed. Processing involves converting, evaluating, analyzing, interpreting, and synthesizing raw collected data and information into a format that enables 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—including a database format—that can be analyzed by a system operator, and correlating information.

**4-62.** 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 COP.

***Report***

**4-63.** 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 mission command network by systems such as DCGS-A. The information and intelligence is deposited in the common database, e-mail accounts, and on the unit's Web page.



**Produce**

**4-64.** The produce task involves combining analyzed information and intelligence from single or multiple sources into intelligence or intelligence products that support known or anticipated requirements. Production also involves combining new information and intelligence with existing intelligence to produce intelligence in a form the commander and staff can apply to the military decisionmaking process (MDMP) and 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. The information 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.
- Tagging and preparing products for dissemination and future data discovery.

**4-65.** The intelligence staff deals with numerous and varied production requirements. These production requirements are based on PIRs and intelligence needs; diverse missions, environments, and situations; and user format requirements. Through analysis, collaboration, and intelligence reach, the G-2/S-2 uses 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 mission variables (METT-TC) factors.

## ESTABLISH AN INTELLIGENCE ARCHITECTURE

**4-66.** Establishing an intelligence architecture involves complex and technical issues that include the following: sensors, data flow, hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and



FOR OFFICIAL USE ONLY

funding. A well-defined and well-designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture provides the best possible understanding of the threat, terrain and weather, and civil considerations. Establish an intelligence architecture includes the following four tasks:

- Perform intelligence reach.
- Develop and maintain automated intelligence networks.
- Establish and maintain access.
- Create and maintain intelligence databases.

## Perform Intelligence Reach

**4-67.** *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 within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (FM 2-0). Intelligence obtained through intelligence reach helps the staff plan and prepare for operations and answer CCIRs without the need for the information to pass through a formal hierarchy. This process allows intelligence analysts to retrieve existing information, products, and data that can support answering CCIRs from outside the unit in a timely manner. Organizations do not need 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.

## Develop and Maintain Automated Intelligence Networks

**4-68.** This task entails providing information systems that connect unique assets, units, echelons, agencies, and multinational partners for intelligence, collaborative analysis and production, dissemination, and intelligence reach. It uses existing automated information systems, such as the DCGS-A, and when necessary, creates operationally specific networks. In either case, these networks allow access to unclassified and classified means, and interoperability across the AO. This task includes identifying deficiencies in the following:

- Systems or networks.
- Service procedures.
- System administration procedures.
- Security procedures.
- Alternate power plans.
- Redundancy.
- System backups.
- Update procedures.

## Establish and Maintain Access

**4-69.** This task involves establishing, providing, and maintaining access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. Its purpose is to facilitate intelligence reporting, production, dissemination, and sustainment; intelligence reach; and a multilevel collaborative information environment.

## Create and Maintain Intelligence Databases

**4-70.** This task entails creating and maintaining unclassified and classified databases. Its purpose is to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach. It also includes the requirements for





FOR OFFICIAL USE ONLY

formatting 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 and standards.
- Update and backup procedures.
- Data mining, query, and search protocols.

## UPDATING THE COMMON OPERATIONAL PICTURE

**4-71.** As required by unit SOPs, new or updated intelligence information must be regularly entered into 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 mission 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. These are sent to the common database from intelligence organizations at various echelons and include combat information transmitted from individual Soldiers and platforms. The G-2 and S-2 monitor the common database to ensure the most current information and intelligence are available.



## NATIONAL-LEVEL SUPPORT

**4-72.** National-level intelligence organizations operate extensive collection, processing, and dissemination systems. They have broad, often unique, analytical capabilities. These intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements.

**4-73.** While national-level intelligence organizations can and will provide support to the commander, they must continue to support national-level decisionmakers. The focus of these national organizations is not evenly split between the two customers; it varies according to the situation. Successful national-level support to commanders depends on efficient and effective cooperation and interoperability, not only vertically but horizontally.

**4-74.** Representatives from some national-level intelligence organizations—such as the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), and the Department of State's Bureau of Intelligence and Research—support the combatant commanders on a full-time basis and are located at command headquarters. These representatives provide liaison with their parent organizations and serve as the commander's advisor on how to best employ their organization's capabilities.

## UNIFIED ACTION INTELLIGENCE OPERATIONS

**4-75.** *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). Joint operations focus and maximize the complementary and reinforcing effects and capabilities of each Service. Commanders synchronize the complementary capabilities of the Service components that make up the joint force.

**4-76.** The employment of military intelligence in campaigns and major operations must be viewed



FOR OFFICIAL USE ONLY

from a joint perspective. The intelligence construct must establish a fully interoperable and integrated joint intelligence capability. Army MI 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.

## MULTINATIONAL OPERATIONS

**4-77.** Multinational operations are the standard for current military operations, making intelligence-sharing with multinational forces very important. National interests require the United States to act together with other nations. In many situations, U.S. military forces will join with foreign military forces to defeat common threats. In most multinational operations, the commander is required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces. A multilevel security system that can easily facilitate sanitization and dissemination of information to U.S. and multinational commanders does not currently exist. Combatant commands and subordinate joint task forces can request that intelligence reports be made releasable to multinational partners as necessary.

**4-78.** Because each multinational operation is unique, there is no fixed set of rules or policies for conducting joint intelligence operations as part of multinational operations. The commander participating in the coalition or alliance operation must develop the policy and procedures for that particular operation. The following general principles provide a starting point for creating the necessary policy and procedures:

- **Maintain unity of effort.** Intelligence officers of each nation need to view the threat from multinational as well as national perspectives. A threat to one element of a multinational force by the common adversary must be considered a threat to all elements.
- **Make adjustments.** There will be differences in intelligence doctrine and procedures among the multinational partners. Major differences may include how intelligence is provided to the commander or procedures for sharing information among intelligence agencies.
- **Plan early and plan concurrently.** This permits solutions to any differences to be developed and tried before operations begin.
- **Share all necessary information.** Multinational partners must share all relevant and pertinent intelligence about the situation and adversary.
- **Perform complementary operations.** Intelligence efforts of the nations must be complementary, and all intelligence resources must be available for application to the whole of the intelligence problem.



## FORCE PROJECTION OPERATIONS

**4-79.** Force projection encompasses processes occurring in a continuous, overlapping, and repeating sequence throughout an operation. (FM 3-0 has a detailed discussion of force projection.) The five processes of force projection are—

- Mobilization.
- Deployment.
- Employment.
- Sustainment.
- Redeployment.

**4-80.** Intelligence and ISR considerations support each process. Built on a foundation of intelligence readiness, the intelligence warfighting function provides the commander with the intelligence needed


FOR OFFICIAL USE ONLY

to conduct (plan, prepare, execute, and assess) force projection operations. Successful intelligence during force projection operations relies on continuous collection and intelligence production before and during the operation.

**4-81.** In force projection operations, higher echelons provide intelligence to lower echelons until the tactical ground force completes entry and secures the lodgment area.

**4-82.** The S-2, G-2, or J-2 must anticipate, identify, consider, and evaluate all threats to the entire unit throughout force projection operations. The intelligence staff answers the CCIRs during the force projection processes. Until the unit's ISR assets are operational in the AO, the intelligence staff depends on intelligence from the senior Army force component or joint task force intelligence sections to answer the unit's intelligence needs. Mobilization is the process of assembling and organizing resources to support national objectives in time of war and other emergencies. (FM 3-35.) During the mobilization process the intelligence staff—

- Establishes habitual training relationships with their Regular Army and Reserve Component augmentation units as well as higher echelon intelligence organizations as identified in existing OPLANs.
- Identifies ISR force requirements for the different types of operations and contingency plans.
- Identifies individual military, civilian, and contractor manpower augmentation requirements for intelligence operations.
- Supports the Reserve Component units by preparing and performing intelligence training and threat update briefings, and by disseminating intelligence.
- Identifies individual mobilization augmentees to fill gaps created by personnel shortages. If possible, these augmentees should be individuals with a working knowledge of unit SOPs who understand the mission.
- Monitors intelligence reporting on threat activity and indications and warning (I&W) data, and watches condition levels.
- Manages information requirements and RFIs from the unit and subordinate units.
- Updates ISR synchronization planning based on augmentation or changes to task organization.
- Notifies attachments to provide updated access rosters and obtains higher headquarters access rosters. Updates throughout mission cycle as required.
- Verifies clearances and accesses within the unit, including sensitive positions and radio-telephone operators.
- Coordinates the Counterintelligence (CI) Awareness and Reporting Program, CI, and OPSEC training and operations.
- Verifies access to intelligence databases through division or subordinate units. Ensures unit intelligence personnel have access to national and strategic databases.
- Obtains current technical intelligence (TECHINT).
- Obtains user bulletins from the DIA.
- Reviews section files. Designates deployable and nondeployable records.
- Coordinates contingency area of interest briefings.
- Inspects unit areas and equipment for physical security deficiencies. Coordinates for support and access.
- Coordinates security force requirements with tasked units and military police (MP).
- Provides updated section alert notification roster to the S-1 or G-1.
- Finalizes security plans and instructions. Checks guard and MP patrols.

**4-83.** Deployment is the relocation of forces and materiel to desired operational areas. (See FM 3-35 for more information on the deployment phases.) Deployment has four supporting phases that are not always sequential and can overlap or occur simultaneously:

- Predeployment activities.
- Fort-to-port.





FOR OFFICIAL USE ONLY

- Port-to-port.
- Reception, staging, onward movement, and integration.

**4-84.** *Employment* is the strategic, operational, or tactical use of forces (JP 5-0). (See FM 3-0 and JP 3-0, for further discussion of employment.) At the beginning of the employment process, intelligence reaches the crossover point. Tactical intelligence becomes the commander's primary source of support, replacing top-driven national and theater intelligence. The commander uses both tactical and operational intelligence to decisively engage and defeat the enemy in combat operations. In stability operations the commander may use all levels of intelligence to accomplish the mission.

**4-85.** *Sustainment* is the provision of logistics and personnel required to maintain and prolong operations until successful mission accomplishment (JP 3-0). (See JP 4-0 and FM 4-0 for details on the sustainment process of force projection operations.)

**4-86.** *Redeployment* is the transfer of forces and materiel to support another joint force commander's operational requirements, or to return personnel, equipment, and materiel to the home and/or demobilization stations for reintegration and/or out-processing (JP 3-35). (See FM 3-35 for further discussion of redeployment.) As combat power and resources decrease in the AO, protection and I&W become the focus of the commander's intelligence requirements. This drives the selection of ISR elements that remain deployed and those that may redeploy. The intelligence staff—

- Monitors intelligence reporting on threat activity and I&W data.
- Continues to perform intelligence support to protection planning.
- Requests intelligence support (theater and national systems) and provides intelligence to support redeployment (reverse intelligence crossover point).
- Captures consolidated databases.
- Transfers data to the appropriate repository such as national databases.
- Evaluates the need for individual mobilization augmentees.
- Captures observations, insights, and lessons in after-action reviews.
- Maintains intelligence readiness.



## INTELLIGENCE PREPARATION OF THE BATTLEFIELD

**4-87.** The S-2 or G-2 is the staff proponent for IPB. IPB is the staff planning activity undertaken by the entire staff to define and understand the operational environment and the advantages and disadvantages of friendly and threat forces. IPB—

- Includes input from the entire staff.
- Is a systematic process of analyzing and visualizing the operational environment in a specific geographic area for a specific mission or in anticipation of a specific mission. The Army uses the mission variables (METT-TC) as the framework for analysis.
- Allows the commander and staff to gain the information necessary to selectively apply and maximize combat power at critical points in time and space.
- Is most effective when it integrates each staff element's expertise into the process.

**4-88.** The IPB process consists of four steps; each step is performed or assessed and refined continuously to ensure that the products of IPB remain complete and relevant, and that the commander receives intelligence support during current and future operations. The four steps of the IPB process are—

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



FOR OFFICIAL USE ONLY

## Define the Operational Environment

**4-89.** The first step in IPB is to identify, for further analysis, specific features of the environment or activities within it, and the physical space where they exist. These features may influence friendly and threat operations. At the end of step 1, the intelligence staff will have—

- Defined and marked on the map the AO, area of influence (AOI) based on the unit's SOPs.
- Identified characteristics of the AO and AOI that could influence the commander's mission.
- Begun or continued information collection.
- Begun or continued the process of identifying gaps in intelligence holdings and started looking for answers to those gaps.

## Describe Environmental Effects on Operations

**4-90.** The second step in IPB is to analyze the environmental effects and describe the effects on threat and friendly capabilities. This step involves the substeps of analyze the environment and describe the environmental effects on threat and friendly capabilities and COAs. The three areas of analysis are—

- Terrain analysis (physical geography), with emphasis on complex terrain, urban terrain, key infrastructure, lines of communications (LOCs) and the effects of weather on the terrain and operations.
- Weather analysis (observed and forecast).
- Civil considerations, with emphasis on the people, cultures, history, and host-nation (HN) government in the AO: These civil considerations comprise six characteristics expressed in the memory aid ASCOPE:
  - Areas.
  - Structures.
  - Capabilities.
  - Organizations.
  - People.
  - Events.



**4-91.** At the end of step 2, the intelligence staff has completed terrain analysis, analysis of civil considerations (using the ASCOPE memory aid), weather analysis and forecast, and an analysis of other significant characteristics of the environment for the AO and AOI. The following have been identified in a graphic or written format:

- Ground and air avenues of approach (AAs).
- Vital ground and key terrain.
- Severely restricted terrain.
- Restricted terrain.
- Built-up areas.
- River and water obstacles.
- Obstacles.
- Ground AAs and mobility corridors.
- Potential engagement areas.
- Defensible terrain.
- Potential objectives, decision points (DPs), named areas of interest (NAIs), and target areas of interest (TAIs).
- Effects on friendly and enemy systems.

**4-92.** The effects of weather and light data include–

- Light data charts.
- Short-term and long-term forecasts (0 to 72 hours).
- Climate studies.



FOR OFFICIAL USE ONLY

- Special studies.
- Weather effects on friendly and enemy systems.

## Evaluate the Threat

**4-93.** In order to understand what the threat can do, it is essential to understand its organization, equipment, doctrine and tactics, intentions, capabilities, vulnerabilities, and current disposition. In step 3, the intelligence staff analyzes the command's intelligence holdings, which they identified in step 1, to determine how the threat normally conducts operations under similar circumstances. When operating against a new or less-defined threat, the intelligence staff may need to concurrently develop or expand intelligence databases and threat models. In order to accomplish this, the intelligence staff should perform threat characteristic (formerly order of battle [OB] factors) analysis for each group identified in step 1. The effects of non-U.S. small arms and light weapons in the urban environment are shown in appendix N.

## Determine Threat Courses of Action

**4-94.** The fourth and final step in the IPB process is the determination of threat COAs. The analysis completed in steps 1, 2, and 3 is used to attempt to determine what the enemy is likely to do. At the end of step 4, the intelligence staff will have—

- Identified the threat's likely objectives and desired end state.
- Identified or developed the full set of COAs available to the threat.
- Considered all possible explanations for threat activities in terms of threat COAs to avoid surprise from unanticipated COAs.
- Evaluated and prioritized each COA.
- Developed each COA in the amount of detail required and time allowed.
- Identified initial ISR requirements.
- Created an event template.
- Produced an event matrix.

**4-95.** To achieve the desired results from step 4, the staff develops three key products:

- Situation template.
- Event template.
- Event Matrix.

### Situation Template

**4-96.** A situational template is a depiction of a potential threat course of action as part of a particular threat operation. Situation templates are developed on the threat's current situation, based on threat doctrine and the effects of terrain, weather, and civil considerations. For example the template may deal with training and experience levels, logistic status, losses, and disposition. The commander dictates the level of threat depiction. The threat depiction is based on consideration of the mission variables (METT-TC) (at a minimum two levels of command below the friendly force) as a part of the commander's guidance for mission analysis.

### Event Template

**4-97.** The event template is a guide for intelligence synchronization and ISR planning. It depicts the NAIs where activity or lack of it will indicate which COA the threat will adopt. The combination of the NAI, indicators, and time phase lines (TPL) associated with each threat COA forms the basis of the event template. The event matrix displays a description of the indicators and activity expected to occur in each NAI. It normally cross-references each NAI and indicator with the times they are expected to occur and the COAs they will confirm or deny. The combination of the NAI, indicators, and TTP associated with each threat COA form the basis of the event template.





FOR OFFICIAL USE ONLY

### Event Matrix

**4-98.** The event matrix, like the event template, is an intelligence tool that does not stand alone. Instead it works in conjunction with the event template, complementing the event template by providing details on the type of activity expected to occur at each NAI, the times the NAI is expected to be active, and its relationship to other events in the AO. Its primary use is in planning intelligence collection; however, it serves as an aid to situation development as well. It is the basis for the ISR plan and is used with the event template to build the decision support template (DST). Also, it is used in conjunction with the event template as a tool to analyze enemy actions and intentions during battle tracking. Since the event matrix is a tool, it has no prescribed format. However, it is a good idea to disseminate it along with the event template to the subordinate intelligence staff as long as it stays within intelligence channels.

## Intelligence Preparation of the Battlefield Products

**4-99.** The process to prepare IPB products begins in step 1 as information is collected, organized, and databased. The following list illustrates macro-level IPB products designed to show the "big picture." Products produced at tactical echelons are more narrowly focused. Major IPB products include overlays, written products and charts, and graphics.

**4-100. Examples of overlays produced during IPB:**

**4-101.** Terrain overlays—

- Cross-country mobility.
- LOCs (transportation, communications, and power).
- Vegetation type and distribution.
- Surface drainage and configuration.
- Surface materials.
- Crop type and distribution.
- Subsurface (bedrock) materials.
- Obstacles.
- Infrastructures.
- Flood zones.

**4-102.** Operations overlays—

- Boundary lines for AO.
- Objective.
- Phase lines.
- Battlefield symbology.

**4-103.** Demographic overlays—

- Ethnicity.
- Religion.
- Tribal affiliations.
- Languages.
- Population.
- Age of population.

**4-104.** Infrastructure overlays:

- LOCs.
- Traffic (type, frequency, occurrence of normal traffic events).
- Public service utilities.
- Communications.
- Electrical power.
- Water supply.
- Fire and rescue.
- Health services.
- Fuel.
- Transportation.
- Media, infrastructure (types).
- Media biographies.
- Economics.
- Political.

**4-105. Examples of information contained in IPB written products:**

- Threat study—potential threat to the mission.
- Military—threat characteristics (formerly OB factors).
- Paramilitary.
- Terrorist organizations.
- Drug trafficking.
- Criminal organizations.
- Nongovernmental organizations (NGOs).





FOR OFFICIAL USE ONLY

- Intergovernmental organizations (IGOs).
- Demographics and cultural studies:
  - Ethnicity.
  - Tribal registration lists.
  - Tribal affiliations.
  - Religion.
  - Languages.
  - Dialects.
  - Number of speakers.
  - Population.
  - Age of population.
  - Living conditions.
  - Dress and appearance.
  - Religious holidays.
  - Education and literacy.
  - Occupations.
  - Gender relations.
  - Kinship systems.
  - Marriage and alliances.
  - Eating habits.
  - Music.
  - Honorific titles.
  - Salient values.
  - Heroes and events.
  - Outlaw gangs.

**4-106.** Infrastructure reconnaissance (see FM 3-34.170):
- Sewage.
- Water.
- Electricity.
- Academics.
- Trash.
- Medical.
- Security.

**4-107.** Other considerations:
- Scientific and technical information—information concerning a nation's scientific and technological abilities, as well as the country's capabilities to use both in support of military objectives by developing new equipment and weapons.
- Third-nation support.
- Banking (all legal aspects).
- Attitudes towards friendly and threat forces.

**4-108.** History aspects (area study) and geography of the area:
- Myths.
- Rumors.
- Migrations.

**4-109. Examples of civil considerations identified during IPB:**

**4-110.** Areas:
- Street and urban patterns.
- Criminal enclaves.
- Underlying terrain.
- Key commercial zones.
- Subterranean passages.
- Political precincts and districts.

**4-111.** Structures (buildings, infrastructure, LOCs):
- Buildings.
- Communications towers.
- Power plants.
- Bridges.
- Construction materials.

**4-112.** Capabilities:
- Fuel and natural resources.
- Fire and rescue.
- Financial structure.
- Domestic and foreign indebtedness.
- Communication.
- Technology base.
- Black market activities and illicit trade.

**4-113.** Organizations:
- Political organizations.
- Labor unions.
- Patriotic service organizations.
- Criminal organizations.





FOR OFFICIAL USE ONLY

**4-114.** People:

- Tribal leaders.
- Labor leaders.
- Individuals of interest.

**4-115.** Events:

- National holidays.
- Religious holidays.
- Elections.
- Disasters.

**4-116.** For more detailed information about IPB see FM 2-01.3, FMI 2-01.301, and FM 5-0.

## ISR PLANNING CONSIDERATIONS

**4-117.** ISR planning consists of two staff processes: ISR synchronization and ISR integration. ISR synchronization is the responsibility of the S-2, G-2, or J-2 officer and intelligence staff. The S-3, G-3, or J-3 is responsible for ISR integration with the support of the S-2, G-2, or J-2. ISR synchronization involves the entire staff and all of the warfighting functions. Satisfying information requirements through staff element coordination facilitates ISR planning. It eliminates the necessity to task an asset to collect information that another unit or asset has already observed in the course of operations.

**4-118.** ISR is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. Aggressive and continuous ISR is a primary means of gaining knowledge of the operation environment. ISR supports operations through four tasks:

- Perform ISR synchronization.
- Perform ISR integration.
- Conduct reconnaissance.
- Conduct surveillance.



**4-119.** As a critical part of the intelligence warfighting function, ISR provides answers to CCIRs and contributes significantly to the commander's situational understanding. It is crucial that all commanders and staff sections participate in ISR planning—from the identification of information requirements through the collection and reporting of information—to answer CCIRs.

**4-120.** Commanders integrate all assets into a single ISR plan in order to capitalize on the different capabilities. They synchronize and coordinate surveillance and reconnaissance missions and employ other units for ISR within the scheme of maneuver. Synchronization and integration of ISR with the overall concept of operations positions ISR assets to continue to collect information; sustain and reconstitute for branches or sequels; or to shift priorities in accordance with the order. Managing the ISR effort entails—

- **Requirements visibility.** Use procedures and information systems to monitor and display the status of information requirements.
- **Asset visibility.** Use procedures and information systems to monitor and display collection asset status, location, and activities.
- **Assessment capability.** Use procedures and information systems to assess the effectiveness of the ISR effort and the operational impact of ISR results (such as its success or gaps in collection) and to task collection assets.

**4-121.** Lessons learned and observations from both combat training center rotations and current operations emphasize the importance of ISR planning. Full staff integration is needed to focus ISR assets on the CCIRs. Successful ISR plans integrate and synchronize the collection effort across all warfighting functions. Successful ISR plans use every available asset: Soldier, sensor, and unit. Effective ISR draws on all available collection assets—internal, external, and joint—and is enhanced by the DCGS-A enterprise.



FOR OFFICIAL USE ONLY

**4-122.** Army intelligence provides timely, relevant, accurate, and synchronized intelligence support to tactical, operational, and strategic commanders from force projection planning to the execution of operations. All intelligence operations are executed within the scope and parameters of applicable laws, policies, and regulations. These directives can be complex. They require attention during ISR synchronization and ISR integration activities.

## ISR Synchronization

**4-123.** The ISR synchronization task accomplishes the following:

- Analyzes information requirements and intelligence gaps.
- Evaluates available assets (internal and external).
- Determines gaps in the use of those assets.
- Recommends ISR assets controlled by the organization to collect on the CCIRs and submits RFIs for adjacent and higher collection support.

**4-124.** ISR synchronization ensures all available information is obtained through intelligence reach, RFIs, and ISR tasks. This results in the successful reporting, production, and dissemination of information, combat information, and intelligence needed to support decision making.

**4-125.** ISR synchronization ensures the commander's requirements drive ISR planning and that ISR reporting responds in time to influence decisions and operations. Intelligence personnel synchronize the ISR effort through coordination with operations personnel. Full staff participation is needed. Synchronizing includes all assets the commander controls—assets of lateral units and higher echelon units and organizations —as well as RFIs and intelligence reach to support intelligence production and dissemination. All of these help answer CCIRs and other requirements.

**4-126.** ISR synchronization identifies the best way to satisfy information requirements concerning the operational environment. Commanders use it to assess ISR asset reporting. The operations process provides the guidance and mission focus that drives the intelligence process. The intelligence process provides the continuous intelligence input, which is essential to the operations process.

**4-127.** The ISR synchronization process is depicted in figure 4-3. These activities and subordinate activities are not necessarily sequential. The ISR synchronization process supports full spectrum operations and does not dramatically change with echelon, although organization, terminology, and tools may vary.





FOR OFFICIAL USE ONLY

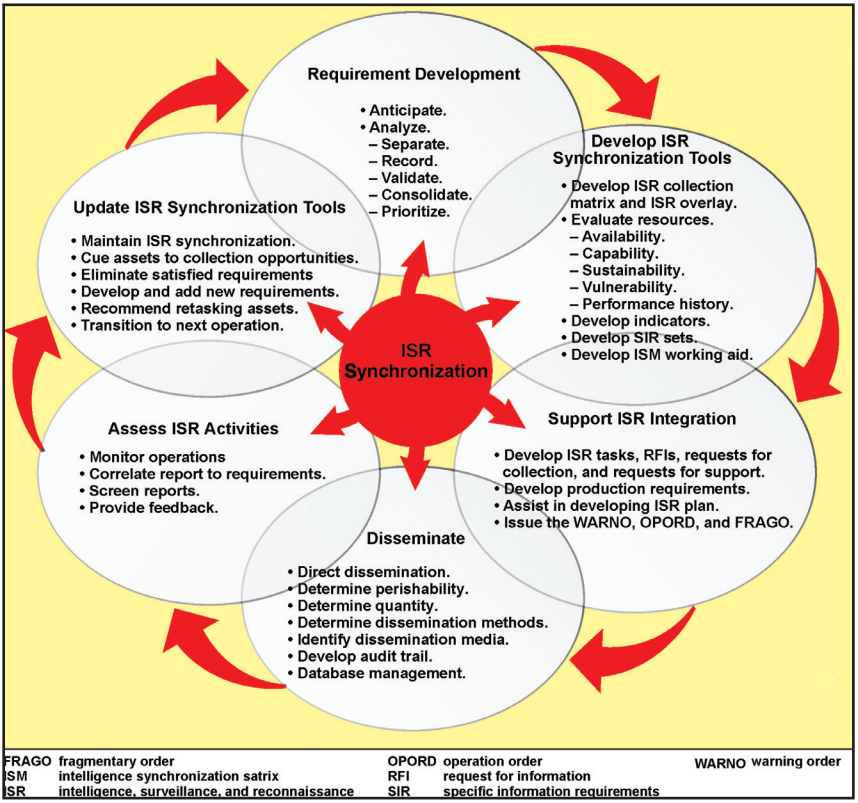



Figure 4-3. ISR synchronization activities

4-128. The intelligence process is driven by a need to provide the commander with information. This information is expressed in the form of requirements. For intelligence purposes, there are three types of requirements that result from ISR synchronization—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 (SIRs), which facilitate the answering of the requirements. The indicators and SIRs are used by ISR planners to develop the ISR plan. Figure 4-4 shows the process of developing requirements and integrating them into the ISR process.





FOR OFFICIAL USE ONLY

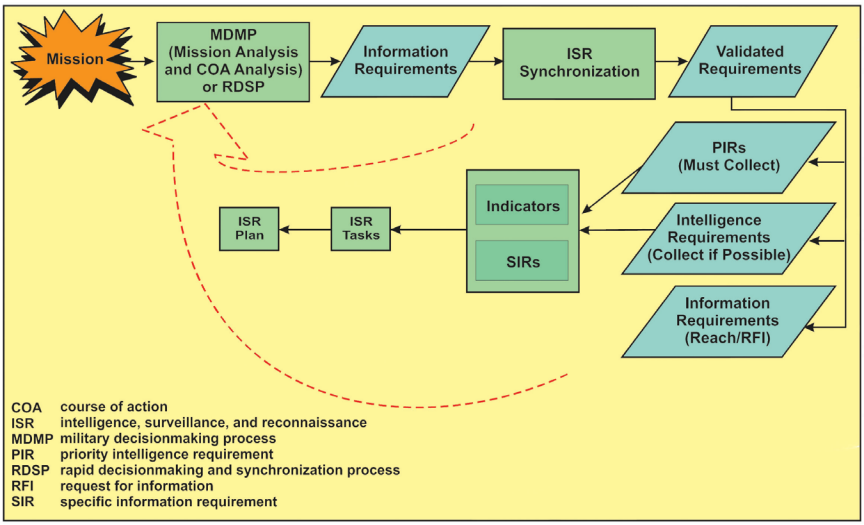



**Figure 4-4. Requirements development and integration into the ISR process**

**4-129.** The three types of validated information requirements are ordered in the following hierarchical structure for purposes of assigning ISR tasks:

- PIR.
- Intelligence requirement.
- Information requirement.

### Priority Intelligence Requirement

**4-130.** A PIR is an intelligence requirement, stated by the commander as a priority for intelligence support, which the commander needs to support decisionmaking and to understand the area of interest 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 FFIRs, are updated as part of updating the CCIRs throughout the operation. PIRs have first priority in collection assets tasked to their collection.

### Intelligence requirement

**4-131.** Joint doctrine defines an intelligence requirement as 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces (JP 2-0). For purposes of the Army intelligence warfighting function and ISR synchronization, an intelligence requirement is a type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. Intelligence requirements must be answered to facilitate operations. They require ISR collection assets to be assigned for their collection, second in priority to PIRs.

### Information requirements

**4-132.** 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). For the purposes of the intelligence warfighting function and ISR synchronization, validated





FOR OFFICIAL USE ONLY

information requirements are requirements that fill a gap in knowledge and understanding of the area of interest (terrain and weather, and civil considerations) or the threat. After validated requirements are identified and the ISR plan is completed, there may be 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, RFIs, or dissemination.

## ISR Integration

**4-133.** ISR integration is the task of assigning and controlling a unit's ISR assets in space, time, and purpose. This is done to collect and report information as a concerted and integrated portion of operation plans and orders. This ensures the best ISR assets are assigned to the task through a deliberate and coordinated effort of the entire staff, across all warfighting functions, by integrating ISR into the operation. (See figure 4-5.)

**4-134.** The S-3, G-3, or J-3, in coordination with the S-2, G-2, or J-2 and other staff members, tasks available ISR assets to best satisfy each requirement. ISR integration is vital in synchronizing the ISR plan with the scheme of maneuver. The result should focus on satisfying the commander's requirements through the translation of ISR tasks into orders.

**4-135.** Intelligence officers use ISR synchronization tools to track planned and ongoing collection operations. First, they evaluate ISR resources based on availability, capability, sustainability, vulnerability, and performance history. Then intelligence officers develop these tools. The two primary tools commonly used to assist the intelligence officer are the ISR overlay and the collection matrix. These tools are not tasking documents; they are used solely as working aids that facilitate the synchronization of collection and analytical efforts across the unit. The ISR overlay and collection matrix help the intelligence officer create the intelligence synchronization matrix.



**4-136.** The operations officer develops the ISR plan. This plan reflects an integrated collection strategy and employment, production, and dissemination scheme that will effectively answer the CCIRs. 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 area of interest.

**4-137.** This task includes updating reconnaissance and surveillance through dynamic retasking and periodic updates of the ISR plan. The operations officer updates the ISR plan based on information received from the intelligence officer. The operations officer integrates and manages the ISR effort through an integrated staff process and procedures. As PIRs are answered and new information requirements arise, the intelligence officer updates the intelligence synchronization tools and provides 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 organic, assigned, attached, and operational control (OPCON) collectors receive appropriate tasking.

**4-138.** The entire staff should be involved and engaged in the unit's orders production and planning activities to ensure early identification of all intelligence requirements.


FOR OFFICIAL USE ONLY

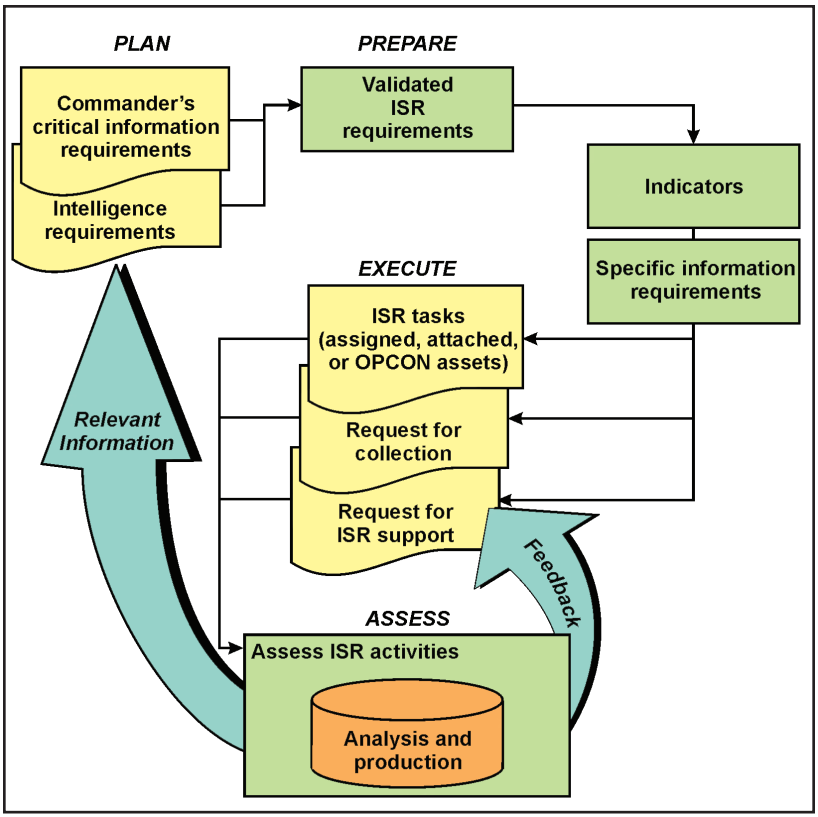



Figure 4-5. ISR relationship to the operations process



## INTELLIGENCE SUPPORT TO TARGETING

**4-139.** *Targeting* is the process of selecting and prioritizing targets, then matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0).

### Targeting Process

**4-140.** The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs. Targeting requires coordinated interaction between the fires, operations, intelligence, information engagement, information operations (IO), and plans cells. Based on the commander's guidance and targeting objectives, the staff determines what targets to attack and how and where to attack them. Targets should be assigned to the systems that are best able to achieve the desired effects. Targeting is based on assets that provide the enemy an advantage, friendly scheme of maneuver, and tactical plans. Targeting options can be either lethal or nonlethal. Soldiers should be aware of no-strike targets, and no-strike target lists. The lists are usually developed at the joint staff level. Soldiers also need to be aware of collateral damage assessments.

**4-141.** Decisions create the guidelines for the acquisition and engagement of targets. Target



FOR OFFICIAL USE ONLY

acquisition (TA) and attack are made through a decision cycle which is outlined in detail in figure 4-6. Decide, detect, deliver, and assess (D3A) together represent the decision cycle or methodology used to translate the commander's intent into a plan. The figure depicts the various steps, tasks, input, coordination and functions that comprise D3A in the decision cycle. Table 4-1 summarizes the output of the D3A targeting process and shows the targeting methodology. Table 4-2 presents a detailed list of the factors that must be considered during targeting. Subsequent paragraphs describe in detail each of the functions of D3A.

**4-142.** In stability operations, target development and targeting are difficult because of the greater emphasis on the effects of combat operations on the local government, Army, police, and the civilian population. This is where the need to consider the second- and third-order effects comes in to play. Providing intelligence support to targeting is one of the four primary intelligence tasks in the Army Universal Task List. It provides the commander information and intelligence support for targeting through lethal and nonlethal actions. The task includes intelligence support to planning (target development) and execution of direct and indirect fires, and information engagement. It also includes assessing the effects of those operations. The S-2, G-2, or J-2 ensures that the ISR plan supports the targeting plan. (For more information on intelligence support to targeting, see TC 2-50.5.)

## Provide Intelligence Support to Target Development

**4-143.** Target development is the systematic evaluation of potential target systems and their components. It is used to determine which elements of military action should, or could, be sued against the targets to achieve the stated objectives. (See FM 6-20-10.) Special consideration should be given to high-value targets (HVTs) and high-payoff targets (HPTs). (See figure 4-6.)

- A *high-value target* is a target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest (JP 3-09).
- A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission (JP 3-60). HPTs are developed from HVTs when the various COAs are wargamed

| | |
|---|---|
| ***Receive guidance on—*** | • Commander's intent.<br>• HPTs.<br>• Attack criteria.<br>• Lead time between decision points and TAIs.<br>• ROE.<br>• Conditions to establish combat assessment requirements. |
| ***Develop—*** | • MCOO.<br>• Situation and event templates.<br>• HVTs. |
| ***Explain—*** | • Threat COA as part of wargaming based on friendly COA, refine event template, assist in developing the HPLT, TSS matrix, and sensor or attack systems matrix. |
| ***Produce—*** | • ISR synchronization tools. |
| ***Brief—***<br>(Ensure all analysts and ISR asset managers understand the commander's intent.) | • Intelligence analyst sections (threat COA, HPTL, TSS, and AGM). |
| ***Collect—*** | • Information for nomination, validation, and combat assessment. |
| ***Disseminate—*** | • HPT related information and intelligence to the fires cell immediately.<br>• Pertinent information and BDA per SOPs and TTP. |
| ***Ensure—*** | • Information collection and intelligence production support all FRAGOs. |

| | |
|---|---|
| AGM—attack guidance matrix | ISR—intelligence, surveillance, and reconnaissance |
| BDA—battle damage assessment | MCOO—modified combined obstacle overlay |
| COA—course of action | ROE—rules of engagement |
| FRAGO—fragmentary order | SOP—standing operating procedure |
| HPT—high-payoff target | TOI—targets of interest |
| HPTL—high-payoff target list | TSS—target selection standard |
| HVT—high-value target | TTP—tactics, techniques, and procedures |

**Figure 4-6. Examples of high-value targets**





FOR OFFICIAL USE ONLY

## Targeting Methodolgy

**4-144.** Decisions create the guidelines for the acquisition and engagement of targets. Target acquisition (TA) and attack are made through a decision cycle which is outlined in detail in figure 4-7. Decide, detect, deliver, and assess (D3A) together represent the decision cycle or methodology used to translate the commander's intent into a plan. The figure depicts the various steps, tasks, input, coordination and functions that comprise D3A in the decision cycle. Table 4-1 summarizes the output of the D3A targeting process and shows the targeting methodology. Table 4-2 presents a detailed list of the factors that must be considered during targeting. Subsequent paragraphs describe in detail each of the functions of D3A.

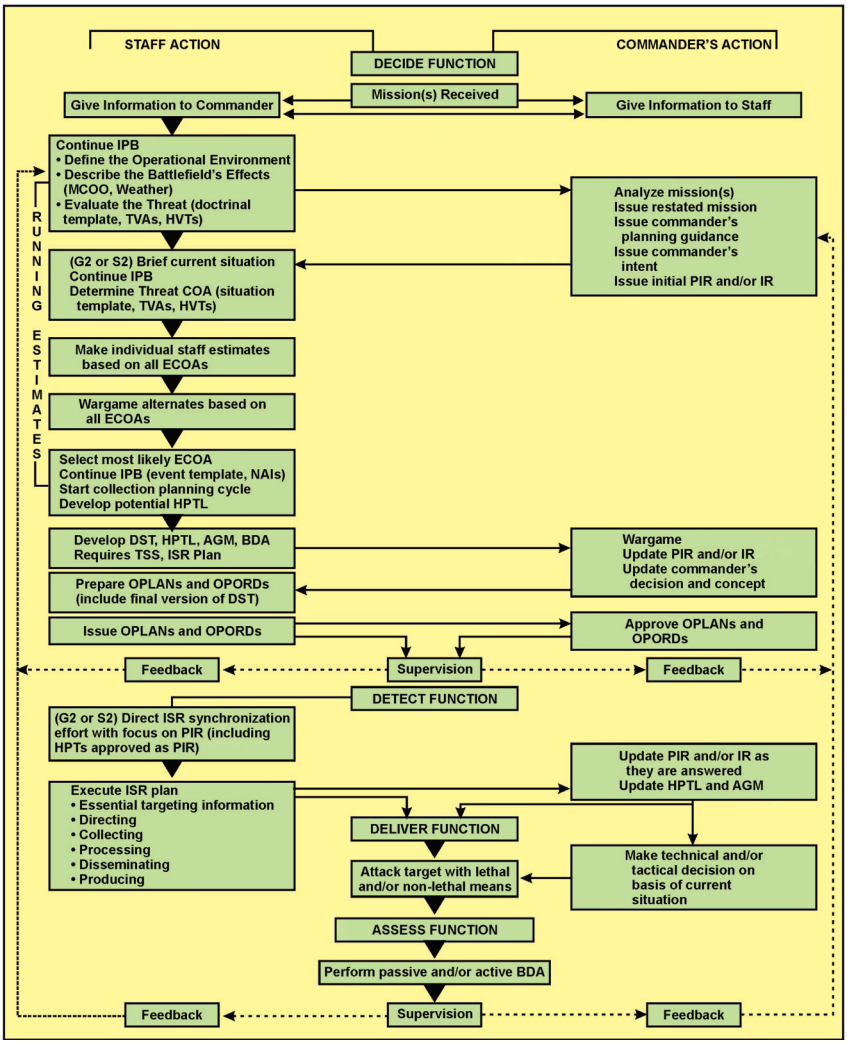



Figure 4-7. D3A targeting process





FOR OFFICIAL USE ONLY

## Table 4-1. Targeting methodology

| *Decide* | *Detect* | *Deliver* | *Assess* |
|---|---|---|---|
| • Target development.<br>• TVA.<br>• HPTs and HVTs.<br>• TSS.<br>• Attack options.<br>• Attack guidance. | • Target detection means.<br>• Detection procedures.<br>• Target tracking. | • Attack.<br>• Planned targets.<br>• Targets of opportunity.<br>• Desired effects.<br>• Attack systems. | • Tactical level.<br>• Operational level.<br>• Restrike.<br>• Feedback. |
| ***Note.*** Tracking the target is applicable during all steps. | | | |
| HPT—high-payoff target<br>HVT—high-value target | | TSS—target selection standard<br>TVA—target value analysis | |

## Table 4-2. Targeting considerations

| | |
|---|---|
| ***Decide:*** *Conduct during the planning phase of the operation. Who or what to attack? Is the target worth engaging with available assets?* | |
| _____ | Are the commander's planning guidance and intent detailed enough to enable the targeting team to determine—<br>• HVTs to nominate as HPTs?<br>• Desired effects on each HPT?<br>• When to attack each HPT?<br>• Any restrictions or constraints?<br>• Which HPTs require BDA? |
| _____ | What targeting assets (organic, attached, or supporting) are available to detect and attack HPTs? |
| _____ | What detect, deliver, and assess support is needed from higher headquarters? |
| _____ | When are requests to higher headquarters submitted to obtain the support when required? |
| _____ | Have target-tracking responsibilities been established? |
| _____ | Are systems in place to handoff the detected targets to assets that are capable of tracking them? |
| _____ | What detect, deliver, and assess support is required from subordinate units, and when is it required? |
| _____ | What detect, deliver, and assess support requests were received from subordinate units, and what was done with them? |
| _____ | Has the AGM been synchronized with the decision support matrix and the maneuver and fire support plans? |
| _____ | Are all commands using a common datum for locations? If not, are there procedures to correct differences in data? |
| ***Detect:*** *Conduct mainly during the preparation and execution phases of the operation. How to acquire the target. Once the target is acquired, how to track the target's movement* | |
| _____ | Do ISR synchronization tools focus on the appropriate PIRs? |
| _____ | What accuracy, timeliness, and validity standards, such as, TSSs, are in effect for detection and delivery systems? |
| _____ | Are all target acquisition systems fully employed? |
| _____ | Have backup target acquisition systems been identified for HPTs? |
| _____ | Have responsibilities been assigned to the appropriate unit or agency for detecting each HPT? |
| _____ | Are HPTs being tracked? |
| _____ | Have verification procedures using backup systems been established where necessary? |
| _____ | Are target acquisition and BDA requirements distributed properly among systems that can accomplish both? |
| ***Deliver:*** *Execute the mission to achieve the desired results. Execute attacks on selected targets IAW the FRAGO and the target synchronization matrix. This includes lethal and nonlethal operations.* | |
| _____ | Have communications links been established between detection systems, the decisionmaker, and delivery systems? |
| _____ | Have responsibilities been assigned to the appropriate unit or agency for attacking each HPT? |
| _____ | Has a backup attack system been identified for each critical HPT? (The primary system may not be available when the HPT is verified.) |
| _____ | Have fire support coordination measures or AGM and clearance procedures been established to facilitate target engagement? |
| _____ | Have on order fire support coordination measures or AGMs been established to facilitate future and transition operations? |
| _____ | Have potential fratricide situations been identified? Have procedures been established to positively control each situation? |
| _____ | Have responsibilities been assigned to the appropriate unit or agency for tracking specific HPTs and providing BDA on specified HPTs? |
| _____ | What are the procedures to update the HPTL and synchronize the AGM and decision support template if it becomes necessary to change the maneuver scheme and fire support as the situation changes? |





FOR OFFICIAL USE ONLY

### Decide in Targeting Methodology

**4-145.** Decide provides the overall focus and sets priorities for ISR and attack planning. Targeting priorities are addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

- The high-payoff target list (HPTL) is a prioritized list of HVTs. Their loss to the enemy contributes to the success of the friendly COA.
- The ISR plan focuses the collection effort to answer the CCIRs, including HPTs designated as collection requirements. The plan, within the availability of additional ISR assets, supports the acquisition of more HPTs. (See FM 2-0, and FMI 2-01.)
- The target selection standards (TSS) matrices address accuracy or other specific criteria requiring compliance before targets can be attacked.
- The attack guidance matrix (AGM), approved by the commander, addresses which targets will be attacked, how, when, and the desired effects.

#### *Target Value Analysis and Wargaming*

**4-146.** Target value analysis (TVA) yields HVTs for a specific threat COA. Target spreadsheets identify the HVTs in relation to a type of operation, and target sheets offer detailed targeting information for each. (See FM 6-20-10, appendix A.) This information is used during the IPB and the wargaming processes. The intelligence staff's analysis section develops both tools. TVA, a detailed analysis of the threat in selected COAs, focuses on the following threat characteristics:

- Composition.
- Disposition.
- Tactics.
- Training.
- Logistics.
- Operational effectiveness.
- Communications.
- Intelligence.
- Recruitment.
- Support.
- Reach.
- National agencies.
- Law enforcement agencies.
- International agencies and NGOs.
- Personality.
- Other threats.

**4-149.** For more information about threat characteristics, see TC 2-33.4.

**4-150.** TVA methodology supports a relative ranking of target sets or categories. The methodology begins when target analysts in the intelligence staff assume the position of the enemy commander. The target analyst, in coordination with other staff members, war-games the operation.

**4-151.** During the war game, friendly COAs are analyzed, based on their effect on enemy operations and the likely responses. Attacked enemy capabilities that force the enemy response are identified. The commander and staff analyze the criticality of friendly capabilities on a specific COA. TAIs are considered the best locations to attack HPTs. Commanders and staff use DPs or time phase lines to ensure the decision to engage or not to engage occurs at the right time. The war game prioritizes HVTs that are critical for the enemy mission to succeed. It also identifies HVT subsets that are HPTs acquired and attacked for the friendly mission to succeed. Selected HPTs are recorded on the DST, at which time the commander and staff analyze the second- and third-order effects.

**4-152.** ISR planners evaluate assets based on their capabilities to detect designated HVTs. HPTs receive priority in the allocation of assets. The fires cell determines friendly weapons systems capable of attacking HVTs with lethal fires. The electronic warfare officer (EWO) nominates and coordinates with the fires cell to provide nonlethal fires.

**4-153.** The intelligence staff analyzes and synthesizes the threat's response to each attack. Targets should be assigned priorities based on description, signature, degradation, and graphic representation. If targets have the same relative importance, a targeting team prioritizes the targets by seeking advice





FOR OFFICIAL USE ONLY

from the fires cell's targeting analyst and the field artillery intelligence officer (FAIO).

*High-Payoff Target List*

**4-154.** Prioritized targets are placed on an HPTL. (See table 4-3.)

**Table 4-3. High-payoff target list example**

| *Event or phase* | | | |
|---|---|---|---|
| ***Priority*** | ***Category*** | ***Target*** | ***Desired effect*** |
| 1 | fire support | AA5001 | suppress |
| 2 | air defense | AA5002 | neutralize |

*Target Selection Standards*

**4-155.** TSS are criteria, determined by the commander, applied to enemy activity (acquisitions and AO information) and used to decide whether the activity is a target. There are two TSS categories—targets, which meet accuracy and timeliness requirements for attack, and suspected targets, which require confirmation before any attack. TSS comprise the following essential elements:

- **High-payoff target.** Designated HPTs the ISR synchronization manager is tasked to acquire.
- **Timeliness.** Valid targets are reported to attack systems within the designated timeliness criteria.
- **Accuracy.** Valid targets are reported to the attack system complying with the required target location error (TLE) criteria. The criterion is the least restrictive TLE, considering the capabilities of available attack systems.

**4-156.** Different TSS may exist for a given enemy activity, based on different attack systems. For example, an enemy artillery battery may have a 150-meter TLE requirement for attack by cannon artillery and a one-kilometer requirement for attack helicopters. TSS are developed by the fires cells in conjunction with the intelligence cell. Intelligence analysts use TSS to quickly determine targets from AO information and pass the targets to the fires cell.



**4-157.** Attack system managers, such as the fires cell, fire control elements, or fire direction centers, use TSS to identify targets for attack. Commands can develop TSS based on anticipated threat characteristics and doctrine equivalent to the available attack systems.

**4-158.** The intelligence staff knows the accuracy of acquisition systems, associated TLE, and the expected enemy target dwell times. The intelligence staff can specify whether information reported to the attack system manager is a target or a suspected target. Certain situations require the system to identify friendly and neutral from enemy before approval to fire. HPTs that comply with the criteria are tracked until they are attacked in accordance with the AGM. Target locations that do not comply with TSS are confirmed before attacked. The TSS can be depicted in a TSS matrix. (See figure 4-8.)

**4-159.** The matrix lists each system that forwards targets directly to the fires cell or fire direction center. The effects of terrain and weather on the ISR assets and on enemy equipment are considered. TSS are keyed to the situation. However, the greatest emphasis is on the enemy situation, considering deception and the reliability of the source or agency that is reporting. HPTLs show the prioritized HPTs identified during wargaming. They have priority for engagement.

| *High-payoff target* | *Timeliness* | *Accuracy* |
|---|---|---|
| 2S3 | 30 minutes | 500 meter |
| M-46 | 30 minutes | 500 meter |
| Air and missile defense | 15 minutes | 500 meter |
| Command posts | 3 hour | 500 meter |
| Ammunition | 6 hour | 1 kilometer |
| Maneuver | 1 hour | 150 meter |

**Figure 4-8. Example of target selection standards matrix**



FOR OFFICIAL USE ONLY

### *Attack Guidance Matrix*

**4-160.** Knowledge of target vulnerabilities and the effect an attack will have on enemy operations allows a staff to propose the most efficient available attack option. Key guidance is whether the commander wishes to disrupt, delay, limit damage, or destroy the enemy. During wargaming, DPs linked to events, areas (NAIs and TAIs), or points in the AO are developed. These DPs cue command decisions and staff actions where tactical decisions are needed. Based on the commander's guidance, the targeting team recommends target engagement in terms of the effects of fire and attack options using the AGM. The AGM is updated during staff planning meetings and when the enemy situation changes. (See table 4-4 for an example of an AGM.) Consider separate AGMs for each phase of an operation.

**Table 4-4. Example of an AGM**

| ***Phase/Event: Attack through the security zone*** | | | | |
|---|---|---|---|---|
| ***High-payoff target list*** | ***When*** | ***How*** | ***Effect*** | ***Remarks*** |
| Command observation posts | P | Fires brigade | N | Plan in initial preparation |
| Reconnaissance and surveillance | P | Fires brigade | N | Plan in initial preparation |
| Target acquisition | P | Fires brigade | N | Plan in initial preparation |
| 2S1 and 2S3 | P | Multiple Launch Rocket System | N | Plan in initial preparation |
| 2S6, SA9, and SA13 | P | Fires brigade | S | SEAD for aviation operations |
| Regimental command post | A | MLRS | N | |
| Reserve battalion | P | Combat aviation brigade | D | Intent to attack reserve battalion in each HOT |
| ***Note.*** [1]This is only an example of an attack guidance matrix. Actual matrices are developed based on the situation. [2]An "H" for harassing fires may be included in the *Effect* column during stability operations. | | | | |
| A—as acquired<br>D—destroy | I—immediate<br>N—neutralize | P—planned<br>S—suppress | SEAD—suppression of enemy air defense | |

### *Completing the Attack Guidance Matrix*

**4-161.** Complete the AGM by filling in the columns in the matrix. First enter the selected targets from the HPTL. In the second column enter the code indicating when the attack will occur. In the third column enter the appropriate attack system. The next column is a description of the desired effect. The last column contains any necessary remarks.

### *Content of the When Column*

**4-162.** Timing the target attacks is critical to maximizing effects. During wargaming, the optimum time is identified and reflected in the when column:

- A "P" indicates the target should not be engaged; rather, it should be planned for future firing or simply put on file. Examples include a preparation, a suppression of enemy air defense (SEAD) program, or a countermobility program.
- An "A" indicates targets should be engaged as acquired by the headquarters, in the priority noted on the HPTL.
- An "I" indicates an immediate attack in special cases. This designation should be limited to a small percentage and only for the most critical types of targets. Having too many targets classed as immediate is disruptive and lowers the efficiency of attack systems. Immediate attacks take precedence over all other attacks. They are performed even if attack systems must be diverted from attacks in progress. Examples of immediate targets include—
  - Missile systems capable of chemical, biological, radiological, nuclear, and high-yeild explosives (CBRNE) attacks.
  - Division headquarters.
  - CBRNE weapons storage and support facilities.
- The Multiple Launch Rocket System (MLRS) may be considered for immediate attack depending on its effectiveness against friendly forces and tactical employment. The S-3, G-3, or J-3 and fire support coordinator or fires cell officer establishes procedures within the command post for immediate target attack.





FOR OFFICIAL USE ONLY

### *Content of the How Column*

**4-163.** How does the attack system link to the HPT? Identify a primary and backup attack system for HPT attacks.

### *Content of the Effect Column*

**4-164.** Effect refers to the target attack criteria. The targeting team specifies attack criteria based on the commander's guidance. Target attack criteria should be quantifiable—for example, percentage of casualties or destroyed elements, time, ordnance, and allocation or application of assets. Effect can be viewed as the number of battery or battalion volleys.

### *Harassing Fire*

**4-165.** Harassing fire is designed to disturb enemy troops, curtail movement, and—by threat of losses— lower morale. The decision to employ harassing fires requires careful consideration, since harassing fires have little real effect on the enemy, subject gun crews to an additional workload, and increase the threat of counterfire. Rules of engagement (ROE) or the potential for adverse public opinion may prohibit its use. However, harassing fires may be a combat multiplier in some situations. Consider using harassing fires in stability operations, delaying actions, and economy of force operations. Harassing fire can either suppress or neutralize an enemy.

### *Suppressive Fire*

**4-166.** Suppressive fire on or about a weapon system degrades the system's performance below the level required to fulfill its mission objectives. Suppression lasts as long as the fires continue—the duration is specified in the call for fire or established by SOPs. Suppression use prevents effective fire on friendly forces. Usually, suppression is used to support a specified movement of forces. The fire support coordinator asks or answers the when and how long questions.



### *Neutralization Fire*

**4-167.** Neutralization fire renders a target temporarily ineffective or unusable. It leaves enemy personnel or materiel incapable of interfering with an operation or COA. The fire support coordinator asks when and for how long the commander wants a target to be neutralized. Most planned missions are neutralization fires.

### *Destruction Fire*

**4-168.** Destruction fire's sole purpose is the destruction of materiel. It physically renders a target permanently combat-ineffective unless the target is restored, reconstituted, or rebuilt. Setting automated fire support default values for 30-percent destruction does not guarantee the commander's intent will be achieved. The remaining 70 percent may still influence the operation. Destruction missions are expensive in time and materiel; therefore, successful commanders consider whether neutralization or suppression is more efficient.

### Content of the Remarks Column

**4-169.** This may be used to note which targets should not be attacked in certain tactical situations, for example, if the enemy is withdrawing. Examples of how to use this column include—

- Accuracy or time constraints.
- Coordination requirements.
- Amount or type of ammunition limitations.
- Battle Damage Assessment (BDA), functional damage assessment (FDA), and munitions effects assessment (MEA).

**4-170.** Deciding which attack system to use occurs simultaneously with the decision on when to acquire and attack the target. When deciding to attack with two different means, such as electronic warfare (EW) and combat air operations, coordination is required. Coordination requirements are



FOR OFFICIAL USE ONLY

recorded during the wargaming process. In stability operations, the attack system may be using IO and civil affairs operations to engage and cause a division between the local populace and the insurgents. Commanders approve AGMs, which detail—

- Prioritized HPTLs.
- When, how, and the desired effects of attack.
- Special instructions.
- HPTs requiring a combat assessment.

**4-171.** Attack guidance is developed during the wargame. It—

- Applies to planned targets and targets of opportunity.
- May address specific or general target descriptions.
- Is provided to attack system managers through the AGM.
- May change as the operation progresses.

### Detect in Targeting Methodology

**4-172.** The S-2, G-2, or J-2 directs the effort to detect identified HPTs. To identify who, what, when, and how for TA, the intelligence staff coordinates with the—

- Intelligence all-source analysis section.
- FAIO.
- Targeting officer and fires cell analyst.
- IO officer.
- Higher, lower, and adjacent intelligence staffs.
- Special operations forces (if applicable).
- National agency support teams (if applicable).

**4-173.** This process sets accurate, identifiable, and timely requirements for ISR systems. The analysis section ensures ISR planner understand these requirements.

**4-174.** Target detection and action requirements are expressed as information requirements. Their priority depends on the importance of the target to the friendly COA and tracking requirements. PIRs and information requirements that support HPT detection are incorporated into the overall unit ISR plan.

**4-175.** The intelligence staff focuses the intelligence acquisition efforts on designated HPTs and PIRs. Situation development information, through detection and tracking, accumulates as ISR assets satisfy PIRs and information requirements. The ISR requirements manager—

- Considers the capabilities and availability of ISR assets within the echelon, and the assets available to subordinate, higher, and adjacent units.
- Considers joint or multinational force assets.
- Translates the PIRs and information requirements into SIRs and recommended ISR tasks and RFIs.
- Arranges direct dissemination of targeting information to the fires cell.

### *Detection in Counterinsurgency Operations*

**4-176.** Targeting in counterinsurgency operations requires a detailed understanding of social networks, insurgent networks, actions, and civil considerations. A target can be a person, place, or object considered vital to defeat or deny threat activities. The target can be successful civic initiatives or new businesses in the IO strategy. Therefore, in a counterinsurgency environment, the detect phase often precedes the decide phase because it is difficult to decide who to target without knowing who or what are the targets.





FOR OFFICIAL USE ONLY

### *Detection Procedures*

**4-177.** The following procedures assist in the target detection process:

- Use all TA assets effectively and efficiently.
- Avoid effort duplication among available ISR assets unless confirmation of target information is required. The intelligence staff ensures there are no gaps in planned coverage, which allows timely collection of combat information to answer the commander's intelligence and TA requirements.
- To detect HPTs, give clear and concise tasking to those TA systems capable of detecting a given target. This information allows analysts to develop the enemy situation and identify targets.

**4-178.** Fires cell personnel provide the intelligence staff with the degree of located accuracy:

- Accuracy requirements are matched to the TLE of the ISR asset, which allows the intelligence staff to develop more detailed TSS.
- Identified NAIs and TAIs are matched with the most capable detection system available. If the target type and its associated signatures—for example, electronic, visual, thermal—are known, the most capable ISR asset can be directed against the target. The asset can be positioned based on estimations of the where and when of the target's location.

**4-179.** Information needed to detect targets is expressed in requirements, which are incorporated into the ISR synchronization tools. The ISR synchronization manager—

- Translates the PIRs and information requirements into SIRs.
- Considers the availability of all ISR assets at all echelons.



**4-180.** As ISR and TA assets collect information for target development, the information is forwarded to the G-2. The G-2—

- Uses the information to perform situation and target development.
- Delivers the information to the fires cell after identification of a target specified for attack. The fires cell executes the attack guidance against the target.

> ***Note.*** Coordination between the intelligence staff and the fires cell is essential to ensure the targets are delivered to an attack system that will engage the target.

**4-181.** The FAIOs coordinate with the intelligence staff and fires cell to deliver HPTs and other targets directly to the fire control element at the fires brigade, or, if approved, through the maneuver commander directly to a firing unit. The results are targets designated in advance for attack.

**4-182.** When the FAIOs obtain intelligence information that warrants attack, the fires cell is notified. This allows the FAIOs to focus on intelligence analysis and the fires cell to manage the control of fires. The targeting officer at maneuver brigade and the S-2 at battalion perform FAIO functions.

**4-183.** Tracking priorities are based on the commander's concept of operations and targeting priorities. Tracking is executed through the ISR plan. Although every target is not tracked, critical targets move frequently and therefore require tracking.

### Deliver in Targeting Methodology

**4-184.** Deliver executes the target attack guidance and supports the commander's plan once the HPTs have been located and identified. (See table 4-5)



FOR OFFICIAL USE ONLY

## Table 4-5. Deliver functions and responsibilities

| | |
|---|---|
| ***Target attacks should—*** | • Satisfy attack guidance developed in **decide** function.<br>• Require two categories of decisions—tactical and technical. |
| ***Tactical decisions determine—*** | • Desired effects, degree of damage, or both.<br>• Attack system to be used.<br>• Attack time based on in the type of target—planned target or target of opportunity.<br>• **Planned target:**<br>▪ Some targets will not appear as anticipated.<br>▪ Target attack takes place only when the forecasted enemy activity occurs in projected time or place. Detection and tracking of activities associated with a target triggers a target attack. |
| ***Targeting team*** | |
| ***G-2/S-2 responsibilities*** | • Verify enemy activity as the planned target to attack.<br>• Validate target by conducting final reliability check of target source and accuracy (time and location). Deliver target to the fires cell.<br>• Current operations officer—check target legality in terms of ROE. |
| ***Fires cell responsibilities*** | • Determine planned attack system availability. Verify as the appropriate system for attack.<br>• Coordinate with higher, lower, or adjacent units; other Services; and multinational and host-nation forces (important where potential fratricide situations are identified).<br>• Issue fire mission request to appropriate executing units.<br>• Inform G-2/S-2 of target attack. G-2/S-2 alerts appropriate system responsible for BDA (when applicable).<br>• **Targets of opportunity—**<br>▪ Are processed as are planned HPTs. Evaluate those not on HPTLs for their attack potentiality.<br>• Decision to attack follows attack guidance and is based on—<br>▪ Target activity.<br>▪ Dwell time.<br>▪ Target payoff compared to other targets processed for engagement.<br>• If the decision to attack is immediate, process the target further.<br>• Assess attack availability and attack system capabilities to engage targets.<br>• If target exceeds availability or capabilities, send target to higher headquarters for immediate attack.<br>• If deferring the attack, continue tracking, determine attack decision points, and modify ISR tasks as appropriate. |
| ***Technical decisions (based on tactical decisions)*** | • Precise delivery means.<br>• Munitions number and type.<br>• Unit conducting the attack.<br>• Attacking unit response time.<br>• Results in the physical attack of targets by lethal or nonlethal means. The fires cell directs attack systems to attack a target once tactical decisions are made.<br>• Fires cell provides attack system manager with—<br>▪ Selected attack time.<br>▪ Desired effects IAW the previous discussion.<br>▪ Special restraints or requests for particular munitions. |





FOR OFFICIAL USE ONLY

**Table 4-5. Deliver functions and responsibilities (continued)**

| ***Targeting team*** | |
|---|---|
| ***Technical decisions (based on tactical decisions)*** | • Attack system managers—such as, FSCOORDs, air LNOs, aviation brigade LNOs, naval gunfire LNOs, maneuver units—determine whether the system complies with requirements. If not, they notify the targeting cell. Some reasons for noncompliance include—<br>▪ System or assets unavailable at specified time.<br>▪ Required munitions unavailable.<br>▪ Target out of range.<br>• Targeting cell decides whether selected system attacks under different criteria or whether to use a different system. |
| ***Targets of opportunity are attacked based on—*** | • The target's activity.<br>• Estimated assembly area activity. |
| ***Desired effects:***<br>***Disrupt***<br>***Delay***<br>***Limit*** | • **Planned targets:**<br>▪ Verify threat activity as that planned to be attacked.<br>▪ Reaffirm decision to attack.<br>▪ Issue the fire mission request (through the fires cell) to appropriate executing units.<br>• **Targets of opportunity:**<br>▪ Targeting team decides payoff and availability of attack systems and munitions. |
| ***Attack system*** | • **Planned targets:**<br>▪ Decision made during the **decide** function.<br>▪ Determine system availability and capability.<br>▪ Targeting team determines the best system available to attack target if system unavailable or capable.<br>• **Targets of Opportunity:**<br>▪ Targeting team determines attack system, subject to maneuver commander's approval.<br>▪ Consider all available attack systems.<br>▪ Attacking targets should optimize capabilities of—<br>• Light and heavy ground forces.<br>• Attack helicopters.<br>• Field artillery.<br>• Mortars.<br>• Naval gunfire.<br>• Combat air operations (CAS and air interdiction).<br>• Offensive EW.<br>▪ Consider availability and capabilities of each resource using—<br>• Desired effects on the target.<br>• Payoff of the target.<br>• Degree of risk to use asset against target.<br>• Impact on friendly operations.<br>• Impact on populace (second and third order effects).<br>▪ Target attack should be coordinated among two or more attack systems.<br>▪ Engaging a target by lethal means, along with jamming or monitoring, may be more beneficial than simply firing at the target. |

| | |
|---|---|
| BDA—battle damage assessment | HPTL—high-payoff target list |
| CAS—close air support | IAW—in accordance with |
| EW—electronic warfare | ISR—intelligence, surveillance, and reconnaissance |
| FSCOORD—fire support coordinator | LNO—liaison officer |
| HPT—high-payoff target | ROE—rules of engagement |

**4-185.** *Combat assessment* is the determination of the effectiveness of force employment during military operations (FM 7-15). It is composed of three elements:

- *Battle damage assessment* is timely and accurate estimate of damage resulting from the application of lethal or nonlethal military force against a target (JP 3-0).
- *Munitions effects assessment* is an assessment of the military force in terms of the weapon system and munitions effectiveness (JP 2-01).
- Reattack recommendation.

### Assessment in Targeting Methodology

**4-186.** Together, BDA and MEA inform the commander of effects against targets and target sets.





FOR OFFICIAL USE ONLY

The threat's ability to make and sustain war is estimated continually. During the effects review of the targets, restrike recommendations are proposed or executed. BDA pertains to the results of attacks on targets designated by the commander. Producing BDA is primarily an intelligence responsibility, but requires coordination with operational elements. BDA requirements are translated into PIRs. BDA—

- Is used, at the tactical level, by commanders to obtain a series of timely and accurate snapshots of their effect on the enemy. BDA provides commanders an estimate of the enemy's combat effectiveness, capabilities, and intentions. From this information, commanders determine when or whether their targeting effort accomplishes their objectives.
- Helps determine if a restrike is necessary. Commanders use BDA to allocate or redirect attack systems to make the most effective use of available combat power.

### Munitions Effects Assessment

**4-187.** The S-3, G-3, or J-3, through the targeting team, performs MEA concurrently and interactively with BDA as a function of combat assessment. From the MEA, changes are recommended to increase effectiveness in—

- Methodology.
- Tactics.
- Weapons systems.
- Munitions.
- Weapon delivery parameters.

**4-188.** Munitions effect on targets is calculated by determining rounds fired on specific targets divided by artillery assets. The targeting team may generate modified commander's guidance concerning—

- Unit, basic load.
- Required supply rate.
- Controlled supply rate.

### Battle Damage Assessment

**4-189.** BDA for specific HPTs is determined during the decide function. BDA is recorded on the AGM and the ISR synchronization matrix. The resources used for BDA are the same resources used for target development and TA. An asset used for BDA may be unavailable for target development and TA. The analysis and control element (ACE) receives, processes, and disseminates to the targeting team, attack results that are analyzed in terms of desired effects. The targeting team should consider the following BDA principles:

- BDA should measure what is important to commanders; it should not make important what is easily measurable.
- BDA should be objective. When an intelligence staff receives a BDA product from another echelon, the conclusions should be verified if time permits. Intelligence staff at all echelons strive to identify and resolve discrepancies among the BDA analysts at different headquarters.
- The assessment's degree of reliability and credibility relies largely on ISR resources. The quantity and quality of ISR assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (an estimation). Effective BDAs use more than one intelligence discipline to verify each conclusion.

**4-190.** Combat assessment has two components. (See table 4-6.) Each requires different sensors, analytical elements, and timeliness; however, these are not necessarily subcomponents of each report. (See FM 6-0.) Combat assessment consists of more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information, such as—

- Whether the targets are moving or hardening in response to the attack.
- Changes in deception efforts and techniques.
- Increased communication efforts due to jamming.
- Whether the effect achieved is affecting the enemy's combat effectiveness as expected.




FOR OFFICIAL USE ONLY

**4-191.** BDA may simply be compiled information about a particular target or area, for example, the area's cessation of fires. If BDA is developed, the targeting team gives intelligence acquisition systems adequate warning to direct sensors at the target at the right time. BDA outcomes may result in changed plans and collapsed decision times. The targeting team periodically updates earlier decisions made during the decide function concerning—

- IPB products.
- HPTLs.
- TSS.
- AGMs.
- ISR synchronization tools.
- OPLANs.

**Table 4-6 Combat assessment tasks**

| *Components* | *Description* |
|---|---|
| ***Physical damage assessment*** | • Quantitative physical damage from munitions blast, fragmentation, or fire.<br>• Based on observed or interpreted damage. |
| ***Functional damage assessment*** | • Estimates the effects on the target's capability to perform its mission.<br>• Assessment based on all-source intelligence.<br>• Includes a time estimate required to reconstitute or replace the target.<br>• Temporary assessment—compared to a target system assessment—used for specific missions. |

**4-192.** From the BDA and MEA, the S-2, G-2, or J-2 or the S-3, G-3, or J-3 considers the achievement of operational objectives and makes recommendations to the commander. Reattack and other recommendations address operational objectives relative to the—

- Target.
- Target critical elements.
- Target systems.
- Enemy combat force strengths.



**4-193.** Combat assessment key players include the commander, operations officer, fire support coordinator, Army aviation officer, air liaison officer, and S-2, G-2, or J-2. The S-2, G-2, or J-2 integrates intelligence and operational data. In coordination with the S-3, G-3, or J-3, the S-2, G-2 or J-2—

- Develops HVTs.
- Develops and recommends information requirements, including those for targeting. Some requirements become PIRs.
- Coordinates with the S-3, G-3, or J-3, aviation officer, and fires cell to develop a fully coordinated targeting and assessment plan.
- Requests ISR support from the appropriate unit or agency to collect information that satisfies the commander's targeting objectives and reporting requirements.
- Establishes procedures to ensure reports from forward observers, scouts, troops in contact, and pilots are available for analysis.
- Matches reporting requirements against the commander's objectives to determine targeting effort drain, develops and maintains historical databases, and disseminates hard and soft copy intelligence and results.
- Uses the results of combat assessment to determine further threat COA development:
  - Determines priority for ISR assets between the targeting effort and the BDA supporting requirements.
  - Determines and updates enemy capabilities based on targeting effort results.

## INTELLIGENCE SUPPORT TO OPERATIONS SECURITY

**4-194.** OPSEC is concerned with protecting the safety and security of the Nation and Soldiers in the field. OPSEC coordinates all actions taken to deny the enemy information concerning military



FOR OFFICIAL USE ONLY

activities or operations. OPSEC includes the daily activities taken to deny an enemy any usable information. This information includes such things as equipment descriptions and capabilities, the number of personnel within a unit, and what training they receive. Whether classified or unclassified, almost any information can be of use to the threat.

**4-195.** OPSEC protects critical information from threat observation and collection in ways that traditional security programs cannot. While these programs, such as information security, protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

**4-196.** In simple terms, the OPSEC process identifies the critical information of military plans, operations, and supporting activities and the indicators that can reveal that information. It then develops measures to eliminate, reduce, or conceal those indicators. For more information on OPSEC, refer to AR 530-1 and FM 3-13.

## Operations Security Definition

**4-197.** *Operations security* is a process of identifying critical information and subsequently analyzing friendly actions involved in military operations and other activities to—

- Identify those actions that can be observed by threat intelligence systems.
- Determine indicators that threat intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- Select and execute measures that eliminate or reduce-to an acceptable level-the vulnerabilities of friendly actions to threat exploitation (JP 3-13.3).

**4-198.** OPSEC applies across the spectrum of conflict to all Army operations and supporting activities, All Army units at battalion level and higher—including equivalent table of distribution and allowances (TDA) organizations—will have functional, active, and documented OPSEC programs. Army activities, agencies, installations, and staff organizations have functional, active, and documented OPSEC programs. These programs use the process described in AR 530-1 to identify and protect critical information.



## The OPSEC Process

**4-199.** OPSEC applies to any plan, operation, program, project, or activity. It provides a framework for the systematic process necessary to identify and protect critical information. The process is continuous. It considers the changing nature of critical information, as well as the threat assessments and vulnerability assessments throughout the duration of the activity. OPSEC uses a five-step process:

- **Identification of critical information.** Determine what information needs protection.
- **Analysis of threats.** Identify the adversaries and how they can collect information.
- **Analysis of vulnerabilities.** Analyze what critical information friendly forces are exposing.
- **Assessment of risk.** Assess what protective measures should be implemented.
- **Application of appropriate OPSEC measures.** Apply countermeasures that protect critical information.

**4-200.** Personnel must know the unit or organization's OPSEC measures and practice them consistently and continuously. The OPSEC officer should see that training regarding OPSEC measures is included in organization's annual training guidance.

**4-201.** The OPSEC program must be coordinated and synchronized with the other security programs of the command's or organizations, such as information security, information assurance, physical security, and protection. This ensures that the security programs do not provide conflicting guidance. They should work together to support each other.


FOR OFFICIAL USE ONLY

**4-202.** Information does not have to be classified to be of intelligence value. Casual discussions about unit strength, morale, training, equipment and readiness—while not always classified—can be valuable to hostile agents. OPSEC actions are as simple as keeping telecommunications brief and to the point, avoiding gossip—even about nonsensitive information—and making sure that the person requesting information has a need to know before releasing any information.

**4-203.** Key points are—

- OPSEC is an analytic process.
- OPSEC is threat-oriented.
- Every operation has vulnerabilities.
- All indicators cannot be eliminated.
- Risk can be mitigated but not avoided.
- An effective countermeasure (anything that works) is a good countermeasure.

## Counterintelligence Support to OPSEC

**4-204.** CI support to OPSEC involves identifying adversary intelligence, TTP, collection methods, analysis, and exploitation capabilities that target friendly EEFIs, and then developing countermeasures.

**4-205.** CI investigations, CI source operations, debriefing of DOD personnel, and screenings of local nationals and contract linguists can determine what EEFIs are being targeted by foreign intelligence and what adversary collection methods and capabilities are being utilized to collect EEFIs. Additionally, cyber-CI elements can perform Internet open-source collection and DOD network and systems analysis to determine OPSEC vulnerabilities and provide support to the Army network threat and vulnerability assessments (VAs). The information provided by CI aids OPSEC planners in identifying and protecting EEFIs, identifying OPSEC indicators, and developing OPSEC measures.



**4-206.** The U.S. Army Intelligence and Security Command (NSCOM) provides data on the foreign intelligence threat, terrorist threat, and CI support to OPSEC programs for Army units, Army Service component commands, direct reporting units, and above. INSCOM elements provide information updates, but do not write threat assessments for the supported command or agency. (The supported organization's intelligence staff performs this function.) Due to changes in AR 530-1, CI support to OPSEC occurs as resources permit. CI may also provide threat briefings and training concerning the protection of U.S. classified information.


FOR OFFICIAL USE ONLY

# Chapter 5

# Intelligence Training

## INTRODUCTION

**5-1.** Military intelligence (MI) training is a continuing process. From initial training through first assignment and beyond, intelligence Soldiers can expect to continually update their skills through both formal and informal means. This process is seen at the unit level in the Army force generation (ARFORGEN) process, during which intelligence Soldiers continually train and use their skills.

**5-2.** This chapter provides an overview of the training available from various organizations, including the U.S. Army Intelligence Center of Excellence (USAICoE) and the U.S. Army Intelligence and Security Command (INSCOM). Unit training is based on guidance received from, and coordinated with, these organizations. For more information on the military occupational specialties (MOSs) and areas of concentration (AOCs) discussed here, see appendix G. For contact information regarding these courses, see appendix H.



## ARMY FORCE GENERATION DRIVES TRAINING MANAGEMENT

**5-3.** The Army prepares and provides campaign-capable expeditionary forces through ARFORGEN. ARFORGEN applies to Regular Army, and Reserve Component (Army Reserve and Army National Guard) units. It is a process that progressively builds unit readiness over time, during predictable periods of availability, to provide trained, ready, and cohesive units prepared for operational deployments. ARFORGEN takes each unit through a three-phase readiness cycle: reset, train/ready, and available. (See FM 7-0.)

**5-4.** Units enter the reset phase when they redeploy from long-term operations or complete their planned deployment window in the available force pool. Units perform individual and collective training on tasks that support their full spectrum operations mission-essential task lists (METLs).

**5-5.** Units move to the train/ready phase when they are prepared to perform higher level collective training and prepare for deployment. Units with a mission progress as rapidly as possible to achieve mission capability. Prior to receiving a mission, units focus on developing their capabilities. In addition to preparing for operational requirements, Army Reserve Component units train for homeland security and homeland defense missions. Army National Guard units train to meet state-established requirements as well. Combatant command requirements accelerate the process as needed and influence when units are manned, equipped, and trained. Forces and headquarters deploying to an ongoing operation, or available for immediate alert and deployment to a contingency, are in the available phase. At the end of the available phase, units return to the reset phase and the cycle begins again.

**5-6.** Both the generating force and the operational Army participate in and respond to ARFORGEN. The generating force supports operational Army training. Operational Army commanders develop plans for training mission-essential tasks. Commanders prioritize resource allocation based on the following factors—

- Time available.
- Training time required.
- Resource availability.
- The mission.



FOR OFFICIAL USE ONLY

**5-7.** The generating force adjusts levels of support to meet operational Army requirements.

## Modular Force Effects on Training Management

**5-8.** Modular units are tailored through ARFORGEN to meet specific mission requirements. Force packages often are composed of units from multiple commands and installations. Thus, modular brigades often deploy and work for a headquarters other than the one exercising administrative control (ADCON) over them. Senior commanders are responsible for the training and readiness of these units until they are assigned or attached to a force package. As a result, both commanders exercising ADCON and future force package commanders can influence the development, resourcing, and execution of unit training plans and deployment preparation. However, unit commanders are ultimately responsible for the training, performance, and readiness of their units.

## Training Relationships



**5-9.** A key ARFORGEN tenet is that home station training responsibilities remain more static than dynamic, minimizing mission command turbulence before deployment. Commanders providing units retain training responsibility—even after a subordinate unit is mission-sourced into an expeditionary force package—until the unit is actually assigned or attached to the expeditionary force package. Force package commanders normally influence the training of units projected for assignment or attachment to the force package by exercising coordinating authority, once delegated, with the providing commander. (See FM 3-0, see FM 2-0.) Force package headquarters periodically provide a training and readiness summary on assigned and attached units to their postdeployment headquarters to facilitate training plans for reset.

## Reserve Component Training Responsibilities

**5-10.** Reserve Components have the additional challenges of interstate coordination and balancing METL training with homeland security requirements. Mission command of Army National Guard units in a Title 32, United States Code (32 USC), status is exercised by the state governor or adjutant general. U.S Army Reserve units are under Title 10 USC. Army Reserve units based in the continental United States are under the ADCON of the Army Reserve Command.

**5-11.** Before mobilization, Reserve Component commanders are supported by available Army training assets and capabilities. When mobilized, Reserve Component units are attached to a gaining headquarters. Most ADCON responsibilities then shift to the gaining headquarters, which becomes the supported command for training.

## Training Fundamentals

**5-12.** MI training requirements are generated by the U.S. Army Training and Doctrine Command (TRADOC) and the critical task list (see below). The requirements are developed by USAICoE. ARFORGEN requirements also impact training, as discussed above.

**5-13.** MI training is broken into three main areas (See figure 5-1):

- Institutional training performed by USAICoE at Fort Huachuca, Arizona.
- Unit training performed by a Soldier's assigned unit.
- Specialized training performed by INSCOM.



FOR OFFICIAL USE ONLY

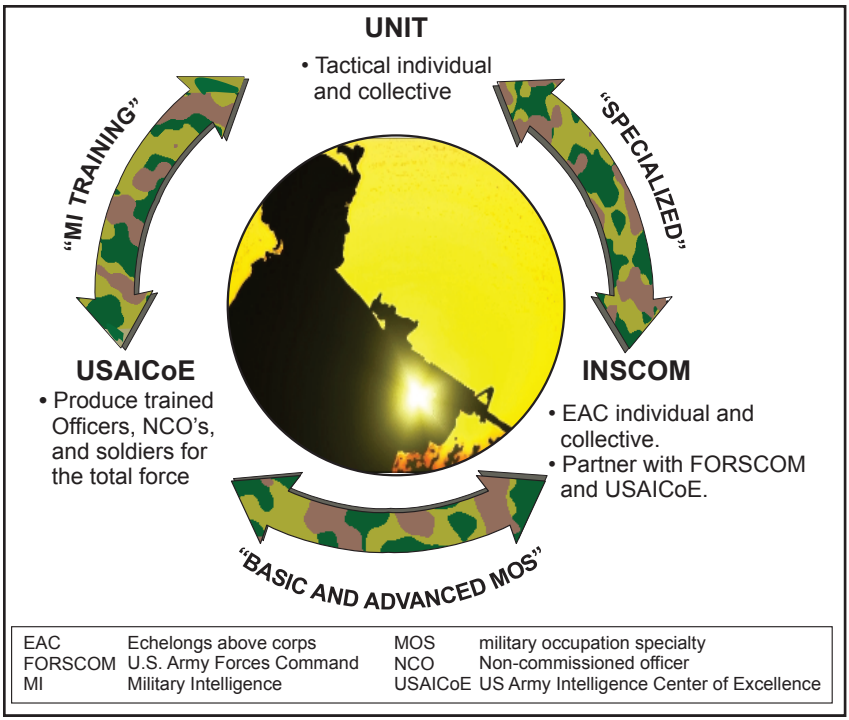



**Figure 5-1. MI training diagram**

## Army Universal Task List

**5-14.** The Army universal task list (AUTL) is a doctrinal foundation and catalog of the Army's tactical collective tasks. The AUTL is written for units at corps level and below. It assists the commander in developing the METL. (See FM 7-15.).

## Critical Task Lists

**5-15.** Critical task lists are assigned to every MOS and specific to the skill levels one through four. They are generic to the MOS and standardized to ensure consistency of training across the Army.

**5-16.** Every two years a critical task and site selection board convenes for each MOS to review the current critical task list and make changes as necessary. It is important to have as many units as possible participate in these boards to ensure that new tasks are captured and tasks that are no longer required are deleted, focusing limited training resources on tasks and skills Soldiers need.





FOR OFFICIAL USE ONLY

# U.S. ARMY INTELLIGENCE CENTER OF EXCELLENCE

**5-18.** USAICoE leads, trains, equips, and supports ARFORGEN and the world's premier corps of MI professionals, who are imbued with the warrior ethos, adaptable, and prepared to perform in a unified action environment upon arrival.

**5-19.** USAICoE performs training at Fort Huachuca, Arizona, and other continental United States locations, and has mobile training teams deployed worldwide.

## 111th Military Intelligence Brigade

**5-20.** The 111th MI Brigade trains technically and tactically competent, adaptive, values-based Soldiers and leaders. The 111th MI Brigade is the primary MI training center for the Army. Three battalions perform training at Fort Huachuca while a fourth is headquartered in Texas and performs training in Texas and Florida. The 111th MI Brigade trains Army intelligence and members of all Services, as well as select civilians and members of foreign militaries. Component battalions of the 111th MI Brigade and their associated duties follow.



### 304th Military Intelligence Battalion

**5-21.** This battalion is primarily responsible for performing officer and warrant officer training. The 304th MI Battalion performs Soldier and leader training.

### 305th Military Intelligence Battalion

**5-22.** This battalion is primarily responsible for performing analyst and aviator training. The 305th MI Battalion is one of the largest MI battalions in the Army, with the mission of performing initial entry training (IET) and military occupational skills-transfer training. They train Soldiers as intelligence analysts, imagery analysts, Common Ground Station operators, system maintainers and integrators, and in the Special Electronic Mission Aircraft Army Aviators course. The trainers provide the skills necessary to support Army commanders.

### 309th Military Intelligence Battalion

**5-23.** The 309th MI Battalion trains 09L interpreters/translators and human intelligence (HUMINT) collection and counterintelligence (CI) professionals.

### 344th MI Battalion

**5-24.** This battalion is headquartered at Goodfellow Air Force Base, Texas. The 344th MI Battalion is primarily responsible for performing signals intelligence (SIGINT) training.

## Courses of Instruction

**5-25.** The USAICoE provides MOS- and AOC-producing courses (table 5-1) and functional courses.



FOR OFFICIAL USE ONLY

Table 5.1 MOS- and AOC-producing courses

| *Commissioned Officer* | *Warrant Officer* | *Enlisted Soldier* |
|---|---|---|
| 35D All-source Intelligence Officer. | 350F All-source Intelligence Technician. | 09L Interpreter/Translator. |
| 35E Counterintelligence (CI) Officer. | 350G Imagery Intelligence Technician. | 35F (96B)* Intelligence Analyst. |
| 35F Human Intelligence (HUMINT) Officer. | 350Z Attaché Technician. | 35G (96D) Imagery Analyst. |
| 35G Signals Intelligence (SIGINT)/Electronic Warfare Officer. | 351L CI Technician. | 35H (96H) Common Ground Station Operator. |
| | 351M HUMINT Collection Technician. | 35L (97B) CI Agent. |
| | 351Y Area Intelligence Technician. | 35M (97E) HUMINT Collector. |
| | 352N Traffic Analysis Technician. | 35N (98C) SIGINT Analyst. |
| | 352P Voice Intercept Technician. | 35P (98G) Cryptologic Linguist. |
| | 352S Non-Morse Intercept Technician. | 35S (98Y) Signals Collector/ Analyst. |
| | 353T Intelligence/Electronic Warfare Systems Maintenance Technician. | 35T (33W) Military Intelligence Systems Maintainer/Integrator. |
| | | 35X (96Z) Intelligence Senior Sergeant. |
| | | 35Y (97Z) CI/ HUMINT Senior Sergeant. |
| | | 35Z (98Z) SIGINT Senior Sergeant. |

*Parentheses in enlisted Soldier column indicate former MOS designators.





FOR OFFICIAL USE ONLY

### Functional Courses

**5-26.** The functional courses listed below prepare a Soldier to carry out specialized duties according to assignment:

- MI Pre-Command.
- Brigade Combat Team S-2.
- G-2X/S-2X.
- 09L MOS.
- Electronic Warfare Tactical Practitioner.
- Intelligence Master Analyst.
- Air Force Tactical Receive.
- Intelligence, Surveillance, and Reconnaissance (ISR) Manager.
- Information Systems Security Monitoring.
- Basic Foreign Instrumentation SIGINT.
- Intelligence in Combating Terrorism.
- RC-12 Guardrail Systems Qualification.
- Guardrail/Common Sensor Pilot Qualification.
- Contemporary Operating Environment.
- Defense Intelligence Agency (DIA) Strategic Debriefing.
- Communications Control Set.
- TROJAN SPIRIT.
- Intelligence Workstation Certification.
- Tactical Exploitation System.
- Combat Tracking.



### Noncommissioned Officer's Academy

**5-27.** The mission of the Noncommissioned Officer's Academy (NCOA), based at Fort Huachuca, Arizona, is to execute resident training to noncommissioned officers (NCOs) in order to develop their leadership and technical skills so that they emerge as confident and competent warriors able to perform and lead unit-level and intelligence operations for an Army and Nation at war, in alignment with the ARFORGEN model. The academy develops and sustains a world-class cadre and fosters teamwork with USAICoE while caring for Soldiers, civilians, and their families.

**5-28.** The NCOA teaches two courses:

- MI Advanced Leader course (previously the Basic Noncommissioned Officer's course) prepares NCOs for platoon operations and technical intelligence competence.
- MI Senior Leader course (previously the Advanced Noncommissioned Officer's course) prepares senior NCOs for company operations, first sergeant leadership and training aspects, and supervisory intelligence operations.

### New Systems Training and Integration Division

**5-29.** The New Systems Training and Integration Division at Fort Huachuca manages training development for new and product-improved intelligence systems and capabilities. It also oversees the development of systems and nonsystems training devices.

### Joint Intelligence Combat Training Center

**5-30.** The 304th MI Battalion operates the Joint Intelligence Combat Training Center (JICTC). JICTC is the premier capstone exercise for the 111th MI Brigade. JICTC trains intelligence professionals and organizations at the USAICoE to successfully execute their mission in a unified action environment. JICTC performs a seven-day intelligence battle staff exercise called Exercise Eagle II. Exercise Eagle II is a multiechelon, multilayered training event based on real-world threats fought on real-world terrain. JICTC uses realistic scenarios modeled on real-world operations. The JICTC trains MI officers, warrant officers, NCOs, and enlisted Soldiers together during the exercise.

**5-33.** JICTC also trains Regular Army, and Reserve Component unit intelligence staffs and sections. Eagle II provides commanders and senior intelligence officers an opportunity to do the following: exercise the intelligence staff during the "walk" and "run" phase of training; reinforce essential skills prior to unit staff group training or unit collective training; and evaluate their leadership and intelligence staff. Commanders can also leverage the JICTC during the "ready" phase of the ARFORGEN process to provide theater-specific training.



FOR OFFICIAL USE ONLY

**5-34.** JICTC holds 20 to 25 exercises per year. The intelligence exercise allows intelligence professionals to perform practical training and gain understanding of the intelligence process in a collective training environment. Students receive practical experience on the targeting process, the ISR activity, and all-source analysis.

**5-35.** Battle simulations replicate the real-world operational environment. JICTC uses a six-month snapshot of time, taken directly from Iraq-based scenarios. It uses actual message traffic and products; current tactics, techniques, and procedures; and systems that are currently used in Iraq. The exercise portrays situations, message traffic, reports, and intelligence products used by deployed units in Iraq. Students use the systems to access information, intelligence reports, products, and real-world databases on secure Internet networks.

**5-36.** JICTC's goal is to produce competent intelligence officers, NCOs, and Soldiers trained on the most current intelligence systems and applications and tools, able to provide intelligence support for the commander's operations in a unified action environment.

## UNIT-BASED TRAINING



**5-37.** After trained intelligence Soldiers arrive at their assignments they train on their specific duties as members of units. Unit-based training ensures that intelligence Soldiers understand and can perform their mission and meet established standards. These standards are based on the AUTL and critical task list, as well as standards specific to the assigned unit.

**5-38.** Training support comes from organic trainers who have received training at outside locations and from mobile training teams. These teams can be furnished by USAICoE, INSCOM, and other organizations through various programs.

**5-39.** MI Soldiers receive open-source intelligence (OSINT) training at their schools, as applicable. Upon arrival at their assignments, unit training should include OSINT training relevant to their duty assignments.

## U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

**5-40.** INSCOM's primary contribution to the training and readiness of Army intelligence units below corps level is the Foundry Program. Foundry provides advanced training opportunities for MI units and Soldiers; training is provided by INSCOM Soldiers and the intelligence community. Foundry also provides cadre, equipment, and regionally focused training at established corps and division Foundry platforms. These platforms provide multidisciplined advanced training and tactical overwatch, giving deploying units a predeployment mission engagement capability.

**5-41.** The Foundry Program gives commanders the means to achieve their priority intelligence training. The goal of the Foundry Program is to provide Soldiers with focused intelligence training to meet their commander's training and readiness requirements, a steady-state regional focus, functional expertise, technical training, and operational readiness opportunities. Soldiers in the Foundry Program receive training that builds on institutional, unit, and individual training and reflects the current and changing operational environment. The training increases functional and regional expertise while developing and expanding contacts within the greater intelligence community. Additionally, the Foundry Program develops and implements longer term sustainment training capabilities through home station training sites. Coordination for Foundry Program execution is primarily through the INSCOM Foundry Program administrator.

**5-42.** Foundry training methods are classroom/immersion, mobile training team, live environment



FOR OFFICIAL USE ONLY

training, and Foundry training sites, which include home station platforms at corps, division, combat training centers, Army Europe, and Army Pacific locations.

**5-43.** Foundry training site opportunities include the following functional areas:
- All-source intelligence.
- SIGINT.
- Geospatial intelligence (GEOINT).
- Measurement and signature intelligence (MASINT).
- HUMINT.
- CI.
- Dialect training.
- Air systems.

**5-44.** Priority for Foundry training is based on five categories:
- **Priority 1.** Soldiers or units in the train/ready force pool with the earliest dates for operational deployments, units on prepare-to-deploy orders, and forces on orders to perform contingency missions.
- **Priority 2.** Other units in the reset and train/ready force pools.
- **Priority 3.** Units that directly or indirectly support the training of tactical forces such as, echelons above corps, MI organizations, and train the trainers.
- **Priority 4.** Training of individual MI Soldiers to augment or supplement tactical forces or support operational missions.
- **Priority 5.** Routine MI skills or systems enhanced training.



**5-45.** Foundry training is not normally used for—
- Army Training Requirements and Resources System courses.
- Courses that award an additional skills identifier or MOS.
- Equipment purchases, including Foundry training equipment.
- Training of untargeted personnel.
- Courses not validated as Foundry opportunities and listed in the Foundry manual of training opportunities.
- Training over 60 days in length.
- Rental of equipment or facilities.
- Contractor-sponsored training events.

## DEPARTMENT OF DEFENSE

**5-46.** Department of Defense (DOD) sponsored programs provide intelligence training to Soldiers and units. These include the HUMINT Training-Joint Center of Excellence (HT-JCOE) and the Defense Language Institute Foreign Language Center (DLIFLC).

### Human Training-Joint Center of Excellence

**5-47.** HT-JCOE, located at Fort Huachuca has the mission to provide advanced, practical-exercise-based, joint HUMINT training; professional development; and certification in several HUMINT fields. These include interrogation, debriefing, and military source operations in support of the requirements of the defense HUMINT enterprise.

**5-48.** HT-JCOE's vision is to provide fully trained and educated HUMINT professionals to the Defense HUMINT Enterprise. HT-JCOE executes training based on common Defense HUMINT Enterprise standards, principles, and procedures to develop the unity of response necessary to influence and shape


FOR OFFICIAL USE ONLY

national HUMINT capabilities. Available courses at HT-JCOE are listed below.

- Advanced Source Operations.
- Joint HUMINT Officer.
- Joint Source Validation.
- Source Operations.
- Defense Strategic Debriefing.
- Joint Interrogation Certification.
- Joint Analyst and Interrogator Collaboration.
- Joint HUMINT Analysis and Targeting.
- Joint Interrogation Management.
- Joint Senior Interrogator.

## Language Training

**5-49.** Language training is performed at the unit or individual level. Funding for language training is available through the Total Army Language Program.



**5-50.** DLIFLC is the proponent for the Defense Foreign Language Program. DLIFLC assists commanders in developing a unit command language program, as well as in maintenance and local evaluation of the program. DLIFLC is regarded as one of the finest schools for foreign language instruction in the Nation. As part of TRADOC, the institute provides resident instruction at the Presidio of Monterey in California in 24 languages and several dialects. Courses are held five days a week, seven hours each day, with two to three hours of homework each night. Courses last between 26 and 64 weeks, depending on the difficulty of the language.

**5-51.** Instruction takes place in eight separate language schools and at the Emerging Languages Task Force, where new surge languages are taught in response to the needs of the sponsoring agencies. The present facilities at the Presidio of Monterey accommodate approximately 3,500 Soldiers, Marines, Sailors, and Airmen, as well as select members from DOD and the U.S. Coast Guard. DLIFLC students must be members of the armed forces or be sponsored by a government agency.

**5-52.** DLIFLC students are taught by more than 1,700 highly educated instructors, 98 percent of whom are native speakers of the languages they teach. Aside from classroom instruction, faculty also write course materials, design the Defense Language Proficiency Tests, and perform research and analysis.

**5-53.** Developments in technology and the Internet permit Soldiers to use their foreign language skills 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 they may attend language courses and live among the local residents. These include the following:
  - International Center at the University of Utah (http://www.international.utah.edu).
  - Worldwide Language Resources (http://www.wwlr.com).
  - National Registration for Language Abroad (http://www.nrcsa.com).
- **International Standards Organization (ISO)-Immersion.** There are commercial and federal programs that provide foreign country environment within the continental United States:
  - Language Enrichment Activities Program, the Foreign Language Training Center, Fort Lewis, Washington.
  - Global Language Systems, Bountiful, Utah (http://www.glsnet.globtra.com/).
- **National Security Agency Joint language centers.** Each of the regional operation centers of the NSA has a language support organization that provides formal language training opportunities:
  - Fort Gordon, Georgia (NSA-G).



FOR OFFICIAL USE ONLY

- Schofield Barracks, Hawaii (NSA-H).
- Medina Annex, Lackland Air Force Base, Texas (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 four military Services conduct language enhancement and language refresher 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 enjoyable ways of learning a foreign language are through movies and television programs. Both foreign and U.S. programs (with foreign subtitles 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. These include the following:
  - Transparent Language (http://www.transparent.com/).
  - Rosetta Stone® (http://www.rosettastone.com also available to the military through Army Knowledge Online [AKO]).
  - Tell Me More (http://www.tellmemorestore.com/).
- **SCOLA®.** This is a nonprofit educational organization that receives and retransmits television programming from around the world in many languages. These programs are available through the Internet to students of language study, ethnic communities, and anyone seeking a global perspective. SCOLA's Web site is http://www.SCOLA.org.
- **Defense Language Institute mobile training teams.** Contact the DLI 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. Many federal programs need linguists. The Reach Language Support Program provides meaningful and challenging translation opportunities to members of the military while providing translations 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 who supports military linguists in personal language program development. The command language program manager 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.** Several language resources are available on the Internet:
  - **Podcasts.** http://www.word2word.com/pod.html.
  - **Google.** This site provides a wealth of language opportunities from music, podcasts, videos, programs, and all sorts of great new technology to support foreign language development (http://www.google.com).
  - **Langnet.** This is a language learning support system with interactive materials designed for those who want to practice and maintain their target language reading and listening skills (http://www.langnet.org).
  - **Foreign language portal.** This contains lists, by foreign language, on the For Official Use Only Army server of foreign language materials (https://www.us.army.mil/suite/doc/5987514).

**5-54.** Rosetta Stone® provides access to courses in over 30 languages. Online access to all 31 Rosetta Stone® language training courses is free to all Regular Army and Reserve Component Soldiers, as well as Army civilian employees and contracted Reserve Officer Training Corps (ROTC) and United States Military Academy (USMA) cadets. The lessons are self-paced and self-directed, Regular Army Soldiers earn one promotion point for each five hours of training credit they complete, while Reserve Component Soldiers earn one retirement point for each three hours of training credit they complete.

## CULTURAL AWARENESS TRAINING

**5-55.** The Professional Military Education Cultural Awareness Training Support Package consists of four levels of training, from initial military training to the captain's career course. The package offers lessons in defining culture, discussions of American and personal culture to determine areas of conflict and biases, the cultures of Iraq and Afghanistan, and the effect of culture on military operations. The training is carried out through multiple practical exercises and situational training exercises.

**5-56.** The U.S Army Training and Doctrine Command Culture Center (TCC) at Fort Huachuca provides cultural awareness training and resources to enhance awareness and maintain foreign language proficiency. Lectures at the TCC are part of the ongoing effort to bring cultural awareness to the forefront of strategic and tactical decisionmaking for commanders throughout the military services.





FOR OFFICIAL USE ONLY

# Chapter 6

# Intelligence Systems

## INTRODUCTION

**6-1.** The intelligence Soldier uses many systems to collect and process information that is communicated as intelligence. This chapter is an overview of the types of systems that the intelligence Soldier is most likely to encounter and use in the field.



## SYSTEMS

**6-2.** *Systems* are functionally, physically, and/or behaviorally related groups of regularly interacting or interdependent elements that form a unified whole (JP 3-0).

**6-3.** An *intelligence system* is any formal or informal system to manage data gathering, to obtain and process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks (JP 1-02). Systems used by the intelligence Soldier depend upon the type of unit, its mission, and its physical location. Equipment is constantly being developed and superseded by new models or versions. Systems shown in the accompanying appendixes are current as of the date of this publication. The successful intelligence Soldier is knowledgeable about current systems and capabilities and is flexible to future changes and enhancements.

### Types of Systems

**6-4.** Systems described in this publication may be one of the four listed below. Each system listed in the appendices will be annotated with the status of the system.

- **Developmental**—A system suitable for evaluation and performance that is not scheduled for production.
- **Prototype**—A system suitable for evaluation of design, performance, and production potential.
- **Quick Reaction Capability (QRC)**—A system used in the field to meet specific requirements.
- **Program of Record (POR)**—A system that has been evaluated and accepted for production.

### Functions of Intelligence Systems

**6-5.** Intelligence systems perform three primary functions:

- Collection.
- Processing.
- Communications and communications support..

#### Collection Systems

**6-6.** Collection systems comprise handheld, manned, unmanned collection and sensor systems. The gather the information that is subsequently processed into intelligence. A collection asset is a system, platform, or capability that is supporting, assigned, or attached to a particular commander. Detailed information about intelligence collection systems is in appendix I.



FOR OFFICIAL USE ONLY

### Processing Systems

**6-7.** A processing system is designed to convert raw data into useful information. Detailed information about intelligence processing systems is in appendix J.

### Communications and Communicaitons Support Systems

**6-8.** *Communications systems* are networks and information services enable joint and multinational warfighting capabilities (JP 6-0). Detailed information about intelligence communications systems is in appendix K.



FOR OFFICIAL USE ONLY

# Appendix A

# Intelligence Products, Facilities, and Networks

## INTRODUCTION

**A-1.** This appendix covers essential, intelligence-related terminology as well as topics that intelligence Soldiers may find useful as they assume their duties. This appendix focuses on types of intelligence products, sensitive compartmented information facilities (SCIF), and automation networks.

## TYPES OF INTELLIGENCE PRODUCTS

**A-2.** The intelligence staff produces and supports multiple products. The following products are discussed below:

- Running estimate.
- Intelligence running estimate.
- Common operational picture (COP).
- Intelligence estimate.

### Running Estimate

**A-3.** A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (FM 5-0). Running estimates provide information, conclusions, and recommendations from the perspective of each staff section. They are a staff technique to support the commander's visualization and decisionmaking and serve 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 information.

**A-4.** Each staff section produces a running estimate. The major difference between the running estimate and the former staff estimate is that the staff not only continuously updates the information in the running estimate, but also continuously updates the conclusions and recommendations while including projections of future conditions in the area of interest.

### Intelligence Running Estimate

**A-5.** The *intelligence running estimate* aids the intelligence staff in tracking and recording pertinent information. It is used to make recommendations to the commander. When applied to the COP, it is a continuous flow and presentation of relevant information and predictive intelligence. When this estimate is combined with the other staff running estimates, it complements the commander's visualization and situational understanding of the area of interest in order to achieve information superiority.

**A-6.** The intelligence running estimate details the intelligence staff's ability 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 furnishes predictive estimates of future threat activity.

The intelligence running estimate consists of all the continuously updated and monitored intelligence available. This is specific intelligence relevant to support current and projected future operations.

**A-7.** The generate intelligence knowledge continuing activity of the intelligence process directly supports the development of the intelligence running estimate, which is then refined and improved following mission analysis. It is further refined and improved based on the results of intelligence surveillance, and reconnaissance operations. The intelligence running estimate is updated as required, based on changes in the threat situation, terrain and weather, and civil considerations. The intelligence running estimate includes—

- Situation and considerations.
- Mission.
- Courses of action (COAs).
- Analysis (threat-based).
- Comparison (threat-based).
- Recommendations and conclusions.

**A-8.** The successful intelligence Soldier clearly understands the weather and terrain effects and is able to visualize the area of operations to develop and maintain the intelligence running estimate. This understanding facilitates accurate assessments and projections regarding the—

- Threat.
- Threat situation (including strengths and weaknesses).
- Threat capabilities and an analysis of those capabilities (COAs available to the threat).
- Conclusions drawn from that analysis.
- Foreign intelligence and international terrorist threat assessment.

**A-9.** The intelligence running estimate details threat characteristics, threat capabilities, and projections of future threat actions.

## Common Operational Picture

**A-10.** Army doctrine defines the *common operational picture* as a single display of relevant information within a commander's area of interest, tailored to the user's requirements, and based on common data and information shared by more than one command (FM 3-0). The COP is the primary tool for facilitating the commander's situational understanding. All staff sections provide input from their area of expertise to the COP.

**A-11.** 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. The Distributed Common Ground System-Army (DCGS-A) is the means for integrating this information into the COP.

## Intelligence Estimate

**A-12.** An *intelligence estimate* is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption (JP 2-0). The intelligence staff develops and maintains the intelligence estimate.

# SENSITIVE COMPARTMENTED INFORMATION FACILITY

**A-13.** SCIFs are facilities used to store, process, and discuss sensitive compartmented information (SCI). SCI material relates either to specific national security topics or programs whose existence may not be publicly acknowledged or to information that requires special handling because of the sensitive nature of the material or program. The standards for construction and maintenance of SCIFs are established by the Director of Central Intelligence and are referenced below.

**A-14.** A SCIF is an accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or electronically processed. SCIFs have personnel access controls to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent—as well as detect—any visual, acoustical, technical, or physical access by unauthorized people. Physical security criteria vary, based on whether the SCIF is in the United States or elsewhere and varies according to the following conditions: closed storage, open storage, continuous operations, and secure working area.

**A-15.** Compliance with Director of Central Intelligence Directive (DCID) 6/9 is mandatory for all SCIFs established after 18 November 2002, including those that make substantial renovations to existing SCIFs. SCIFs approved before that date do not require modification to meet the DCID standards.

**A-16.** The physical security safeguards set forth in DCID 6/9 are the standards for the protection of SCI. Senior officials of the intelligence community (SOICs), with the Director of Central Intelligence's concurrence, may impose more stringent standards if extraordinary conditions and circumstances warrant. SOICs may not delegate this authority. Additional costs resulting from the imposition of more stringent standards shall be borne by the requiring agency, department, or relevant contract.

**A-17.** In situations where conditions or unforeseen factors render full compliance with these standards unreasonable, the SOIC or designee may waive specific requirements in accordance with DCID 6/9. However, this waiver must be in writing and must specifically state what has been waived. The cognizant security authority must notify all co-utilizing agencies of any waivers it grants. All SCIFs must be accredited by the SOIC or a designee prior to performing any SCI activities.

**A-18.** One person is now authorized to staff a SCIF, eliminating the two-person rule.

## Concept

**A-19.** SCIF design balances threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk. Each security concept or plan must be submitted to the cognizant security authority for approval. Protection against surreptitious entry, regardless of SCIF location, is always required. Security measures must be taken to deter technical surveillance of activities taking place within the SCIF. TEMPEST security measures must be considered if electronic processing of SCI is involved.

**A-20.** In military and civilian compounds, security controls such as identification checks, perimeter fences, police patrols, and other security measures may exist. When considered together with the SCIF location and internal security systems, those controls may be sufficient for use in lieu of certain physical security or construction requirements contained in DCID 6/9.

**A-21.** Proper security planning for a SCIF is designed to deny foreign intelligence services and other unauthorized personnel the opportunity to enter undetected into those facilities and exploit sensitive

activities or materials. Faulty security planning and equipment installation jeopardizes security and wastes money. Adding redundant security features causes extra expense, wasting money that could be used on other needed features. When security features are neglected during initial construction, retrofitting of existing facilities to comply with security requirements is necessary.

## SCIF Accreditation

**A-22.** The cognizant security authority ensures SCIFs comply with DCID 6/9. The cognizant security authority is authorized to inspect any SCIF, direct any deficient situation to be corrected, and withdraw SCIF accreditation. The procedures for establishing and accrediting SCIFs are:

- The procedures for establishment and accreditation of SCIFs from conception through construction must be coordinated and approved by the SOIC or cognizant security authority.
- SCI shall never be handled, processed, discussed, or stored in any facility other than a properly accredited SCIF unless written authorization is granted by the cognizant security authority.

**A-23.** An inspection of the SCIF shall be performed by the cognizant security authority or appointed representative prior to accreditation. Periodic reinspections shall be based on threat, physical modifications, sensitivity of programs, and past security performance. Inspections may occur at any time. Inspections may be announced or unannounced. The completed fixed facility checklist will be reviewed during the inspection to ensure continued compliance. Technical surveillance countermeasures evaluations may be required at the discretion of the cognizant security authority, as conditions warrant. Inspection reports shall be retained within the SCIF and by the cognizant security authority. All SCIFs shall maintain, on site, current copies of the following documents:

- DCID 6/9 Fixed Facility Checklist.
- Accreditation authorization documents, such as those dealing with physical security, TEMPEST, and automated information systems.
- Inspection reports, including TSCM reports, for the entire period of SCIF accreditation.
- Operating procedures, special security officer contractor/special security officer (CSSO/SSO) appointment letters, memoranda of agreement, emergency action plans (EAPs), and similar documents.
- Copies of any waivers granted by the cognizant security authority.

## Ground Operations

**A-24.** Establishing an operating a SCIF in ground operations has many facets, and there are many rules that vary with the type of operation. Successful intelligence personnel are familiar with the varied requirements.

### Purpose

**A-25.** This section outlines the physical security requirements for operation of a SCIF while in a field or tactical configuration, including training exercises. It also addresses the standards for truck-mounted or towed-trailer-style shelters designed for use in a tactical environment but used in a garrison environment. These are known as a semipermanent SCIF.

### Applicability and Scope

**A-26.** Recognizing that field and tactical operations, as opposed to operations within a fixed military installation, are considered less secure, minimum physical security requirements must be met and maintained. Situation and time permitting, the minimum standards will be improved upon by using the security considerations and requirements for permanent secure facilities as an ultimate goal. If available, permanent-type facilities will be used. Under field or combat conditions, a continuous 24-hour operation is mandatory. Every effort must be made to obtain the necessary support—such as security containers,

vehicles, generators, fencing, guards, and weapons—from the host command.

### Tactical SCIF

**A-27.** A tactical SCIF (T-SCIF) should be located within the defensive perimeter of the supported headquarters and preferably also within the command post perimeter.

- The T-SCIF shall be established and clearly marked using a physical barrier. Where practical, the physical barrier should be triple-strand concertina or general purpose barbed tape obstacle. The T-SCIF approval authority shall determine whether proposed security measures provide adequate protection based on local threat conditions.
- The perimeter shall be guarded by walking or fixed guards who provide observation of the entire controlled area. Guards shall be armed with weapons and ammunition. The types of weapons will be prescribed by the supported commander. Exceptions to this requirement during peace may only be granted by the T-SCIF approval authority based on local threat conditions.
- Access to the controlled area shall be restricted to a single gate or entrance, which will be continually guarded. An access list shall be maintained and access restricted to those people whose names appear on the list. The T-SCIF shall be staffed with sufficient personnel as determined by the on-site security authority, based on the local threat conditions. Emergency destruction and evacuation plans shall be kept current. SCI material shall be stored in lockable containers when not in use.
- Communication shall be established and maintained with backup response forces, if possible.
- When the T-SCIF moves, the SSO or designee shall perform an inspection of the vacated T-SCIF area to ensure SCI materials are not inadvertently left behind.
- Reconciliation of T-SCIF activation and operational data shall be made not more than 30 days after SCIF activation. Interim reporting of SCIF activities may be made to the cognizant security authority.

### Responsibilities

**A-28.** The cognizant security authority is responsible for ensuring compliance with these standards and providing requisite SCI accreditation. The cognizant security authority may further delegate T-SCIF accreditation authority one command level lower. The senior intelligence officer is responsible when a temporary field or T-SCIF is used in support of field training exercises. During a period of declared hostilities or general war, a T-SCIF may be established at any level of accreditation upon the verbal order of a general or flag officer commander.

### Accreditation of Tactical SCIFs

**A-29.** An accreditation checklist is not required for establishment of a T-SCIF. Approval authorities may require use of a local tactical deployment checklist. The element requesting establishment of a T-SCIF shall notify the cognizant security authority or designee prior to commencement of SCIF operations. The message shall provide the following information:

- Identification number of parent SCIF.
- Name of the T-SCIF.
- Deployed from (location).
- Deployed to (location).
- SCI level of operations.
- Operational period.
- Name of exercise or operation.
- Identification of the type of facility used for T-SCIF operations (such as vans, buildings, tents).
- Points of contact (responsible officers).
- Description of security measures for entire operational period of T-SCIF.
- Comments.

### Physical Configuration

**A-30.** A T-SCIF may be configured using vehicles, trailers, shelters, bunkers, tents, or available structures to suit the mission. Selection of a T-SCIF site should always consider effective and secure

mission accomplishment.

### Tactical SCIF Operations Using Vans, Shelters and Vehicles

**A-31.** When a rigid-side shelter or portable van is used for SCI operations, it must be equipped with either a combination lock that meets all requirements of federal specification FF-L-2740 or other lock approved by the cognizant security authority. The combination to the lock or keys shall be controlled by the SSO at the security level for which the T-SCIF is accredited. The shelter or van shall be secured at all times when not being used as a SCIF.

**A-32.** The SCIF entrance of a radio-frequency-shielded enclosure designed for tactical operations may be secured with the manufacturer-supplied locking device or any combination of the locking devices mentioned above.

### T-SCIF Operations within Existing Permanent Structures

**A-33.** A T-SCIF may be operated within an existing structure when—

- The location is selected on a random basis.
- The location is not reused within a 36-month period. If reused within 36 months for SCI discussion, a technical surveillance countermeasures evaluation is recommended.

**A-34.** There is no restriction over SCI discussion within a T-SCIF during war.

### Mobile Signals Intelligence SCIFs

**A-35.** A continuous 24-hour operation is mandatory for mobile signals intelligence (SIGINT) SCIFs. In addition the following conditions must be met:

- The T-SCIF shall be staffed with sufficient personnel, as determined by the on-site security authority, based on the local threat conditions.
- External physical security measures shall be incorporated into the perimeter defense plans for the immediate area in which the T-SCIF is located.
- A physical barrier is not required as a prerequisite to establish a mobile SIGINT T-SCIF.
- External physical security controls will normally be a responsibility of the people controlling the day-to-day operations of the T-SCIF.
- Communications shall be established and maintained with backup guard forces, if possible.
- Emergency destruction plans shall incorporate incendiary methods to ensure total destruction of SCI material in emergency situations.

**A-36.** A rigid-side shelter or a portable van are two possible configurations that may be used. When a rigid-side shelter or portable van is used, it is subject to the following additional restrictions:

- If it is a shelter, it shall be mounted on a vehicle in such a way as to provide the shelter with the capability of moving on short notice.
- A GSA-approved security container shall be permanently affixed within the shelter. The combination to the lock will be protected to the level of security of the material stored therein.
- Entrance to the T-SCIF shall be controlled by SCI-indoctrinated people on duty within the shelter. When situations occur where there are no SCI-indoctrinated people within the shelter, such as during redeployment, classified material shall be stored within the locked GSA container and the exterior entrance to the shelter will be secured.
- Entrance to the T-SCIF shall be limited to SCI-indoctrinated people with an established need-to-know whenever SCI material is used within the shelter.

**A-37.** When a rigid-side shelter or portable van is not available and a facility is required for SCI operations, such as in the case of a soft-side vehicle or man-portable system, the SCIF is subject to the following additional restrictions:

- Protection will consist of an opaque container such as a leather pouch, metal storage box, or other

suitable container that prevents unauthorized viewing of the material.

- This container shall be kept in the physical possession of an SCI-indoctrinated person.
- The quantity of SCI material permitted within the T-SCIF will be limited to that which is absolutely essential to sustain the mission. Stringent security arrangements shall be employed to ensure that the quantity of SCI material is not allowed to accumulate more than is absolutely necessary.
- All working papers generated within the T-SCIF shall be destroyed at the earliest possible time after they have served their mission purpose, preventing accumulation of unnecessary classified material.
- If automated information system (AIS) equipment is used to store or process SCI data, a rapid and certain means of destruction shall be available to automated information system operators to ensure the total destruction of classified material under emergency or combat conditions.
- Upon cessation of hostilities, all classified material shall be returned to the parent element of the SCIF for reconciliation of records and destruction of obsolete material.

### Emergency Action Plans

**A-38.** An EAP will be written. The EAP provides for evacuation and destruction of classified material in the event of emergency, civil unrest, or natural disaster. If (AIS) equipment is used to store or process SCI data, a rapid and certain means of destruction shall be available to AIS operators to ensure the total destruction of classified material under emergency or combat conditions. Evacuation plans and destruction equipment must be approved by the cognizant security authority and tested by mission personnel. Emergency destruction and evacuation plans will be kept current. For an example of an emergency action plan, see DCID 6/9. For more information on SCIFs refer to DCID 6/9.

## AUTOMATION NETWORKS

**A-39.** The intelligence community relies heavily on AIS networks. Successful intelligence officers are familiar with the various networks available to Soldiers.

### Joint Worldwide Intelligence Communications System

**A-40.** The Joint Worldwide Intelligence Communications System (JWICS) is a system of interconnected computer networks used by the Department of Defense (DOD) and the Department of State to transmit classified information—up to and including information classified TOP SECRET and SCI—by packet switching using TCP/IP protocols in a secure environment. JWICS also provides services such as hypertext documents and electronic mail (e-mail). In other words, the JWICS, together with its counterpart, the SECRET internet protocol router network (SIPRNET), is the DOD's classified version of the civilian internet.

### National Security Agency/Central Security Service Classified Network

**A-41.** The National Security Agency/Central Security Service (NSA/CSS) Classified Network is the collection of data and voice networks under the direct operational control of Director NSA/Chief CSS. It provides classified information technology services for the NSA enterprise.

### SECRET Internet Protocol Router Network

**A-42.** The SIPRNET is a system of interconnected computer networks DOD uses to transmit classified information—up to and including information classified SECRET—by packet switching over the (TCP/IP) in a completely secure environment. It also provides services such as hypertext documents and electronic mail.

**A-43.** Except for existing within a secure environment, the SIPRNET is virtually indistinguishable from the internet to the user. Its chief visible difference is the domain name system, with almost all sites being under .smil.mil or .sgov.gov. Among SIPRNET's many features, computers cleared for SIPRNET access—

- Connect to the network via secure dial-up or local area network.
- Access Web pages written in standard HyperText Markup Language.
- Can upload and download files via file transfer protocol connections using a standard Web browser.
- Can send or receive e-mail messages through simple mail transfer protocol services using e-mail programs.

**A-44.** All data transmitted on SIPRNET between secure facilities must be encrypted by approved NSA encryption systems. No access is permitted between SIPRNET and the Nonsecure Internet Protocol Router Network (NIPRNET), although the public internet can be used to transmit encrypted SIPRNET packets.

### Nonsecure Internet Protocol Router Network

**A-45.** NIPRNET is used to exchange unclassified but sensitive information between internal users as well as provide users with access to the internet. NIPRNET comprises internet protocol routers owned by DOD. NIPRNET was created by the Defense Information Systems Agency to replace the earlier military network. NIPRNET is separate but parallel to the SIPRNET and provides seamless interoperability for unclassified combat support applications as well as a gateway to the public internet.

## COLLABORATIVE TOOLS

**A-46.** Intelligence Soldiers need tools to collaborate with their counterparts. A number of tools are standard.

### ZIRCON/MIRC Relay Chat

**A-47.** ZIRCON is an internet relay chat, a form of real time internet chat or synchronous conferencing. ZIRCON is mainly designed for group (many-to-many) communication in discussion forums called channels, but also allows one-to-one communication and data transfers via private message. The Web chat utility is used primarily for analyst-to-analyst collaboration, giving analysts the opportunity for immediate feedback from fellow analysts. ZIRCON can also be used to communicate immediate tasking requirements, intelligence requirements, and other products or requests. ZIRCON can increase the capabilities of SIGINT Soldiers without increasing the unit's footprint. MIRC is a shareware internet relay chat for Windows. While a fully functional chat utility, integrated scripting language makes it extensible and versatile. MIRC is used in the same manner as ZIRCON.

### Electronic Mail

**A-48.** E-mail is used in much the same way as the chat functions—for collaboration, to pass on information, and as a sometimes faster means of passing on information requirements and requests for information.

### Web sites

**A-49.** Web sites are used to post the most up to date graphics, information requirements, priority intelligence requirements, commanders critical information requirements, online reference materials,

and links to these materials. Many units use Web sites to host this information on SIPRNET.

## Video Teleconferencing

**A-50.** Video teleconferencing uses audio and video telecommunications to bring people at different sites together for a meeting. This can be as simple as a conversation between two people in private offices (point-to-point) or may be more complex and involve several sites (multipoint) with more than one person in large rooms at different sites. Besides the audio and visual transmissions, video conferencing can be used to share documents, computer-displayed information, and whiteboards.

# Appendix B

# Emerging Capabilities

## INTRODUCTION

**B-1.** Capabilities and equipment are ever-changing as science and knowledge advance. Emerging capabilities that impact intelligence operations include—

- Biometrics.
- Distributed Common Ground System-Army (DCGS-A).
- Human terrain analysis teams.
- Document and media exploitation (DOMEX).
- Red teaming.
- Company intelligence support team (COIST).
- Counter-radio controlled improvised explosive device systems.

## BIOMETRICS

**B-2.** A *biometric* is a measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual (JP 2-0). *Biometrics-enabled intelligence* is the intelligence information associated with and or derived from biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist/insurgent network and related pattern analysis; facilitates high-value individual targeting, reveals movement patterns, and confirms claimed identity (DODD 8521.01E).

**B-3.** Typical automated biometric systems include five integrated components:

- **Collection device.** This is hardware found on a biometric device that converts biometric input into a digital signal and conveys this information to the processing device.
- **Algorithms.** This is a sequence of instructions that tells a biometric system how to solve a particular problem. An algorithm has 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.** This is used to store collected information for later matching.
- **Decision process.** This is an automated or human-assisted process or analysis that produces a decision by matching components against specific search criteria.
- **Dissemination process.** This is a process that transmits the data collected to whomever and wherever it needs to be in a timely manner.

**B-4.** The implementation of these five components leads to personal identification and the identification of an individual with certainty. Implementation occurs in three stages:

- The sensor collects biometric data of or on a feature. The sensor may collect fingerprints, an iris scan, a photographic image of a face, or a deoxyribonucleic acid (DNA) sample, for example.
- The system stores the biometric feature in a mathematical template in a database.
- The processing device runs a search of the template against a matching algorithm that compares the new template to templates previously stored in the database.

**B-5.** Commanders need 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 to positively identify known threats. Biometric systems collect biometric data and combine that information with contextual data to produce an electronic dossier on the individual.





FOR OFFICIAL USE ONLY

**B-6.** Personal identification includes positively identifying friendly, adversary, and nonadversary forces. Intelligence-related functions that biometrics can support or enhance include—

- Intelligence analysis.
- Screening of foreign national and local employee hires.
- Counterintelligence (CI) and protection.
- Interrogation and detention operations.
- High-value target (HVT) confirmation, including high-value individuals and individuals killed in action.
- Base access and local security.
- Population control or census through screening, enrolling, and badging operations.

**B-7.** The ability to positively identify and place an individual within a relevant context adds a level of certainty that significantly enhances the overall effectiveness of the mission. Personal identification, enabled by biometric technology, can help identify and locate specific individuals in support of targeting. This capability is necessary for protection and security missions as well as in situations when an operational capability is required to achieve an advantage in all operational themes and across the spectrum of conflict.

**B-8.** Affixing an individual's identification using the individual's unique physical features and linking this identity to the individual's past activities and previously used identities provides accurate information on the person. Identity items of interest include friendly forces' accesses, permissions, clearance status, medical information, and unique biometrically-based identifiers. Biometric identity information on adversary or unknown persons is also of interest. Ensuring access to all available information about an individual is critical to functions such as screening persons for access to vessels or positions of trust and prosecuting terrorists and other criminals. Biometric capabilities continue to develop, and current operations continue to evolve. Integrating the operational, intelligence, and communication aspects of biometrics systems into a cohesive concept of employment is necessary to maximize the advantages of biometrics-enabled intelligence (BEI).

## DISTRIBUTED COMMON GROUND SYSTEM-ARMY

**B-9.** DCGS-A provides a netcentric, intelligence, surveillance and reconnaissance (ISR), weather, geospatial engineering, and space operations capability to organizations of all types, at all echelons—from battalion to joint task force level. DCGS-A will be the ISR component of the modular and future force Mission Command System and will become the Army's primary system for ISR tasking, posting, and processing, and/or conducting analysis concerning the threat, terrain and weather, and civil considerations at all echelons.



**B-10.** DCGS-A provides the capabilities commanders need to access information from all data sources and to synchronize sensors. DCGS-A provides continuous access to and synthesis of data and information from joint and interagency capabilities, multinational partners, and nontraditional sources. These capabilities allow forces to maintain an updated and accurate awareness of the operational environment. DCGS-A contributes to visualization and situational awareness, thereby enhancing tactical maneuver, maximizing combat power, and enhancing the ability to conduct full spectrum operations in an unpredictable and changing operational environment.

**B-11.** DCGS-A facilitates the rapid conduct of operations and synchronization of all warfighting functions. DCGS-A gives commanders the ability to operate within the threat's decision cycle and shape the environment for successful operations. The core functions of DCGS-A are—

- Receipt and processing of selected ISR sensor data.
- Control of selected Army sensor systems.
- Facilitation of ISR synchronization.



FOR OFFICIAL USE ONLY

- Facilitation of ISR integration.
- Fusion of sensor information.
- Direction and distribution of relevant threat information and intelligence.
- Facilitation of the distribution of friendly and environmental (weather and terrain) information.

**B-12.** For additional information on DCGS-A, see appendix E.

## HUMAN TERRAIN ANALYSIS TEAMS

**B-13.** 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 other cultures within the area of operations (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. Intelligence professionals 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.

**B-14.** Effective intelligence professionals understand and appreciate their own culture—individual, military, and national—in relation to the various cultures of others in the AO. Just as culture shapes how other groups view themselves and the world around them, culture also 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 local population, commanders expose and question their assumptions about the situation. They seek to understand how enemies, partners, and the population view a situation.

## DOCUMENT AND MEDIA EXPLOITATION

**B-15.** Modern military operations take place in volatile, complex, and ever-changing operational environments. It is essential for tactical military leaders to have access to accurate and timely information when conducting operations. Tactical, operational, and strategic leaders are enabled with accurate extraction, exploitation, and analysis of captured materials. Captured materials are divided into captured enemy documents (CEDs) and captured enemy materiel (CEM).

**B-16.** DOMEX is the systematic extraction of information from all media in response to the commander's collection requirements. When conducted properly, DOMEX operations—

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



**B-17.** DOMEX is an increasingly specialized, full-time mission requiring advanced automation and communication support, analytical support, and expert linguists. DOMEX and translation operations were previously considered purely human intelligence (HUMINT) processing activities, directly associated with language capabilities and extensive background knowledge in area studies. However, current doctrinal thought acknowledges that HUMINT is no longer the sole asset responsible for and capable of performing DOMEX operations. Personnel involved in DOMEX do not require HUMINT training to screen or translate a document; rather, it is best to use HUMINT assets sparingly to conduct


FOR OFFICIAL USE ONLY

the HUMINT mission. DOMEX is an Army-wide responsibility. While HUMINT assets may be used, when available, to perform the DOMEX mission, HUMINT organizations are consumers of DOMEX information rather than major providers.

**B-18.** 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 Soldiers. This not only enables rapid exploitation and evacuation of captured materials but also hastens the feedback commanders receive from the higher echelon analysis.

**B-19.** 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.

**B-20.** DOMEX personnel are usually not available below battalion level except in military intelligence organizations. The intelligence staffs must prepare their subordinate units for DOMEX operations. There are two techniques for doing this. When intelligence and target-language personnel are available, they can be task-organized as intelligence support teams and placed with companies or platoons. Alternatively, the intelligence section can train company or platoon personnel in specific handling, screening, and inventorying techniques.

**B-21.** Where tactical assets are insufficient, operational and strategic assets can be requested to support a unit's organic assets. This can be done through personnel augmentation or virtual or long-distance support. DOMEX support elements provide this support worldwide.

**B-22.** The skills, knowledge, and equipment for specialized processing are available at intelligence community organizations through the communications architecture. Units can request support from a number of organizations such as—

- National Media Exploitation Center.
- National Ground Intelligence Center.
- Joint document exploitation centers.

**B-23.** These organizations use specialized techniques and procedures to extract additional information from captured audio and video materials. Application of specialized processing techniques and procedures may require the classification of the processed information and restrict its dissemination.

## RED TEAMING

**B-24.** Red teams provide commanders with an enhanced capability to explore alternatives during planning, preparation, execution, and assessment. Whenever possible, commanders employ red teams to examine plans from a threat's perspective. A red team is a special staff section whose members primarily plan future operations. Red team members anticipate the cultural perceptions of partners, enemies, adversaries, and others. They conduct independent critical reviews and analyses.

**B-25.** 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 help commanders account for the threat and environment in plans, concepts, organizations, and capabilities. These perspectives also address the standpoint of multinational partners, enemies, adversaries, and others in the AO.

## COMPANY INTELLIGENCE SUPPORT TEAMS

**B-26.** As company elements deploy to engage and defeat adversary forces in complex environments, the speed with which intelligence analysis and products from higher echelons reach them can make the difference between success and failure. Higher echelons, with limited personnel and a broad scope of analytic requirements, may not fully meet the intelligence requirements of a company commander. This is due to the overwhelming amount of data thrust into the intelligence framework from an ever-increasing amount of collection assets.

**B-27.** Battalion intelligence staffs may not have adequate resources to process and produce intelligence specifically geared for a company. This capability gap is not unique to current operations. In order to solve this problem, subordinate units build COISTs to satisfy their intelligence requirements. A COIST assists the commander with intelligence support for any operational environment.

**B-28.** A COIST is an organization formed at the company level to perform intelligence tasks as directed by the commander. Commanders usually establish COISTs while conducting stability operations. However, company commanders may form COISTs to provide intelligence support during offensive, defensive, or civil support operations as well.

## COUNTER-RADIO CONTROLLED IMPROVISED EXPLOSIVE DEVICE SYSTEMS

**B-29.** Systems to defeat improvised explosive devices (IEDs) have become increasingly essential in modern warfare. Such systems are constantly being designed to meet the challenging changes in enemy techniques. See appendix K.

**B-30.** See TC 2-22.601 for additional information on the Army's Counter-Radio Controlled Improvised Explosive Device Electronic Warfare (CREW) systems.

# Appendix C

# Intelligence and Signal Synergy: Cyberspace Operations

## INTRODUCTION

**C-1.** The Department of Defense (DOD) designation of cyberspace as a new fifth domain—along with air, land, maritime, and space—demonstrates now and into the future the importance of cyberspace as key terrain for a technologically-dependent nation. For two decades antagonists have battled to control cyberspace. Criminal activities and espionage are ever-escalating as shown by the rise in the number of cyber intrusions, cyber attacks, and stolen data. These activities are an increasing danger to the nation and to the military. Intelligence assessments predict that the numerous cyber threats and their capabilities will continue to grow in scale and mature technologically, thus adding to this danger. The cyber domain is rife with dynamic change, vulnerabilities, challenges, and opportunities for friendly and threat forces. With the ever-growing convergence of communications and networking technologies, the Army faces challenging paradigm shifts in understanding, developing, growing, and sustaining cyber capabilities, and in conducting cyber operations (such as defense, exploitation, and attack in and through cyberspace). To gain and maintain an advantage, while placing adversaries at a disadvantage, requires that the Army bring focus and resources to this new arena.

**C-2.** This appendix introduces the emerging field of cyberspace operations. It addresses the key concepts of cyberspace operations and touches on the role that military intelligence (MI) and signal Soldiers play in executing cyberspace operations. It also examines the way ahead as described in the *2010 Quadrennial Defense Review*, the *Quadrennial Roles and Missions (QRM) Review Report 2009*, and the *Army's concept of operations, Cyberspace Operations Concept Capability Plan,* published 22 February 2010.

## KEY CONCEPTS OF CYBERSPACE OPERATIONS

**C-3.** *Cyberspace* is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (CJCSCM-0363-08). In today's operational environments commanders consider cyberspace as well as the traditional domains of air, land, sea, and space.

**C-4.** *Cyberspace operations* are the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (CJCS Memo 19 Aug 2009).

**C-5.** Cyberspace operations encompass actions to gain advantage, protect that advantage, and place adversaries at a disadvantage in the cyber/electromagnetic contest. Commanders seek to retain freedom of action in cyberspace and in the electromagnetic spectrum, while denying adversaries freedom of action.This enables Soldiers to perform other operational activities in and through cyberspace, as well as in the other four domains. Cyberspace operations are not an end in themselves. Rather, they are an integral part of full spectrum operations—which include related activities prevalent in peacetime military engagement—that focus on winning the cyber/electromagnetic contest. Cyberspace operations are continuous. Engagements occur daily, most often without the commitment of additional forces.

**C-6.** Cyberspace operations are integrated with the commander's other capabilities to gain advantage, protect that advantage, and place adversaries at a disadvantage in operations. Converging technologies increasingly affect operations and influence capability development.

**C-7.** Cyberspace operations are performed at the national, joint, and Army levels by both the generating force and the operational Army. The Army provides forces to U.S. Cyber Command (USCYBERCOM), all combatant commanders, and joint task forces through the request-for-forces process. These forces are capable of performing offensive and defensive cyberspace operations for joint operations and can support tactical operations through global reachback or support teams.

## Intelligence and Signal Synergy

**C-8.** Although Cyberspace operations combines aspects of both signals and signals intelligence (SIGINT), it belongs to neither branch. Cyberspace operations takes as a starting point the legacy concepts of Network Operations and Network War and brings them forward as CyberNetOps and CyberWar. These functions are linked and mutually supporting, while maintaining separate identities (see figure C-1). Cyberspace warfare is the component of Cyberspace operations that extends cyber power beyond the defensive boundaries of the Global Information Grid to detect, deter, deny, and defeat adversaries. CyberWar targets computer and telecommunications networks, embedded processors, and controllers in threat equipment, systems, and infrastructure. CyberWar uses cyber exploitation, cyber attack, and dynamic cyber defense in a mutually supporting and supported relationship with CyberNetOps and cyber support.

**C-9.** CyberNetOps includes cyber defense actions, which combine information assurance, computer network defense (including response actions), and critical infrastructure protection with enabling capabilities (such as electronic protection and critical infrastructure support) to prevent, detect, and ultimately respond to an adversary's ability to deny or manipulate information and/or infrastructure. Cyber defense is integrated with the dynamic defensive aspects of cyberspace warfare to provide defense in depth.

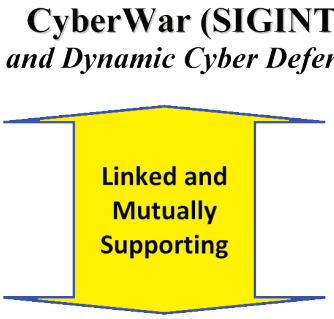



**Figure C-1. Relationship of CyberWar and CyberNetOps**

**C-11.** As figure C-1 shows, CyberWar attacks and exploits adversary networks and performs dynamic cyber defense through a variety of means. CyberNetOps operates friendly networks and defends them from attack. Dynamic cyber defense actions combine policy, intelligence, sensors, and highly automated processes to identify and analyze malicious activity, simultaneously tip and

cue, and execute preapproved response actions to defeat attacks before they can do harm. Dynamic cyber defense uses the Army defensive principles of security, defense in depth, and maximum use of offensive action to engage cyber threats. These actions include surveillance and reconnaissance to provide early warnings of pending enemy actions. Dynamic cyber defense is integrated with the defensive aspects of CyberNetOps to provide defense in depth.

**C-12.** Some of the ways that intelligence supports cyberspace operations are—

- Counterintelligence.
- Analysis and tracking of cyber threats.
- Tipping and cueing to CyberNetOps.
- Incident handling.
- Digital forensics.
- Developmental and operational testing.
- Opposition force-based red teams.
- Penetration testing.

## The Way Ahead

**C-13.** The 2010 Quadrennial Defense Review states that today's security environment demands improved capabilities to counter cyberspace threats. In the twenty-first century, modern armed forces cannot conduct effective, high-tempo operations without resilient, reliable information and communication networks and assured access to cyberspace. The Department of Defense (DOD) must actively defend its networks.

**C-14.** Network defense requires the DOD to operate effectively in cyberspace. Assessments of conflict scenarios involving state adversaries pointed to the need for improved capabilities to counter threats in cyberspace. There is no exaggerating Soldiers' dependence on DOD's information networks for mission command of forces, the intelligence and logistics on which they depend, and the weapons technologies being developed and fielded.

**C-15.** DOD's information networks are targets for adversaries who seek to blunt U.S. military operations. Indeed, these networks are infiltrated daily by many sources, ranging from individuals and small groups to agents of some of the largest countries in the world. For example, criminals may try to access DOD's healthcare systems to obtain personal information to perpetrate identity theft. Terrorists may seek to disrupt military networks and systems to cause chaos and economic damage. Foreign intelligence or military services may attempt to alter data in DOD databases to hinder the military's ability to operate effectively. DOD must actively defend its networks.



**C-16.** Cyber defense is no small task. DOD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DOD computers and telecommunications tools in use in 88 countries, employing thousands of warfighting and support applications. The number of potential vulnerabilities, therefore, is staggering. Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favor the offense. The attacker's advantage grows as hacker tools become cheaper and easier to employ while the skills of adversaries become increasingly sophisticated.

**C-17.** Soldiers must be constantly vigilant and prepared to react nearly instantaneously if they are to effectively limit the damage inflicted by the most sophisticated types of attacks. In this environment, the need to develop strategies, policies, authorities, and capabilities for DOD to manage and defend its information networks is manifest.

**C-18.** DOD is taking several steps to strengthen capabilities in cyberspace:

- Develop a more comprehensive approach to DOD operations in cyberspace.
- Develop greater cyber expertise and cyber awareness.
- Centralize command of cyber operations.
- Enhance partnerships with other agencies and governments.

### Develop a More Comprehensive Approach to DOD Cyberspace Operations

**C-19.** Developing a department wide comprehensive approach helps build an environment in which cyber security and the ability to operate effectively in cyberspace are viewed as DOD priorities. Strategies and policies to improve cyber defense in depth, resiliency of networks, and surety of data and communication allow DOD to continue to have confidence in its cyberspace operations. A central component of this approach is cultural and organizational. The DOD is adapting and improving its operational planning, networks, organizational structures, and relationships with interagency, industry, and international partners. New concepts—such as dynamic network defense operations—can enhance effectiveness by enabling more rapid actions and more comprehensive actions to protect the DOD's networks.

### Develop Greater Cyberspace Expertise and Awareness

**C-20.** DOD is redoubling its efforts to imbue its personnel with a greater understanding and appreciation for the threats and vulnerabilities in cyberspace and to give Soldiers the skills to counter those threats and reduce the vulnerabilities at the user and system administrator levels. DOD can no longer afford to have users think of its information technologies and networks as simply the benign infrastructure that facilitates their work. Users and managers must be held accountable for ensuring network security and for implementing best practices. DOD is growing its cadre of cyber experts to protect and defend its information networks. DOD is also investing in and developing the latest technologies to enable its forces to operate in cyberspace under a wide range of conditions, including in contested and degraded environments.

### Centralize Command of Cyberspace Operations

**C-21.** In an effort to organize and standardize cyber practices and operations more effectively, DOD has established USCYBERCOM—a subunified command under U.S. Strategic Command—to lead, integrate and better coordinate the day-to-day defense, protection, and operation of DOD networks. USCYBERCOM will direct the operation and defense of DOD's information networks. It will prepare to and when directed execute full spectrum cyberspace military operations. USCYBERCOM will also play a leading role in helping to integrate cyber operations into operational and contingency planning. In addition, the DOD is training cyber experts equipped with the latest technologies to protect and defend its information networks. Essential to the success of this new approach will be the improved capabilities and growth of the Service components that are established to support USCYBERCOM.

### Enhance Partnerships with Other Agencies and Governments

**C-22.** Freedom of operation in cyberspace is important, and DOD must have the capabilities to defend its own networks. However, the interdependence of cyberspace means DOD networks are heavily dependent on commercial infrastructure. Just as it does in performing many other missions, DOD needs to collaborate with other U.S. government departments and agencies and international partners to support their efforts and ensure the ability to operate in cyberspace. This mutual assistance includes information sharing, support of law enforcement, defense support to civil authorities, and homeland defense. In particular, DOD is strengthening its cooperation with the Department of Homeland Security, which leads the national effort to protect federal information systems.

# Appendix D

# Intelligence Support to the Military Decisionmaking Process

## INTRODUCTION

**D-1.** The *military decisionmaking process (MDMP)* combines the conceptual and detailed components of planning. Commanders use the MDMP to build plans and orders for extended operations as well as to develop orders for short-term operations within the framework of a long-range plan. This appendix reviews MDMP as it relates to the intelligence Soldier. Figure D-1 illustrates MDMP.

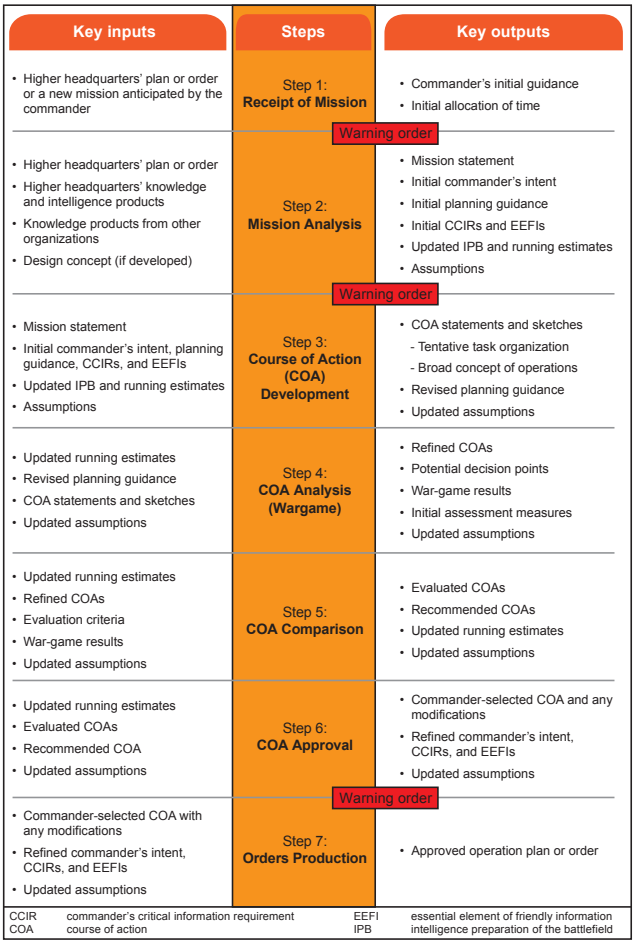



Figure D-1. MDMP Chart





FOR OFFICIAL USE ONLY

## MISSION ANALYSIS

**D-2.** MDMP begins with an analysis of the mission assigned by the higher headquarters. Most intelligence section actions during mission analysis facilitate the commander's situational understanding.

**D-3.** Thorough mission analysis is crucial to planning. The mission analysis process and its products help commanders refine situational understanding and determine the restated mission. Accurate situational understanding enables commanders to better visualize the operation. There are several distinct 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 categories of relevant information—threat, terrain and weather, and civil considerations.

**D-4.** Additionally, the process includes an analysis of the higher headquarters' plan or order to determine critical facts and assumptions; specified, implied, and essential tasks; and constraints that affect initial intelligence, surveillance, and reconnaissance (ISR) activities. Intelligence section actions during mission analysis include developing an ISR plan, the refining of the commander's situational understanding, and the refining of staff running estimates based on that same understanding.

**D-5.** To avoid misunderstanding, and to ensure there is a clear and common understanding of what is factual and what is assumption, all-source analysts must tell the commander and staff what they know and why they know it; what they think and why they think it; what they do not know and what they are doing about it. This promotes critical thinking. It also generates the staff discussion required to formulate sound courses of action (COAs).



## ANALYZE THE HIGHER HEADQUARTERS' ORDER

**D-6.** Mission analysis begins with an analysis of the higher headquarters' order. The intelligence staff focuses on how the higher headquarters' commander and intelligence staff view the threat. This knowledge helps shape the intelligence preparation of the battlefield (IPB) effort. The higher headquarters' order also contains information on that headquarters' ISR operations and available ISR assets. This information contributes to ISR synchronization.

## PERFORM INITIAL INTELLIGENCE PREPARATION OF THE BATTLEFIELD

**D-7.** The intelligence officer leads the staff through IPB. Other staff sections assist the intelligence section in developing the IPB products required for planning. IPB starts immediately upon receipt of the mission, is refined throughout planning, and continues during preparation and execution. (See FM 2-01.3 for the IPB steps.) IPB is based on continuous assessment of operations. The following describes the primary results of IPB supporting mission analysis.

## EVALUATE MILITARY ASPECTS OF THE TERRAIN

**D-8.** Utilizing the topographic team, analysts conduct a detailed terrain analysis of the area of operations (AO). They focus on natural and manmade features that may affect operations. The analyst briefs the commander and staff on the effects the terrain may have on both friendly and threat forces in terms of the military aspects of terrain—observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealmen. The analyst also briefs what effect the weather will have on terrain. The product resulting from terrain analysis is the modified combined

obstacles overlay. (See FM 2-01.3 for a detailed explanation of terrain analysis and the other standard products developed as a result of the analysis.)

## EVALUATE WEATHER CONDITIONS AND EFFECTS

**D-9.** If assigned to the intelligence section, the U.S. Air Force weather team provides weather forecasting and analysis under the direction of the intelligence officer. The intelligence section briefs the commander and staff on the weather forecast. The intelligence section concentrates on how the weather will affect warfighting functions in general, as well as how it will affect personnel and equipment specifically. (See FM 2-01.3 for a detailed explanation of weather analysis.)

## EVALUATE CIVIL CONSIDERATIONS

**D-10.** ASCOPE is an acronym for area, structures, capabilities, organizations, people, and events. These categories are used to analyze and describe civil considerations that may affect operations. The analyst includes the effects urban centers may have on friendly and threat forces in civil considerations. There is no standard product resulting from this analysis. The intelligence officer generally develops products that describe the situation and facilitate the commander's situational understanding. This is especially critical when conducting stability and civil support operations. (See FM 2-01.3 and FM 3-06 for detailed discussions of analyzing civil considerations.)

## DEVELOP THREAT CAPABILITIES

**D-11.** To accurately depict how a threat commander might deploy and maneuver forces on the battlefield, an analyst must understand how the threat is organized and equipped, what the threat's capabilities are, and how the threat has employed forces in the past. An understanding of threat characteristics and detailed organizational charts assist in this analysis. Maintaining accurate data on threat characteristics is essential when conducting combat assessment. Threat characteristics for conventional forces are generally available within the intelligence community. The analyst generally has to develop threat characteristics for emerging threats such as terrorists and insurgents. This is accomplished by using information gained from national combatant commands and theater intelligence organizations, as well as from the publications of threat groups.

## DEVELOP THREAT MODELS

**D-12.** Depending on the mission, there are three types of threat models generally required for planning. The first two are used in conventional operations. They show how the threat might execute offensive and defensive operations against friendly forces. The third is used to show how irregular forces might execute operations in complex terrain, such as an urban area. Each product includes a graphic depiction of the accompanying threat COA statement. These models communicate the threat's disposition, objectives, goals and end state, and main and shaping efforts. They also communicate how the threat is expected to maneuver. Additionally, these products explain the threat's intent for fires, ISR, information engagement, command and control warfare, and logistics. Finally, they explain the threat's failure options and a recommendation on how to defeat the threat. Depending on the mission, the analyst may develop more than one threat model to describe possible threat COAs.

## IDENTIFY HIGH-VALUE TARGET LIST

**D-13.** Every threat situation template and threat COA statement is accompanied by a high-value target list that describes and prioritizes, in terms of their relative worth, those assets that the threat

commander requires to achieve stated objectives. The analyst develops this list in coordination with the rest of the staff. The list can include specific individuals, and organizations.

## DEVELOP AN EVENT TEMPLATE AND MATRIX

**D-14.** Developed as the basis for the decision support templates and the ISR overlay, the event template and matrix helps identify the commander's decision points and determine ISR strategies. The event template and matrix ensure a consistent and well-reasoned portrayal of threat capabilities throughout planning. They are critical in tying ISR and the concept of operations together. The event template and matrix are not briefed during mission analysis, but they must be ready for COA development.

## DETERMINE SPECIFIED, IMPLIED, AND ESSENTIAL TASKS

**D-15.** The analyst analyzes the higher headquarters order, identifying the specified ISR tasks assigned to the unit and developing implied tasks that must be performed to accomplish the stated specified tasks. The analyst provides a list of specified and implied tasks to the operations section and assists in determining essential tasks for inclusion in the unit's restated mission.

## REVIEW AVAILABLE ASSETS



**D-16.** 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 review, the analyst determines whether the unit has the assets needed to accomplish all collection tasks. The intelligence section identifies any shortages and makes recommendations for additional resources.

## DETERMINE CONSTRAINTS

**D-17.** A higher commander normally places constraints on subordinate commanders. A typical constraint for ISR operations would be 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. They might also be stated in the annexes to the order.

## IDENTIFY CRITICAL FACTS AND ASSUMPTIONS

**D-18.** Along with the rest of the staff members, the intelligence section is responsible for gathering two categories of information concerning assigned tasks—facts and assumptions.

**D-19.** In determining initial intelligence requirements, the intelligence staff examines the facts and assumptions the staff has developed. Information required to confirm or refute an assumption about the threat or area of interest may produce intelligence requirements. Similarly, it may be necessary to monitor the situation for any changes to facts about the threat or area of interest that might affect the plan or order. The intelligence staff considers these requirements as it plans ISR operations.

**D-20.** Throughout planning, commanders and staffs periodically review all facts and assumptions. New facts may alter requirements and require a review of the mission analysis. Assumptions may have become facts or may have become invalid. Whenever facts or assumptions change the commander and staff assess the impact that these changes have on the plan and make the necessary adjustments, including changing the commanders critical information requirements (CCIRs), if necessary.

## DETERMINE INITIAL INFORMATION REQUIREMENTS

**D-21.** Determining the initial information requirements is the first step in developing an ISR plan. Priority intelligence requirements (PIRs) are not developed by the staff until after the COA analysis. They are not approved by the commander until COA approval. In the mission analysis briefing, after stating what they know, what they think they know, and what they do not know, the analyst recommends what information the intelligence section should be collecting and analyzing to support continued planning and COA development. Identifying information requirements helps the commander filter the available information by defining what is important to mission accomplishment. It also helps to focus the efforts of the rest of the staff and subordinate commands.

## DETERMINE THE INITIAL INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE, PLAN

**D-22.** By the time the staff completes the mission analysis and finalizes the initial IPB products, the intelligence officer and staff should have developed the initial collection requirements. These collection requirements are the basis of the initial ISR plan, requests for collection, and requests for information (RFIs) to higher and lateral units conducting ISR operations. By this time, intelligence gaps are identified and ISR planners have developed an initial strategy on how to answer the gaps. The operations officer and the remainder of the staff should have a thorough understanding of the unit's missions, tasks, and purposes.

**D-23.** The operations section is the staff proponent of the ISR plan. The ISR plan 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. This is necessary to answer the CCIRs, PIRs, and friendly force information requirements and other intelligence requirements. The intelligence section must have its input and products available to publish as part of the warning order that the S-3 issues at the conclusion of mission analysis.



## UPDATE THE OPERATIONAL TIMELINE

**D-24.** The commander and staff integrate the operational timeline established by the higher headquarters with the projected threat operational timelines developed during IPB. They do this to determine windows of opportunity for exploiting threat vulnerabilities or times when the friendly unit may be at risk from threat activity.

## DELIVER A MISSION ANALYSIS BRIEFING

**D-25.** 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 IPB products developed for threat, terrain and weather, and civil considerations. The analyst may also brief the initial ISR plan if the unit is in a position to begin collection operations. The analyst should also brief the identified intelligence gaps in support of further planning. The mission analysis briefing is a decision briefing. It results in an approved restated mission, commander's intent, and commander's planning guidance. The analyst presents only the information needed by the commander to develop situational understanding and formulate planning guidance.

## DERIVE INPUT FROM THE INITIAL COMMANDER'S GUIDANCE

**D-26.** After the intelligence section briefs the commander and offers recommendations, the commander considers those recommendations before formulating the commander's intent.

## ISSUE A WARNING ORDER

**D-27.** Immediately after the commander gives planning guidance, the operations officer issues a warning order. At a minimum, the intelligence section input into the warning order includes—

- Threat situation paragraph.
- PIRs, priority of collection.
- Priority of support.
- ISR tasks.

**D-28.** Additionally, if initial IPB products have not been made available to higher headquarters and subordinate commands, the products should be issued with the warning order.

## COURSE OF ACTION DEVELOPMENT

**D-29.** COA development involves updating the running estimates and preparing COA options for the commander's consideration. (See Appendix A for more information on running estimates.) 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 any opportunities the environment and threat situation offer. The staff attempts to mitigate the most significant risks. The intelligence analyst works closely with the operations section and the staff to analyze relative combat power and develop friendly COAs. All friendly COAs are based on the threat situation template, the threat event template, and the matrix produced by the analyst 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 tools in preparation for COA analysis.

## COURSE OF ACTION ANALYSIS (WARGAMING)

**D-30.** Analysis of COAs is a disciplined process that includes sequential rules and steps. It relies heavily on an analyst's understanding of doctrine, tactical judgment, and experience. The intelligence analyst has two areas of responsibility in the war game—to role-play the threat commander and act as the ISR officer.

**D-31.** Playing the threat commander, the intelligence analyst uses the threat situation template and the event template and matrix to—

- Develop critical threat decision points in relation to friendly COAs.
- Project threat reactions to friendly actions.
- Project threat losses.

**D-32.** As the ISR officer, the intelligence analyst—

- Identifies new information requirements.
- Assists the staff in developing PIRs.
- Refines the situation and event templates.
- Develops the ISR overlay and synchronization tools.
- Assists in the development of the high-payoff targets and the decision support template.

**D-33.** At the conclusion of the war game, pending COA approval by the commander, every intelligence product that must be published with the warning order is complete.

## COURSE OF ACTION APPROVAL

**D-34.** Following an analysis of the COAs, the staff identifies its preferred COA and makes a recommendation to the commander. This occurs during a decision briefing presented by the operations officer. During this briefing, the analyst briefs any changes to the current threat situation and any terrain and weather, and civil considerations that have changed since the commander was last briefed.

## ORDERS PRODUCTION

**D-35.** The staff, led by the operations officer, 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 conduct their operations. However, this is not the first time subordinate commanders and their intelligence staffs have seen this data. Parallel and collaborative planning involves intelligence analysts at all echelons. They have reviewed each other's intelligence products as they were developed. At this point, they clarify changes and submit requests for additional information and product support. The staff reviews the order before it is issued.

# Appendix E

# Distributed Common Ground System-Army Concepts

## INTRODUCTION

**E-1.** The Army's operational focus has shifted from the division to the brigade combat team (BCT) during the past decade. The change caused numerous intelligence complications. The primary problem was the inability to pass critical information and intelligence to the level required. The solution to the problem is the Distributed Common Ground System-Army (DCGS-A) program. By design, DCGS-A breaks stovepiped data barriers, alters collaboration methods, and enhances BCT commanders' ability to act on actionable intelligence.

**E-2.** This appendix provides background information about DCGS-A for the intelligence Soldier. Topics covered include the challenges that DCGS-A addresses, its applications and configurations, and the ways the analyst uses the system.



## WHAT IS DCGS-A

**E-3.** DCGS-A supports three primary roles:

- As the intelligence, surveillance, and reconnaissance (ISR) component of the Mission command Information System, DCGS-A provides the ability to discover and use all relevant threat, noncombatant, and terrain and weather data.
- As an analyst tool, DCGS-A provides intelligence domain experts the capability to collaborate, synchronize, and integrate organic and nonorganic direct and general support collection elements with operations. DCGS-A provides access to information in a multitude of databases and allows analysts to process, analyze, and exploit technically complicated data and information on behalf of commanders.
- As a ground station, DCGS-A provides organizational elements with the ability to control select sensor platforms and payloads and subsequently process the collected data.

**E-4.** DCGS-A employs a network-based architecture using Web-based services to provide intelligence analysts with access to large volumes of information as well as the visualization tools needed to manage that information and perform in-depth analysis. This architecture gives the analyst access to information and products from numerous databases and programs of record. It displays data from individual programs of record including the All-Source Analysis System (ASAS), common ground station (CGS), and others. (Information on these systems can be found in appendix J.)

**E-5.** DCGS-A synchronizes intelligence support with operations. BCT intelligence officers have access to information and intelligence that previously was available only at division and higher.

**E-6.** Because of its access to near real-time intelligence collection, DCGS-A allows commanders to better support Army tactical tasks. DCGS-A provides—

- Increased situational awareness, reducing operational risk to commanders and allowing for more effective and precise employment of lethal and nonlethal fires.
- A more complete operational view—from tactical to strategic level—while synchronizing operations with ISR employment. This enables dynamic opportunities for targeting, situational development, and predictive analysis.

## DCGS-A CAPABILITIES

**E-7.** Intelligence is the knowledge that BCT intelligence officers use to support commanders in synchronizing operations, massing combat power, and protecting the force. There is no such thing as perfect intelligence. However—when properly focused, planned, and executed—intelligence operations are invaluable. DCGS-A greatly assists synchronization of collection assets to accomplish a unit's mission. To use intelligence effectively, intelligence officers understand—

- The capabilities and limitations of the intelligence warfighting function.
- The intelligence architecture, which includes mission command; processing, collaborative and distributed analysis; ISR activities; and intelligence networks and communications.
- The focusing of ISR activities.
- How commanders and their staffs synchronize ISR with other operations.

**E-8.** The capabilities of DCGS-A synchronize collection assets from division to BCT with increased access to critical information. The accessibility to previously restricted information allows intelligence personnel at the lowest level to leverage the vast intelligence enterprise. Intelligence personnel can better assess the current operational environment and acquire actionable intelligence in a timely manner. Previously, collection, processing, and analysis occurred in a stovepiped process that denied critical information to most intelligence personnel, particularly at brigade level and below. Consequently, commanders' decisions, often made without access to critical information, carried unnecessary risk.

**E-9.** When properly employed, DCGS-A facilitates and leverages a cross-domain enterprise approach to achieving superior situational understanding. It enables rapid and adaptive planning, preparation, execution, and assessment against a highly adaptive threat. DCGS-A provides real-time, constant, precision-networked, wide-area, high-capacity, and multisensor intelligence analysis capabilities to supported (or maneuver) commanders. DCGS-A merges the capabilities of existing intelligence and terrain and weather systems into a single system. DCGS-A is capable of ingesting, cataloging, and sharing massive amounts of information with both current and planned mission command systems and weapons platforms.

**E-10.** The capabilities that DCGS-A provides to the intelligence community enable the development of a multifunctional analyst. These are analysts who can incorporate other specialized disciplines, such as geospatial intelligence (GEOINT), signals intelligence (SIGINT), human intelligence (HUMINT), or counterintelligence, into their own intelligence discipline. DCGS-A provides common tools that give all analysts greater understanding of each discipline and enable cross-training. Common tools enhance analysts' ability to share data and information and to collaborate in answering priority intelligence requirements. These tools support the DCGS-A concept of teaming to solve problem sets rather than depending on the current discipline-centered approach. Multifunctional analysts employ their skills at the lowest echelon. Often, lower echelons have limited resources and personnel. The analytical capabilities of these analysts are a resource the S-2 or G-2 officer can exploit for situational awareness, mission accomplishment, and risk reduction.

## THE INTELLIGENCE WARFIGHTING FUNCTION

**E-11.** DCGS-A's primary function is to provide timely, relevant, accurate, and predictive intelligence support to commanders who are planning, preparing, and executing decisive actions within the area of operations (AO). Other functions implied or associated with intelligence, are—

- Integrated ISR planning focused through the S-2 or G-2 and operations S-3 or G-3 but thoroughly planned by the entire staff.
- Changes and adjustments to reconnaissance and surveillance collection.
- Analysis, production, and dissemination (including presentation) of intelligence and combat information—the heart of the intelligence warfighting function.

- Integrated and employed electronic warfare, which is an integrated part of fires and targeting.
- Support for protection and providing the critical ability to protect the force through counterintelligence by supporting counterreconnaissance, analyzing the threat's multidiscipline ISR operations, and recommending countermeasures to those threat operations.

## THE ARMY UNIVERSAL TASK LIST AND THE DCGS-A APPLICATION

**E-12.** DCGS-A enables commanders to meet the intelligence requirements of Army tactical tasks through system configuration and application.

**E-13.** Army tactical task 2.0 the intelligence warfighting function, is the primary warfighting function and mission area that DCGS-A supports. The intelligence warfighting function activity generates knowledge of and products portraying the threat and the environmental features commanders require.



**E-14.** DCGS-A supports the following Army tactical tasks and mission areas:
- Support to force generation and all subtasks.
- Support to situational understanding and all subtasks.
- Perform intelligence, surveillance, and reconnaissance and all subtasks.
- Support to targeting and information superiority and all subtasks.

**E-15.** In support of the four tasks of the intelligence warfighting function, military intelligence personnel also—
- Manage tactical information.
- Integrate intelligence products.
- Collect relevant information.
- Process relevant information to create a common operational picture (COP).
- Display a COP tailored to user needs.
- Store relevant information.
- Disseminate COP and execution information to higher, lower, adjacent, supported, and supporting organizations.
- Communicate with non-English speaking forces and agencies.
- Assess tactical situation and operations.
- Monitor the situation or progress of operations.
- Evaluate situations or operations.
- Provide combat assessments.
- Perform battle damage assessments.
- Perform the military decisionmaking process.
- Integrate space capabilities.

## DCGS-A AND THE INTELLIGENCE PROCESS

**E-16.** DCGS-A assists the S-2 or G-2 in guiding and narrowing the focus of ISR activities to—
- Obtain and clearly articulate PIRs.
- Drive the intelligence preparation of the battlefield (IPB) process throughout the military decisionmaking process (MDMP).

**E-17.** The S-2 or G-2 coordinates with both the executive officer and the operations officer to plan and synchronize ISR activities. The S-2 or G-2 ensures that IPB drives the rest of the planning process. ISR activities are planned and controlled as part of the larger integrated staff effort through the mission command system. While the S-2 or G-2 is the IPB and ISR integrator, the S-3 or G-3 synchronizes

ISR assets with the operation. The intelligence officer ensures all personnel with functional expertise participate in and provide input into the wargame process including the IPB process and ISR planning and execution.

**E-18.** DCGS-A facilitates the war-game process by providing common analyst tools to the analysts and Mission command System operators. Sharing data and products across various domains allows S-2s and G-2s to quickly redirect collection efforts in direct support of current operations, in addition to answering critical PIRs for their commanders.

**E-19.** S-2s and G-2s ensure ISR activities are continuous by synchronizing collection requirements with the executive officers and S-3s or G-3s. Intelligence personnel—through the intelligence architecture—continuously perform intelligence tasks to meet commanders' requirements before deploying and during operations.

**E-20.** DCGS-A eliminates stovepiping of assets and allows analysts to access information regardless of their location. DCGS-A facilitates ISR activities by providing a single point of access to multiple sensor feeds, as well as the tools required for analysis.



**E-21.** DCGS-A provides the foundation to implement a cross-domain infrastructure between the intelligence and mission command networks. DCGS-A uses a non-proprietary hardware approach. The data transfer capability from DCGS-A workstations to alternate sources and operating systems allows for optimal mission success in diverse operational environments and strategies, such as time-sensitive targeting and protection of the force.

## DCGS-A AND THE ANALYST

**E-22.** Analysts no longer have to learn multiple operating systems to run a query, depict icons on a map, or share data. DCGS-A provides common analyst tools that can query through a single entry, visualize graphically the military and nonmilitary data in one central location, and collaborate in defining finished products through Internet communications.

### Single-Entry Query

**E-23.** Act requires precise knowledge of self, opponent, and environment. Distributed and simultaneous operations demand the right knowledge at the right time. Operations also require comprehension of more aspects and terrain in the operational environment, rather than only the military aspects of designated objectives. Difficult environments and adaptive enemy operations dictate highly-detailed intelligence and may hinder the anticipation of future events. Large amounts of intelligence and other types of information demand rapid and accurate processing, swift and accurate analysis, and robust distribution capacity.

**E-24.** In order to see the diverse operational environments, analysts must be able to quickly sift through massive amounts of information. To do this, analysts now have one point of entry to query the vast amount of knowledge that has been collected and is available. The ability to enter a single string of queries and produce returns from all types of repositories enables analysts to concentrate on pattern-of-life analysis, economic analysis, cultural analysis, and more.

### Visualization

**E-25.** Cultural, religious, ethnic, political, and economic realities complicate understanding of the future geopolitical environment. The resulting mix of global, strategic, operational, and tactical issues

transcends borders and involves opponents with worldwide connections. This presents a demanding combination of challenges and dilemmas for the United States. Security challenges vary and are unpredictable within the spectrum of conflict. The allegiances of many entities within the operational environment are difficult to determine. While some entities may clearly be neutral, others may interchange. They may be a threat in certain U.S. efforts while supportive of others. The requirement to transform what the collectors see into understanding is the most important element facing intelligence personnel in their mission to support commanders, and it is the most difficult task.

### Collaboration

**E-26.** Intelligence personnel understand the operational environment from an intelligence perspective and must support commanders in performing both collaborative planning and the execution of plans. DCGS-A allows commanders to draw upon other resources, such as terrain and environmental effects, by leveraging geospatial technology and information databases, home-station operations centers, and live and virtual staffs. This capability to collaborate when assessing courses of action, visualizing potential outcomes, making decisions, and developing and disseminating plans enhances the speed of planning, preparation and execution. It enhances the ability to simultaneously control operations that are widely separated in nature, time, and space.



## DCGS-A CONFIGURATIONS

**E-27.** DCGS-A is configured to enable commanders to better understand the operational environment in near real time. Figure E-1 illustrates the overall configuration of version 3 of DCGS-A. There are three DCGS configurations:

- Fixed.
- Mobile.
- Embedded.

### Fixed

**E-28.** The fixed configuration leverages the power and stability of sanctuary for the most complex processing and analytic tasks. Additionally, it provides the greatest historical data repository. Aligned geographically, U. S. Army Intelligence and Security Command (INSCOM) brigades host these fixed sites. The fixed DCGS-A configurations facilitate intelligence reach by providing the extensive intelligence analysis and strategic planning from stationary locations. Regionally focused, fixed DCGS-A performs a dedicated overwatch function for deployed units. The fixed configuration connects DCGS-A with other variations of the DCGS system of systems and with national sources through provided communications.

### Mobile

**E-29.** The mobile configuration of DCGS-A provides a tactical, deployable capability to deliver responsive forward support to commanders from battalion-level through operational headquarters levels. This configuration is allocated between two development increments; DCGS-A Mobile Basic and DCGS-A Mobile Extended. Analytical tools, sensor inject, data storage, and integration with other mission command systems are the highlights of the mobile configuration. The configuration is the access point or intelligence service provider for ISR data and information in combatant commands. Implementing the complex capabilities into the mobile configuration requires two different releases. The DCGS-A Mobile Basic and Mobile Extended provide commanders with access to ISR components from maneuver battalion to joint task forces. DCGS-A Mobile Basic and Mobile Extended are a significant shift from hardware-based systems to systems with software-based capabilities.

### Mobile Basic

**E-30.** The Mobile Basic configuration is organic to and directly supports modular brigades and division intelligence personnel. The BCT is the principal user. DCGS-A Mobile Basic capabilities are modular and scalable to meet supported unit deployment and tactical mobility criteria. They can operate independently, but are more capable when connected to operational and strategic level sensors, sources, and people. DCGS-A Mobile Basic provides a wide range of ISR capabilities, including direct access to and control of select sensor platforms. When not deployed, mobile assets can operate as part of the ISR network and be fully integrated into DCGS-A Mobile Extended and home-station operations. Upon full fielding, DCGS-A Mobile Basic capabilities displace and replace current tactical intelligence task, process, exploit, and disseminate systems within the division headquarters intelligence staffs and BCTs.

**E-31.** The DCGS-A Mobile Basic configuration contains a mixture of multisecurity-level, multifunction workstations and portable multifunction workstations. The mixture is based on the number of personnel supported and the unit's mission.



**E-32.** The DCGS-A Mobile Basic provides select services to intelligence and nonintelligence platforms. At echelons above BCT, Mobile Basic is augmented with national, combatant command, and Army sensor data link and data processor plugs. The Mobile Basic configuration is capable of receiving these plugs when augmentation is directed.

### Mobile Extended

**E-33.** The DCGS-A Mobile Extended configuration incorporates current capabilities found at division and higher, allowing access to select services down to battalion. Dissolving the stovepipe funnels enables the analyst to perform processing, exploitation, and dissemination at one location. The extended configuration possesses a robust hardware-processing and data-storage capacity. Forward-deployed organizations collaborate with—and reach to—mobile extended configurations across the network, substantially expanding commanders' situational awareness without increasing the forward footprint.

## Embedded

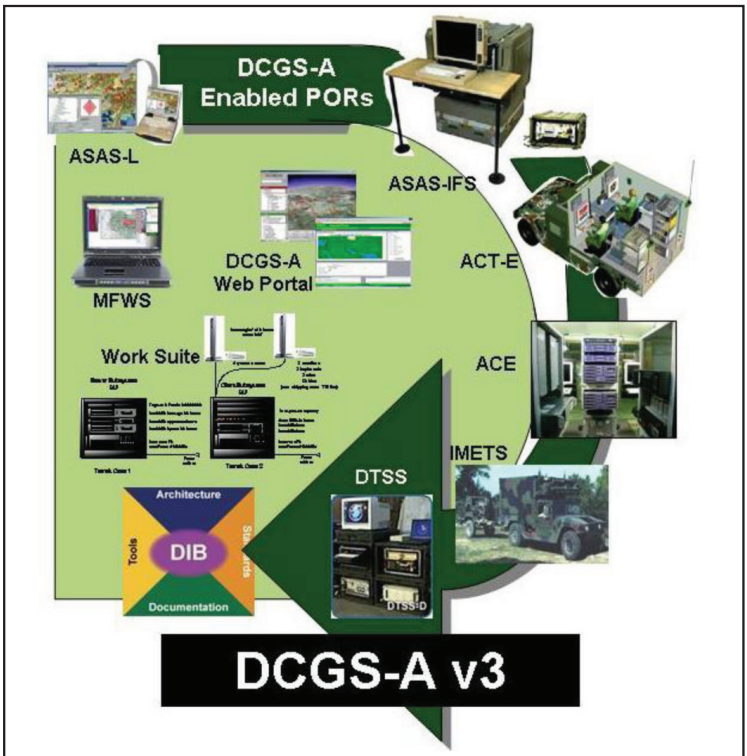
**E-34.** The embedded DCGS-A software on mission command systems connects the intelligence enterprise with the mission command network. Embedded software gives battalion and company intelligence efforts unprecedented access to data previously unavailable. Historically, surveillance and reconnaissance collected from nonmilitary intelligence sources were available to the intelligence enterprise. The embedded software provides shared access to both the mission command and the intelligence enterprise. This provides a more complete picture of the operational environment to commanders. Embedded software capabilities provide commonality and standardization, improving interoperability, reducing training time, and increasing sustainability. Embedded software resides on local workstations and is available through the network. The network secures the embedded software by controlling user access and permissions.

# DISTRIBUTED COMMON GROUND SYSTEM—ARMY VERSION 3

**E-35. Nomenclature:** AN/TSC-177 and AN/TSQ-256(V)1.

**E-36. Project name:** Distributed Common Ground System- Army Version 3 (DCGS-A v3).

**Figure E-1. DCGS-A V3**




***SYSTEM SUMMARY***

***FEATURES***

- All-source intelligence fusion, analysis and dissemination system.
- Integrates collection management functionality.
- ISR systems technical control system.
- Army Mission Command System interoperable.
- Processes/disseminates collateral reports
- Alerts criteria or event.
- Detection of inbound message traffic.
- Integrated map functionality.
- Access to national, joint, and theater intelligence databases.
- Configurable to operate as a stand-alone system.

***TABULATED DATA:***

**BAL**

- Computer type: Laptop.
- Models. Alienware, Dell M90.

**Work Suite**

- Computer-type Servers.
- Models:. 2x Dell 2850, 1 x Dell 1850.

**E-37. Function:** DCGS-A v3 is a tactical lightweight scalable system that provides a DCGS-A Mobile capability to the Army forces down to battalion level. DCGS-A v3 provides automated intelligence processing, analysis, collection or ISR management, and dissemination to G-2s, S-2s and analytic work centers.

**E-38. Description:** DCGS-A v3 extends capabilities provided by the DCGS-A v2 (formerly known as JIOC-I) to the tactical-level Army. DCGS-A v3 merges the functions of the ASAS-Light AN/TYQ-93A(V)3 and ASAS-IFS AN/TYQ-93B(V)2 providing a core intelligence set of capabilities to tactical Army forces as part of the DCGS worldwide, distributed, network-centered, system-of-systems architecture, enabling collaborative intelligence operations and products.

**E-39.** To accelerate the capabilities that DCGS-A offers, many programs of record are being DCGS-A enabled via hardware and software upgrades and technical insertions. The end result is to create an integrated ISR capability that provides global reachback to theater, joint, multinational, and national data sources, repositories, and analytic resources, thus giving Army forces fully integrated and timely intelligence in the (AO) . This is accomplished by interfacing with other DCGS nodes such as the DCGS-A (Fixed) within the military intelligence brigade at theater through the DCGS-A backbone. DCGS-A v3 provides broad access to sensors or platforms such as JSTARS, electro-optical and infrared, SIGINT, Global Hawk, and Predator unmanned aerial systems (UASs), HUMINT, and other collection platforms such as Rivet Joint and E-3. These systems are discussed in appendix I.

**E-40.** DCGS-A v3 provides interaction with other intelligence and electronic warfare systems, mission command, and select joint systems as a coherent system of systems. Previous to version 3, individual mission command systems interacted with DCGS-A. DCGS-A is tactically scalable and provides the workstation with a set of analyst tools that include additional collaborative capabilities. It provides Soldiers a seamless capability to share preprocessed intelligence information and graphic IPB products from the battalion command post to brigade DCGS-A v3 Server.

**E-41. Organization:** Stand-alone work suites are fielded to ISR analytic sections and centers requiring a robust automated intelligence processing and storage capability. These include but are not limited to the Army headquarters (operational command post), corps/division tactical command post, special forces battalion, MI company (Ranger Regiment), space brigade, and others.

**E-42. System description:** The DCGS-A v3 consists of a combination of work suites with client terminals and stand-alone workstations, called basic analyst laptops, running the Multifunctional Workstation software application. Work suites are embedded into existing programs of record (for example, DCGS-A enabled ASAS analysis and control element [ACE]) but may be fielded to work centers requiring robust analytic processing and storage up and beyond that provided by the basic analyst laptop or DCGS-A enabled ASAS-L and ASAS-IFS, such as the Army operational CP or corps/division tactical command post. The work suites' data repository and server applications are the focal point for accessing the DCGS-A Web Portal and accessing client and server applications.

**E-43. Hardware—**

- BAL: Alienware Laptop with 3.8GHz CPU, 2GB RAM and 17" display.
- Work Suite: Server subsystem (transit case 1) contains two Dell 2850 servers; one is the message database server and the other is the spatial database server, a Dell 1850 applications server, and an uninterruptible power source. Client subsystem (transit case 2) contains two Dell 1850 client computers, a Cisco 3550-24 switch, an UPS, and two 24-inch liquid crystal display(LCD) monitors with keyboard and mouse.

**E-44.** Software (See figure E-2 for DCGS-A V3 software builds.)—

- Multifunctional workstation software:
  - MS XP Pro SP2.
  - Acrobat Reader 7.0.
  - Easy CD Creator.
  - MS Office XP ED 2003 SP1.
  - Web-based DCGS-A applications.
  - Query tools (QueryTree & Pathfinder).
  - ArcIMS.
  - NAI tool.
  - FusionNet client.
  - Jabber client.
  - Analyst Notebook 6.0.
  - ArcGIS 9.1 Suite.
  - Symantec anti virus.
  - Integrated Pathfinder.
  - NAI 2.1 search alerts.
  - IWEDA client.
  - AXIS Pro.
  - ELT 3500.
- Work suite:
  - MS XP Pro.
  - Acrobat Reader 7.0.
  - Analyst Notebook 6.0.
  - Analyst Notebook Oracle Plugin.
  - Analyst Notebook Scraper.
  - ArcGIS Arc View 9.1 (concurrent).
  - ArcGIS Arc Editor 9.1 (concurrent).
  - ArcGlobe (3D analyst) (concurrent).
  - ArcGIS Spatial Analyst (concurrent).
  - ArcGIS Tracking Analyst (concurrent).
  - ArcReader.
  - TerraExplorer Viewer.
  - Aspera Web 1.2.0.10.
  - Sonic CD/DVD RecordNowPlus.
  - GeoRover.
  - Image Access Solutions Client (JPEG 2000).
  - JRE 1.5.03 (JAVA).
  - FusionNet client.
  - Jabber client.
  - Netscape 7.0.
  - Urban Tactical Planner.
  - WinZip 9.0.
  - WS FTP 9.01.
  - Oracle 10.2g Admin client.
  - NdCore client 3.1.
  - Starlight client 2.10.
  - Pathfinder extension.
  - Symantec antivirus.
  - NT Toolbox.
  - Active State PERL.
  - IWS client 2.5.1.3.
  - Windgrinder/Sunder.
  - Military Analyst.
  - Military Overlay Editor (MOLE).
  - MIRC Chat.
  - MS Office ED 2003 SP1.

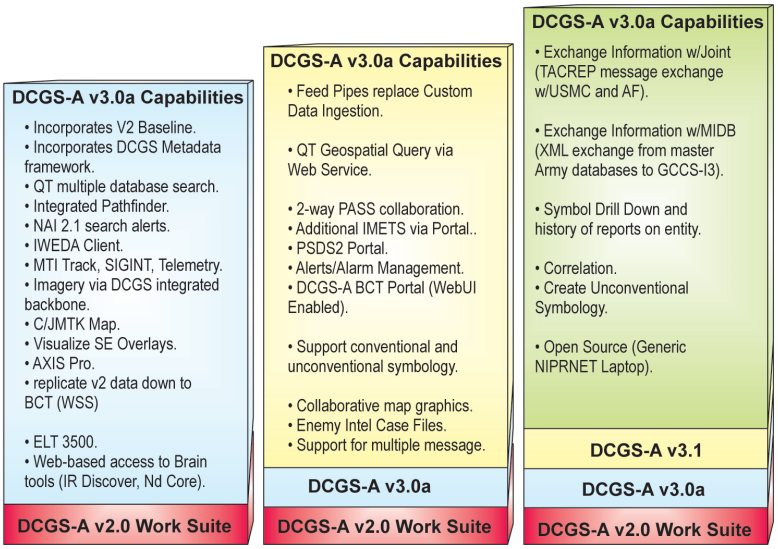



Figure E-2. DCGS-A V3 software builds

**E-45. Deployment and operations:**

- **Security:** The DCGS-A v3 and DCGS-A enabled programs of record operate at the security level appropriate to the organization it is supporting (for example, SECRET, TS/SCI, releasable to multinational partners, other).
- **Interoperabilty:**
  - DCGS-A v3 is interoperable with the DCGS-A (fixed) brain and DCGS-A v2, and DCGS-A enabled programs of record. DCGS-A v3 is backward compatible with ASAS Block II ACE, CGS, IMETS, DTSS, TBMCS, GCCS-I3, the Marine Corps IAS, and other joint systems, allowing two-way exchange of graphic and imagery exchanges, select message exchanges, as well as database population, to support operations across the spectrum of conflict.
  - The DCGS-A v3 software interfaces with Army Battlefield Command System through BC PASS Server, FBCB2, GCCS-A, AFATDS, and the MCS/CPoF. It uses standard IP e-mail communications for inbound and outbound messages through the CMP to send and receive USMTF and VMF messages.

**E-46. Intelligence dissemination:** The dissemination of intelligence between distant sites relies on the Army Common User System or unit-provided communications (for example, Trojan Spirit). With built-in e-mail, FTP, and Web servers, DCGS-A v3 can send and receive a variety of tactical intelligence reports and products such as external database coordination messages. In addition, DCGS-A v3 also enables two-way communication of critical battlefield messages such as tactical reports. DCGS-A v3 allows the intelligence officer or analyst to browse other systems' Web pages and send and receive NITF imagery, graphic intelligence summaries (INTSUMs), storyboards, and overlays.

# DISTRIBUTED COMMON GROUND SYSTEM- ARMY VERSION 4

**E-47. Nomenclature:**

- Multifunctional Workstation (MFWS) AN/TSQ-256 V1/V2/V3.
- Data Analysis Central (mounted/deployable basic variants) AN/TYQ-152 V1/V2.
- Multi-Intelligence Processing System (MIPS) mounted and deployable variants AN/TYQ-XXX V1/V2.


***SYSTEM SUMMARY***

***FEATURES:***

- All-source intelligence fusion, analysis and dissemination system.
- Integrates collection management functionality.
- ISR systems technical control system.
- Army Battlefield Command System interoperable.
- Processes/disseminates collateral reports.
- Alerts criteria/event detection of inbound message traffic.
- Integrated map functionality.
- Access to national, joint, and theater intelligence databases.
- Configurable to operate as a stand-alone system.

**Figure E-3. DCGS-A V4**

**E-48. Function:** DCGS-A v4 is the first fielded version of DCGS-A (Mobile). (See figure E-3.) It provides a tactical lightweight scalable system-of-systems hosting DCGS-A capability to the tactical Army down to battalion level. DCGS-A v4 expands upon its predecessor, the DCGS-A v3. It provides automated intelligence processing, analysis, collection/ISR management, geospatial services, weather services, Army space operations, and dissemination. It provides them to intelligence officers along with their analytic work centers, S-2Xs, operational management team, topographic, weather, and

space teams.

**E-49. Description:** DCGS-A v4 is a combination of various mounted and deployable variants, each tailored to meet the specific demands of the tactical Army. DCGS-A v4 supports conventional and asymmetric warfare in terms of mobility, processing, storage, and dissemination for intelligence, geospatial, weather, and space operations.

**E-50.** DCGS-A v4 consolidates or replaces Army ISR ground processing stations, including legacy systems, with a single, integrated system. It interfaces with a variety of sensors via combination of direct and indirect sensor datalinks and tactical communication systems. DCGS-A v4 receives overhead sensor data either directly or indirectly via the network. These links and networks provide the capability for the DCGS-A v4 operators to control and direct the sensors.

**E-51.** DCGS-A v4 serves as the primary mission command information system for tactical Army intelligence. It provides single-source and all-source processing, analysis, production, and dissemination. It is essential to the support of mission command. The core functions of DCGS-A v4 are receipt and processing of select ISR sensor data; control of select Army sensor systems; intelligence synchronization; ISR planning, reconnaissance, and surveillance integration; fusion of all-source information; single-source processing and analysis; and direction and distribution of relevant red (threat), gray (nonaligned), and blue (friendly) and environmental (weather, terrain, and space) information.



**E-52.** The DCGS-A v4 software interoperates with other DCGS-A systems and with intelligence and electronic warfare/ISR systems including legacy and DCGS-A enabled programs of record. It supports mission command and information operations through rapid dissemination of actionable intelligence from all available sources. The DCGS-A v4 provides a seamless intelligence mission command architecture consisting of workstations, servers, mass storage devices, cross-domain security solutions and communications modules that are internally connected via a local area network (LAN).

**E-53.** DCGS-A v4 consolidates and/or replaces the programs of record shown in table E-1.

**Table E-1. Programs of record**

| | |
|---|---|
| A18176 | ACT-E AN/TYQ-103(V)3 |
| A35329 | ASAS-LIGHT AN/TYQ-93A(V)4 |
| A35397 | ASAS-IFS AN/TYQ-93b(v)2 |
| A52995 | ACE-DIV/ACR AN/TYQ-89 |
| A53199 | ACE-CORPS AN/TYQ-92 |
| C18244 | CI&I OPS AN/PYQ-7 |
| C60421 | ASAS-CCS AN/TYQ-128(v)3 |
| C60625 | ASAS-CCS AN/TYQ-128(V)2 |
| D02704 | PROPHET-CONTROL AN/MLQ-40(V)1 |
| D10281 | DTSS-LIGHT AN/TQY-67A |
| D11248 | DTSS-T AN/TYQ-48 |
| D11498 | DTSS-D AN/TYQ-71 |
| J41800 | IMETS-LIGHT AN/GMQ-36 |
| M55690 | IMETS-HEAVY AN/GMQ-40A/B/C |
| T09221 | DTES AN/TSQ-219(V)3 |
| T37036 | CGS AN/TSQ-179(v)2 |
| TBD | Guardrail Ground Baseline (GGB) |
| NA | E-TRACKWOLF (analytic processor and workstations) |

**E-54. System description:** DCGS-A v4 consists of commercial-off-the-shelf, common hardware software equipment and selected items of government-furnished equipment integrated within standard Army shelters or transit cases tailored to meet the needs of supported commanders. The components of this system are described below.

## MFWS

**E-55.** The MFWS comes in three variants: Portable MFWS AN/TSQ-256(V)1, a laptop; the multi-level MFWS AN/TSQ-256(V)2, a desktop capable of processing two or more security levels; and the fixed MFWS AN/TSQ-256(V)3. The MFWS is the intelligence staff officer, space staff officer, and analyst interface to the DCGS-A (Mobile) family of systems and access to the DCGS integrated backbone. The MFWS can be found within the maneuver BCT, division, corps, and Army headquarters. The MFWS works in tandem with one or more DCGS-A (Mobile) or DCGS-A (Fixed) systems. It facilitates reach by providing the tactical force with a intelligence processing, analysis, and planning capability from a mobile location. Tactically focused, the MFWS takes advantage of the heavy lifting processing and storage capability provided by the DCGS-A (Fixed) within the theater reach back MI brigade and DCGS-A v4 Basic systems at Army, corps, division, BCT, and armored cavalry regiment headquarters. Nondeployed units can aid the intelligence effort in performing tactical regional overwatch functions or aiding operationally engaged units.



## Basic

**E-56.** The Mounted Basic AN/TYQ-152(V)1 and Deployable Basic AN/TYQ-152(V)2 each consist of three extremely capable and powerful modules: analytic workstation module, admin/server module, and communications module. It provides relevant information about threats and the operational environment, information that is used to execute battles, engagements, and other missions across the spectrum of conflict. The AN/TYQ-152 has an internal communication support assembly package to provide a communications front-end for pushing and pulling sensor data, databases, messages, reports, and products. It provides intelligence gateway access across communication networks including NSANET, JWICS, SIPRNET, NIPRNET, and multinational. It also connects to multiple sensors, collectors, and knowledge centers through the DCGS integrated backbone via standard Army area communications. The AN/TYQ-152 rapidly processes and fuses large volumes of combat and sensor information to produce enemy situation reports, target folders and nominations, threat warnings, and battlespace reports as part of the joint common operational picture.

## MIPS

**E-57.** The Mounted MIPS AN/TYQ-XXX(V)1 and Deployable MIPS AN/TYQ-XXX(V)2—like the DCGS-A v4 Basic (AN/TYQ-152)—also consists of three capable modules, although providing less storage and direct sensor feeds than its mounted and deployable basic counterparts. It too provides relevant information about threats and the operational environment, information that is used to plan and execute battles, engagements, and other missions across the full spectrum of operations. The AN/TYQ-XXX has an internal communication support assembly package to provide a communications frontend for pulling and pushing of databases, messages, report products, and select access to direct data feeds. It provides intelligence gateway access across communication networks including JWICS, SIPRNET, and multinational. It also connects to multiple sensors, collectors, and knowledge centers through the DCGS integrated backbone via standard Army area communications. The AN/TYQ-XXX rapidly processes and fuses large volumes of combat and sensor information to produce enemy situation, target folders and nominations, threat warnings, and battlespace reports as part of the JCOP.

**E-58. Deployment and operations:**

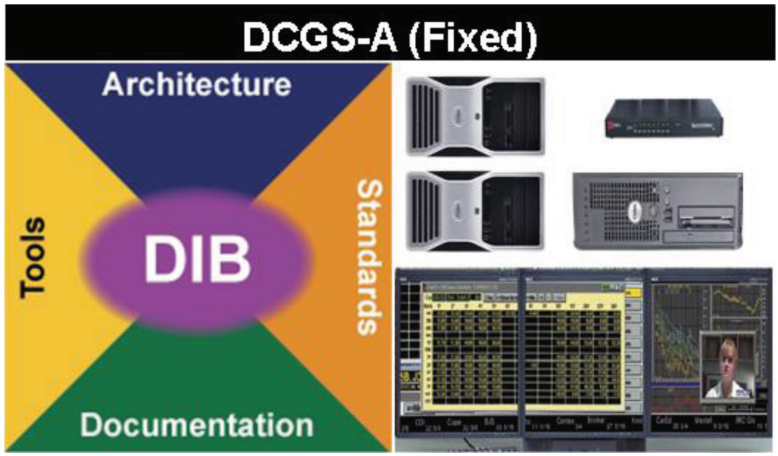
- **Security:** The DCGS-A v4 and DCGS-A enabled programs of record operate at the security level appropriate to the organization it is supporting (for example, SECRET, TS/SCI, releasable to multinational, other).
- **Interoperability:**
  - DCGS-A v4 is interoperable with the DCGS-A (Fixed) brain, DCGS-A v2/v3, and DCGS-A-enabled programs of record. DCGS-A v4 is backward compatible with ASAS Block II ACE, CGS, IMETS, DTSS, TBMCS, GCCS-I3, the Marine Corps IAS, other intelligence and joint systems allowing two-way exchange of graphic and imagery exchanges, select message exchanges, as well as database population, to support the full range of military operations.
  - The DCGS-A v4 software interfaces with ABCS through BC PASS Server, FBCB2, GCCS-A, AFATDS, and the MCS/command post of the future. It uses standard IP E-mail communications for inbound and outbound messages through the CMP to send and receive USMTF and VMF messages.



**E-59. Intelligence dissemination:** The dissemination of intelligence between distant sites relies on ACUS or unit-provided communications (for example, Trojan Spirit). With built-in e-mail, FTP, and Web servers, DCGS-A v4 can send and receive a variety of tactical intelligence reports and products, such as EDC messages. In addition, DCGS-A v4 also enables two-way communication of critical battlefield messages such as TACREP and TIDAT reports. DCGS-A v4 also allows the intelligence officer or analyst to browse other systems' Web pages, as well as send and receive NITF imagery, graphic INTSUMS, storyboards, and overlays.

# DISTRIBUTED COMMON GROUND SYSTEM-ARMY (FIXED)

**E-60. Nomenclature:** AN/FSQ-209(V)1.




***SYSTEM SUMMARY***

***FEATURES:***

- DCGS integrated backbone.
- Performs "heavy lifting" for DCGS-A (Mobile) systems.
- All-source intelligence fusion, analysis and dissemination system.
- Integrates collection management functionality.
- ISR systems technical control system.
- Processes/disseminates collateral reports.
- Alerts criteria/event detection of inbound message traffic.
- Access to National, joint, and theater intelligence databases.

***TABULATED DATA:***

- OL-695 Data Analysis-Programming Group: 1.
- ON-579 Interconnecting Group: 1.
- OJ-777 Communications System Control Group: 1.
- OL-696 Digital Computer System: 100 to 140.

**Figure E-4. DCGS-A (Fixed)**

**E-61. Function:** DCGS-A (Fixed) depicted in figure E-4, is the strategic variant of the DCGS-A family of systems. It facilities reach back operations by supporting the tactical force with an intelligence processing, analysis, and planning capability from a fixed location. The DCGS-A brain provides the heavy lifting in terms of processing and storage for DCGS-A (Mobile) systems. DCGS-A (Fixed) facilitates regional overwatch, reach back operations by supporting the tactical force with an intelligence processing, analysis, and planning capability from a fixed location.

**E-62.** The DCGS-A (Fixed) provides ISR tasking, collection, processing, exploitation, and dissemination supporting the theater commander's ability to execute mission command, synchronize fires, rapidly shift battle focus, provide indications and warning, achieve situational understanding, and protect the force.

**E-63. Description:** DCGS-A (Fixed) hosts DCGS-A software and is the core framework for a worldwide distributed, network-centric, system-of-systems architecture that performs collaborative

intelligence operations and production. It consolidates the functions of three programs of record into an integrated ISR capability and provides global reachback to national data sources and analysis resources, giving the Army fully integrated and timely intelligence in the operational environment; interfacing with other DCGS-A nodes through the DCGS integrated backbone. The DCGS integrated backbone provides a distribution of ISR data, processes, and systems. DCGS-A (Fixed) networks to other service DCGS family of systems, national sources (through network and direct feed), commercial sources, theater sources, intelligence community partners, JTF assets, and knowledge centers through the Global Information Grid (GIG).

**E-64. System development:** DCGS-A (Fixed) falls under the direction of the program manager for DCGS-A with INSCOM oversight.

**E-65. Organization:** DCGS-A (Fixed) is afforded one per theater army military intelligence brigade. DCGS-A (Fixed) consolidates or replaces the following programs of record within the theater army MI brigade:

- T13901—TES-Forward AN/TSQ-219(V)2.
- T13833—TES-Main.
- T37036—CGS AN/TSQ-179(V)2.



**E-66. System description:** DCGS-A (Fixed) consists of three main nodes of commercial off-the-shelf, and selected items of government-furnished equipment. The three nodes are—

- DCGS integrated backbone comprised of the OL-695 data analysis-programming group and the ON-579 interconnecting group. The DCGS integrated backbone encapsulates the server domain providing the network, cross-domain solutions, routers, hubs and switches between the servers, various workstations, and the DCGS-A Web portal.
- OJ-777 communications system control group.
- OL-696 digital computer system. These three nodes support the four DCGS-A (Fixed) domains:
  - Single-source domain.
  - Fusion domain.
  - Server domain.
  - Battle captain visualization domain.

**E-67. OL-695 Server Domain:**

- JWICS processing, application and storage servers for imagery (including the IPL and IESS), MASINT, HUMINT, M3, GIS servers (including the ARCIMS, ARCSDE, and the DTSS), DCGS-A brain, Web server, security servers, exchange server, domain servers, and the DCGS integrated backbone server.
- SIPRNET processing, application, and storage servers for video exploitation, IPL, MASINT, HUMINT, DOMEX, M3, GIS servers (including ARCIMS, ARCSDE, DTSS), weather server (IMETS), DCGS-A brain, Web server, security servers, exchange server, domain servers, and DCGS integrated backbone server.
- NSANET processing, application, and storage servers for HIGHCASTLE, OneRoof, MailOrder, imagery servers, GIS servers (including ARCIMS, ARCSDE, and DTSS), DCGS-A brain, Web server, security servers, exchange server, domain servers, and DCGS integrated backbone server.
- Multinational processing, application, and storage servers for imagery, GIS (including ARCIMS, ARCSDE, and DTSS), Web server, security servers, exchange server, domain server, and DCGS integrated backbone server.

**E-68. ON-579 Interconnecting Group:**

- 72 switches.
- 39 100-port routers and 30 16-port routers.
- 6 network routers.
- 60 secure phones.
- 5 one-way trusted links.
- 10 SunRay Trusted Workstation clients.
- 1 SunFire V480 Trusted Workstation server.
- 3 SunFire Trusted Releaser and 3 SunFire Trusted Webshield.
- 2 Cisco 4-port firewalls.
- 3 SunFire v240 ISSE Guards.
- 2 SunFire V480.
- 1 Dell 2850s.
- 4 Boarder Guards.
- 40 Cisco IP Phones for JWICS.
- 20 NSTS phones and an NSTS switch.
- 4 Polycom Sound Station XE (Star Phone for conferences).
- 2 video conferencing cameras, 2 VTC switch, Video Streaming, 2 VTC displays, and other miscellaneous items.

**E-69. OJ-777 Communications System Control Group:** The OJ-777 CSC group consists of 12-position workstations for use by the watch officer or battle captain and fusion analysts. Workstations associated with the control group are used by the watch officer or battle captain to visualize the battlefield, quality assurance/quality control QA/QC and final release of reports and products, monitoring the current situation, and overall orchestration of the intelligence effort. All-source analysts use the workstations for the following: data mining and exploiting single-source intelligence, indications and warning, fusing single-source reporting, link/node analysis, correlation, target development and target nomination, maintaining continuity of facilities, units, individuals, and organizations, ISR mission management, all-source assessments, studies, IPB, and reporting.

**E-70. OL-696 Digital Computer System:** Each DCGS-A (Fixed) site has from 100 to 140 OL-686, commonly known as the Fixed MFWS. The OL-696 forms the same basic computer configuration as that of the DCGS-A v4 MFWS (AN/TYQ-256(V)3. The fixed MFWS is an individual single-source analyst workstation supporting SIGINT, HUMINT, GEOINT, and MASINT. The workstations are used for the following: single-source report processing, data mining and exploitation, net/link/node analysis, correlation, target development and maintaining continuity of facilities, individuals, organizations and units, mission management, single-source assessments, studies, electronic IPB, support to electronic warfare operations, and reporting.

**E-71. Hardware:**

**E-72. *OL-695 Data Analysis-Programming Group:***

- JWICS servers: SGI 350S Server, five SunFire V440 servers, two SunFire V1280 servers, three SunFire V880 servers, SunFire V890 server, SunFire V240 server, 12 Dell 2850s, and a HP Blade server. Storage servers include a 250TB HITACH AMS1000, two 5TB SAN Imagery RAID, and six 1.5TB SunStorEdge 3510s.
- SIPRNET servers: Blackbox Diamond 108S server, Adtec EDJE-2000 server, three SunFire V440 servers, two SunFire V880 servers, 16 Dell 2850s, and two HP Blade servers. Storage servers include a 250TB HITACH AMS1000, two 730GB SunStorEdge 3510s.
- NSANET servers: A SunFire V440 server, two SunFire V480 servers, two SunFire V880 servers, two SunFire V210 servers, and 15 Dell 2850s. Storage servers include a 250TB HITACH AMS1000, a 730GB SunStorEdge 3510, a 365GB SunStorEdge 3510, a 1TB Dell PowerVault 220, and a Storageteck L20 for tape backup.

- Multinational servers: A SunFire V440 server, two Sunfire V880 servers, and 12 Dell 2850s.
- Storage servers include a 25TB NetApp FAS 980 and a 730GB SunStorEdge 3510.

**E-73. Operations:**

- **Security:** The DCGS-A (Fixed) operates at the security level appropriate at the SECRET, TS/SCI, and releasable to multinational levels.
- **Interoperability:** DCGS-A (Fixed) is designed to be interoperable with all other DCGS-A configurations as well as other service configurations of DCGS. This interoperability is capable primarily due to the integration of the DCGS integrated backbone whose configuration is managed by the jointly staffed DSCG Management Office (DMO). The DCGS integrated backbone consists of tools, standards, architecture, and documentation that enable the discovery, access, delivery, and collaborative use of ISR data and information and other enterprise services, across the ISR enterprise.

**E-74. Intelligence dissemination:** Much like DCGS-A V3 and V4, DCGS-A at the fixed-site facilitates the dissemination of intelligence between distant sites utilizing the relatively ubiquitous bandwidth available at most fixed locations. DCGS-A facilitates intelligence reach operations by providing the heavy lifting intelligence analysis and strategic planning in stationary locations. Regionally focused, DCGS-A (Fixed) will also perform a dedicated overwatch function for operationally engaged units. Fixed DCGS-A will connect with forward deployed mobile and embedded DCGS-A through the GIG and Warfighter Information Network—Tactical (WIN-T).

# Appendix F

# Military Intelligence Organizations

## INTRODUCTION

**F-1.** This appendix discusses the Army intelligence organizations and elements and their applications in theater, corps, division, and below. Effectively leveraging the Army intelligence organizations maximizes the intelligence support to combat operations.



## INTELLIGENCE AS AN ENTERPRISE

**F-2.** The Army implements the enterprise approach to its intelligence operations by operating a digital information and intelligence network that assists senior intelligence officers at all levels in producing intelligence and synchronizing intelligence support to commanders. The Army intelligence enterprise is linked to and can leverage support from the defense intelligence enterprise as well as from nonmilitary members of the intelligence community.

## THE ARMY INTELLIGENCE ENTERPRISE

**F-3.** The Army intelligence enterprise is the sum total of the networked and federated systems, and efforts of the military intelligence personnel (includeng collectors and analysts), sensors, organizations, information, and processes that allow the focus necessary to use the power of the entire intelligence community (See FM 2-0). The Army intelligence enterprise comprises the following elements:

- U.S. Army Intelligence and Security Command (INSCOM) staff.
- INSCOM functional commands and military intelligence brigades.
- Battlefield surveillance brigades (BFSB) and military intelligence battalions.
- Theater, corps, division, brigade combat team (BCT), and maneuver battalion intelligence staffs.
- Military intelligence companies assigned to BCTs.
- Surveillance troops assigned to BCTs.
- Company intelligence support teams (COISTs).

**F-4.** The Army intelligence enterprise is fully integrated into the defense intelligence enterprise. Figure F-1 illustrates the linkage between the defense and Army intelligence enterprises.

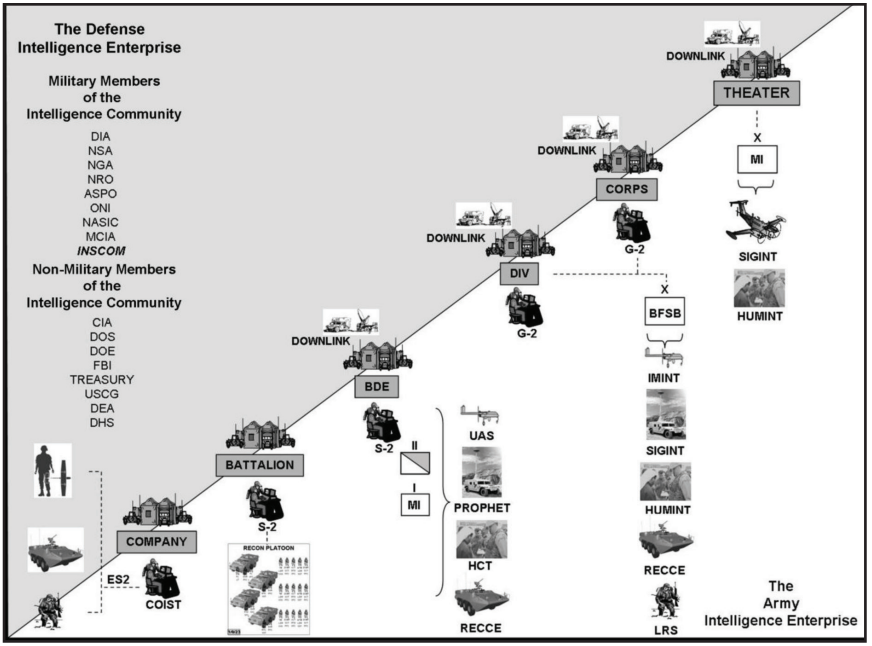



Figure F-1. The Army intelligence enterprise

## INTELLIGENCE AND SECURITY COMMAND

**F-5.** INSCOM is a member of Army and the defense intelligence enterprise. It has five primary components: Department of the Army Intelligence Information Services (DA-IIS), the National Ground Intelligence Center (NGIC), Foundry, the Army Operations Activity (AOA), and the 902nd military intelligence brigade. Each of these components provides unique intelligence services and support. Figure F-2 illustrates the INSCOM component of the Army intelligence enterprise.

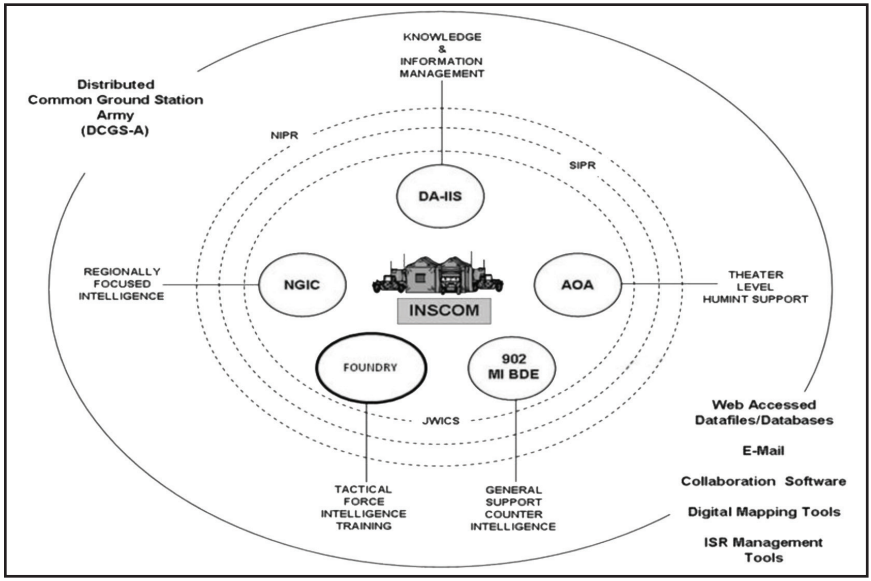



**Figure F-2. The INSCOM component of the Army intelligence enterprise**

## Theater Army Headquarters Intelligence Staff

**F-6.** The theater army headquarters has an intelligence staff that assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units. During deployment, the theater G-2 is augmented with an analysis and control element (ACE) from a supporting military intelligence brigade.

**F-7.** The theater G-2 is equipped with Web-based intelligence processors that allow data sharing with all echelons. These processors are connected to Joint Worldwide Intelligence Communications System (JWICS), SECRET Internet protocol router network (SIPRNET), and Nonsecure Internet protocol router network (NIPRNET). These processors are interoperable with all Army Battle Command Systems (ABCS) and can share data with all organizations in the Army and defense intelligence enterprises as well as those nonmilitary members of the intelligence community that use JWICS, SIPRNET, and NIPRNET.

**F-8.** Throughout Army force generation (ARFORGEN), the theater G-2 and its attached ACE provide regionally focused tactical intelligence overwatch. A supporting military intelligence brigade provides collection support. Figure F-3 illustrates theater G-2 integration into the Army intelligence enterprise.

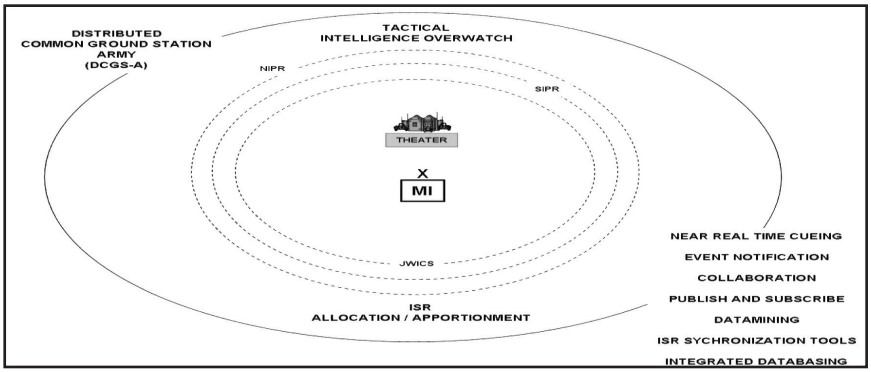



**Figure F-3. The theater component of the Army intelligence enterprise**

## Corps Headquarters Intelligence Section

**F-9.** The corps headquarters has a G-2 staff that assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units.

**F-10.** Like the theater army G-2, the corps G-2 is equipped with Web-based intelligence processors that allow data sharing with all echelons. These processors are connected to JWICS, SIPRNET, and NIPRNET. These processors are interoperable with all ABCS and can share data with all organizations in the Army and defense intelligence enterprises as well as those nonmilitary members of the intelligence community that use JWICS, SIPRNET, and NIPRNET. Figure F-4 illustrates corps G-2 integration into the Army intelligence enterprise.

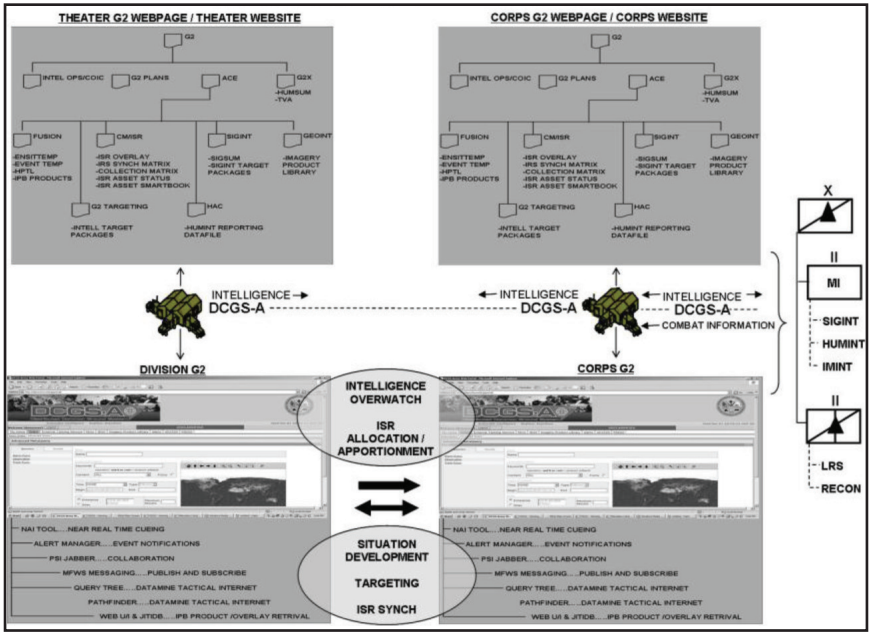



**Figure F-4. Corps to theater Army intelligence enterprise**

## Division Headquarters Intelligence Section

**F-11.** The division headquarters has a G-2 staff that assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units.

**F-12.** Like the theater army and corps G-2, the division G-2 is equipped with Web-based intelligence processors that allow data sharing with all echelons. These processors are connected to JWICS, SIPRNET, and NIPRNET. These processors are interoperable with all ABCS and can share data with all organizations in the Army and defense intelligence enterprises as well as those nonmilitary members of the intelligence community that use JWICS, SIPRNET, and NIPRNET. Figure F-5 illustrates division G-2 integration into the Army intelligence enterprise.

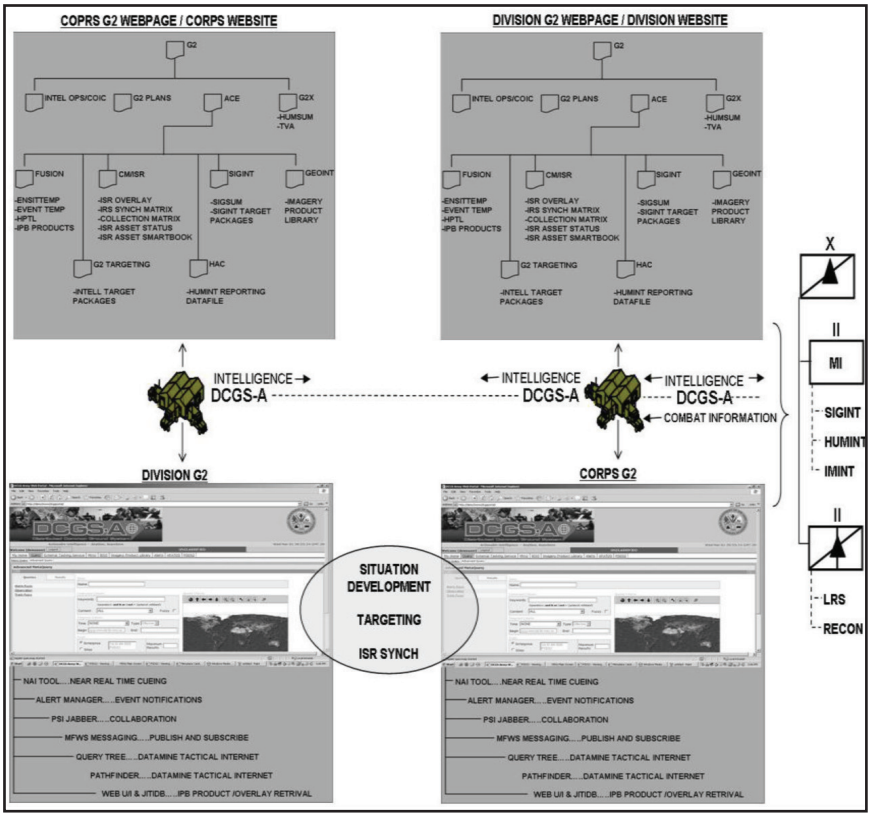



**Figure F-5. Division to corps Army intelligence enterprise**

## Brigade Combat Team Headquarters Intelligence Section

**F-13.** The BCT is configured in one of three ways: as a heavy brigade combat team (HBCT), an infantry brigade combat team (IBCT), or a Stryker brigade combat team (SBCT). The HBCT and IBCT each have a brigade special troops battalion (BSTB) under which the military intelligence company falls for command and control. The military intelligence company (MICO) in an SBCT is directly subordinate to the SBCT. The BCT headquarters has an S-2 staff that assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units.

**F-14.** Like the theater army, corps, and division G-2, the BCT S-2 is equipped with Web-based intelligence processors that allow data sharing with all echelons. These processors are connected to JWICS, SIPRNET, and NIPRNET. These processors are interoperable with all ABCS and can share data with all organizations in the Army and defense intelligence enterprises as well as those nonmilitary members of the intelligence community that use JWICS, SIPRNET, and NIPRNET. Figure F-6 illustrates BCT S-2 integration into the Army intelligence enterprise.

**F-15.** The S-2 section is structured, equipped, and trained to support the BCT commander and staff in

evaluating the operational environment to support brigade operations. The BCT intelligence staff is the first echelon where all of the intelligence warfighting function elements come together.

**F-16.** The brigade intelligence staff consists of the S-2 and the S-2 staff. The S-2 is responsible for intelligence operations, planning, production, and training. The brigade does not have a dedicated S-2 operations officer or planner authorized according to the table of organization and equipment (TOE); therefore, the S-2 must task organize to accomplish these functions.

## S-2 Intelligence Officer

**F-17.** The S-2 is the BCT's senior intelligence staff officer for all intelligence, surveillance and reconnaissance (ISR) synchronization matters. The S-2 ensures the brigade's complex ISR operations satisfy the commander's critical information requirements (CCIR) specifically the priority information requirements (PIR) and those of subordinate units. The S-2, together with the S-3, helps the commander coordinate, integrate, and supervise the execution of ISR plans and operations. The S-2 is also responsible for providing immediate intelligence support to subordinate unit commanders. The S-2 advises the commander on the capabilities of organic ISR assets, echelons above brigade intelligence collection capabilities, automated intelligence systems, and the intelligence architecture. The S-2 assists the commander on focusing and integrating these assets and resources to satisfy the brigade intelligence requirements.

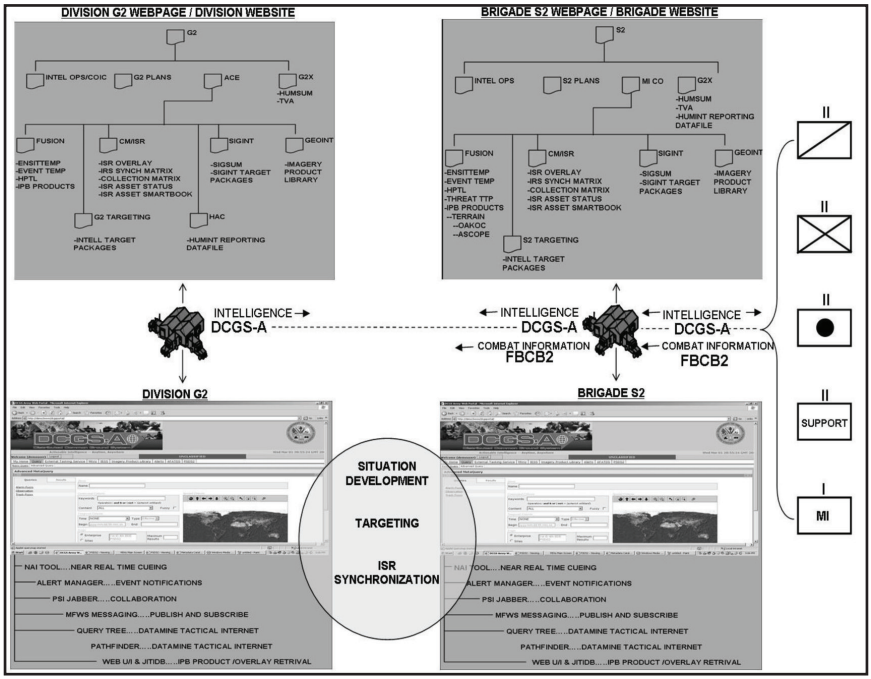



**Figure F-6. BCT to division Army intelligence enterprise**

## S-2 Operations

**F-18.** The S-2 operations team is responsible for threat situation development and presentation in support of current full spectrum operations. The S-2 operations team focuses on threat activity within the brigade's area of operation (AO) and area of interest that affect the current operation. The S-2 operations team uses the Distributed Common Ground Station-Army (DCGS-A) enterprise and automated tools to continuously integrate information and intelligence products from subordinate battalion S-2s and supporting ISR organizations to update the threat situation. This situation assessment forms the threat portion of the brigade common operational picture (COP). The S-2 operations team assists the S-2 in tracking threat courses of action (COAs) and alerting the commander of changes to predicted threat COAs, capabilities, or intentions.

## S-2 Plans

**F-19.** The S-2 plans team is responsible for threat COA development and wargaming.

## S-2X

**F-20.** The S-2X is the commander's principal advisor for all matters concerning the conduct of human intelligence (HUMINT) and counterintelligence (CI) activities. The S-2X provides oversight and technical support for all HUMINT and CI activities. The S-2X assists the brigade in developing the HUMINT and CI (when CI resources are attached) collection requirements.

**F-21.** The S-2X section provides the expertise for the conduct of HUMINT and CI operations (when CI resources are attached) in the brigade's operational environment. While the military intelligence company (and reconnaissance squadron for the SBCT) is responsible for tactical HUMINT collection and CI support within the brigade, the S-2X provides the collection focus, technical support, and technical guidance. The S-2X receives direct support and advice from the brigade operational legal team (BOLT).

**F-22.** Within a BCT there are no organic CI operational management teams (OMTs) or CI teams. CI teams may be pushed down from the BFSB or other higher echelon unit to a BCT. These teams must be controlled by the brigade S-2X.

## S-2 Weather Team

**F-23.** For the brigade to conduct effective full spectrum operations, all the brigade's staff sections as well as subordinate commands and staffs must have current, high-resolution, tailored weather intelligence information upon demand. Although the brigade will rely heavily on "reach" for intelligence and weather support, it will require local tailoring of weather products by on-site weather people. A deployed battlefield weather team (BWT) will be inside the military decisionmaking process (MDMP) process loop at the brigade level and will be ready to recommend alternative ingress, egress, or COAs to exploit weather intelligence as a force multiplier. To effectively support the brigade's warfighting capabilities, the BWT is allocated workspace and power within the brigade.

## Brigade Special Troops Battalion S-2 Section

**F-24.** The S-2 is the officer in charge (OIC) of the BSTB section, and is responsible for collecting and applying intelligence to support operations. The S-2 section plays a vital role in planning and executing battalion operations. The S-2's coordination and interaction with the S-3 is critical to deploying battalion assets and BCT mission accomplishment.

## Armored Reconnaissance and Surveillance Battalion S-2 Section

**F-25.** The S-2 and staff are responsible for the following functions: pulls higher current situation overlays, collaborates and integrates with BCT ISR integration platoon and BCT S-2, loads relevant overlays and maintains the enemy situation overlay. The S-2 section also forwards sensor and/or unit reports to the BCT S-2.

### Surveillance Troop

**F-26.** The *surveillance troop* and the ground reconnaissance troops of the SBCT reconnaissance squadron execute reconnaissance and surveillance. The reconnaissance squadron and the troop coordinate the reconnaissance and surveillance to—

- Answer the commander's CCIR.
- Answer gaps in the unit's intelligence preparation of the battlefield (IPB) through intelligence requirements.
- Support targeting through target acquisition.

**F-27.** The surveillance troop consists of a headquarters section, an air reconnaissance platoon, a multi-sensor platoon, and a chemical, biological, radiological, and nuclear (CBRN) reconnaissance platoon. The reconnaissance squadron receives a TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT)-Lite team which may be attached or operational control (OPCON) from the signal company to support unmanned aircraft system (UAS) video dissemination to the brigade tactical operations center (TOC). Figure F-7 illustrates the organization of the surveillance troop.

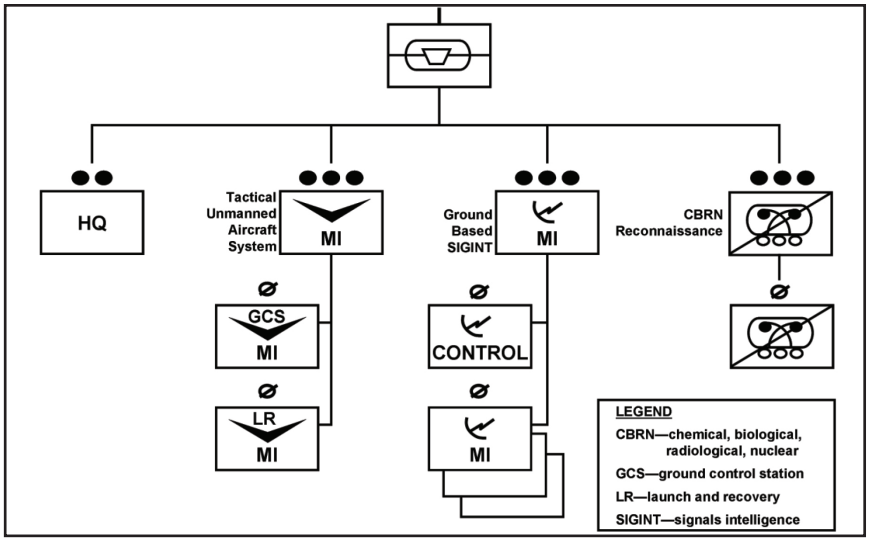



**Figure F-7. Surveillance troop organization**

## Fires Battalion S-2 Section

**F-28.** The fires battalion S-2 is responsible for collecting and applying intelligence to support operations. The S-2 provides IPB and an update of the enemy situation.


FOR OFFICIAL USE ONLY

## Maneuver Battalion Headquarters Intelligence Section

**F-29.** The maneuver battalion has an intelligence section that produces the intelligence products and assessments required for offensive, defensive, stability, and civil support operations. Normally, this means taking an intelligence product developed by the brigade staff and refining it to support battalion operations. However, this is not always the case. The S-2 section also conducts independent analysis and develops independent intelligence products that it posts to the intelligence portion of the battalion's website.

**F-30.** Through its intelligence processors, the battalion S-2 is fully integrated into a secure digital network and has immediate access to all information and intelligence produced by the brigade S-2 as well as those products developed by division, corps, theater, national intelligence agencies, and nonmilitary members of the U.S. intelligence community. These intelligence processors enable the battalion S-2 to maintain intelligence datafiles that are searchable by authorized users. These processors also give the battalion S-2 the ability to collaborate and conduct parallel planning with external intelligence agencies.

**F-31.** Through the S-2 section, combat information collected by maneuver companies and reconnaissance forces is processed and made available to interested intelligence agencies. Figure F-8 illustrates battalion S-2 integration into the Army intelligence enterprise.

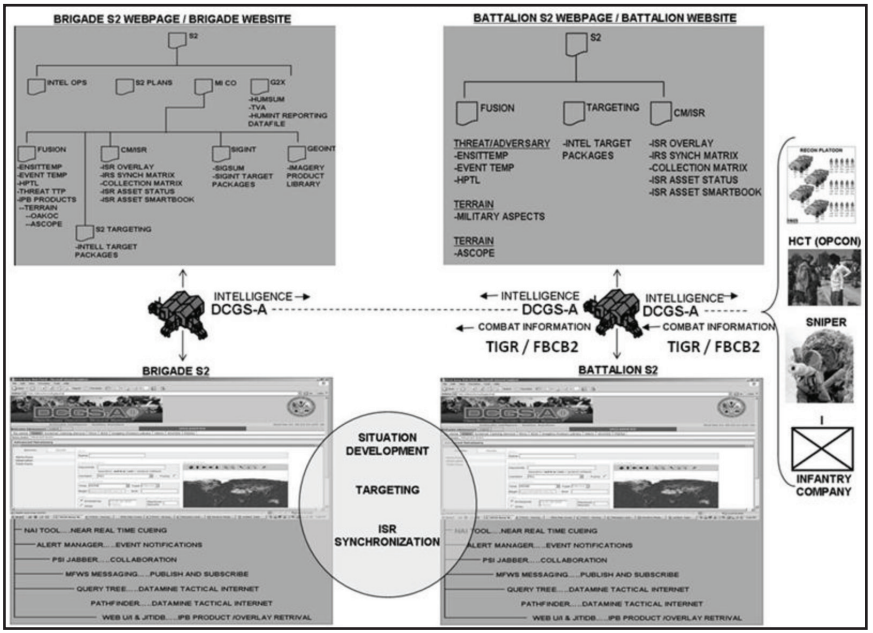



**Figure F-8. Battalion to brigade Army intelligence enterprise**

## Military Intelligence Company

**F-32.** The military intelligence company conducts ISR analysis, intelligence synchronization, and HUMINT collection. It provides analysis and intelligence synchronization support to the BCT S-2. The company supports the BCT and its subordinate commands through collection, analysis, and

dissemination of intelligence information and products. It provides continual input for the commander through maintaining the threat portion of the COP in a timely and accurate manner. The military intelligence company also collaborates with the BCT S-3 in integrating ISR tasks and coordinating requirements and HUMINT operations as directed by the BCT S-3 and S-2X.

**F-33.** The military intelligence company is assigned to the brigade special troops battalion (BSTB) for command and control, but much of their oversight comes from the BCT S-2. It operates under the direction of the S-2, but must keep the BSTB commander informed as determined by unit standing operating procedures (SOP). The composition of the militarsy intelligence company is shown in figure F-9.

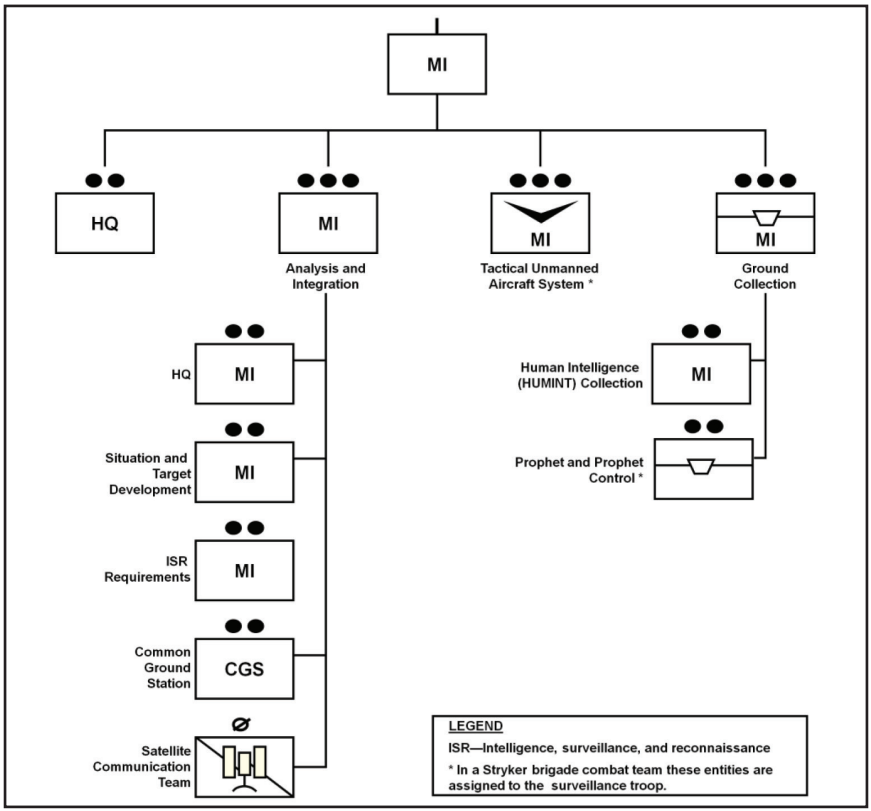



**Figure F-9. Organization of the military intelligence company**

### Headquarters Element

**F-34.** The company headquarters element consists of the commander, First Sergeant, and supply sergeant. The headquarters personnel control all the company's operational, logistical, administrative, and training activities.

### Platoon Headquarters

**F-35.** The platoon headquarters is normally located where it can best command and control the platoon elements. All three platoons—analysis and integration, UAS, and ground collection—normally will be co-located with the BCT S-2. Elements of the UAS platoon and ground collection platoon could be deployed anywhere in the AO.


FOR OFFICIAL USE ONLY

### Analysis and Integration Platoon

**F-36.** The analysis and integration platoon provides the BCT S-2 analytical support. The ISR requirements section and the situation and target development section collocate with the brigade command post and are under OPCON of the BCT S-2. They provide the BCT S-2 automated intelligence processing, analysis, and dissemination capabilities as well as access to the intelligence products of higher echelons.

### Tactical Unmanned Aircraft System Platoon

**F-37.** The UAS platoon provides the commander real-time visual imagery in support of reconnaissance and targeting operations.

> ***Note.*** Within an SBCT, the UAS platoon and ground collection platoon are assigned to the surveillance troop, instead of the military intelligence company.

### Ground Collection Platoon

**F-38.** The ground collection platoon contains a tactical HUMINT section and a Prophet control section.

**F-39.** The tactical HUMINT section collects HUMINT through screening interrogations, debriefing contact operations, and support to document and media exploitation (DOMEX). The tactical HUMINT Section coordinates and executes HUMINT operations as directed by the brigade S-3 in coordination with the brigade S-2 and S-2X. The Prophet control section coordinates and executes signals intelligence (SIGINT) operations as directed by the brigade S-3 in coordination with the brigade S-2.

**F-40.** The BWT, when attached, provides the BCT with a weather prediction and weather effects analysis capability. The BWT is the main source of weather support for all brigade warfighting functions. As a member of the commander's special staff, the staff weather officer (SWO) is responsible for coordinating weather and service matters through the S-2. The SWO is the weather liaison between Army customers and the Air Force forecasting resources developed at centralized (regional) production centers. The Army commander has tactical control (TACON) of the SWO.

## Fundamental Considerations

**F-41.** The military intelligence company commander assists the brigade S-2 with the development of the intelligence running estimate and all intelligence products and deliverables needed to support the brigade orders process. These include but are not limited to the mission analysis briefing, base operation order (OPORD) input, annex B, and annex L. The military intelligence company commander advises the brigade S-3 on the employment of what echelon above brigade intelligence collection platforms or agencies are available in the brigade AO that can be incorporated into brigade planning. As soon as the brigade commander approves the plan, the military intelligence company commander produces the company OPORD, and prepares to support the brigade's ISR plan.

## Command and Support Relationships

**F-42.** The ISR requirements section and the situation and target development section of the analysis and integration platoon normally operate under OPCON of the BCT S-2. The UAS platoon and the ground collection platoon assets may be deployed within the BCT's AO under differing command and support relationships. The SBCT's reconnaissance squadron assets may deploy under differing command and support relationships that may also require similar coordination and planning. These relationships may require the military intelligence company commander to conduct logistical and security coordination and planning with other brigade command and control elements. Support relationships are specific relationships established between supporting and supported units. The military intelligence company may place HCTs in direct support to brigade elements. In this support relationship, the military


FOR OFFICIAL USE ONLY

intelligence company retains command and control of the teams including responsibility for logistics and task organization. The maneuver unit can position the team within its AO and set its collection priorities. This is most common in supporting offensive and defensive operations. In general support the teams operate in the AO of brigade elements but are under the OPCON of the brigade, as exercised through the military intelligence company commander and the ground collection platoon leader for positioning the assets and for assigning collection priorities. Additionally, the military intelligence company commander may physically co-locate the OMT of the ground collection platoon with the brigade's S-2X section.



## Command Posts and Operations Centers

**F-43.** The command and control facilities and the DCGS-A enterprise provide the commander with the means necessary to manage information, coordinate action, make decisions, and disseminate orders for effective command and control. These facilities sustain the operation through continuity, planning, and coordination of operations and support. The military intelligence company normally is co-located with the brigade TOC to facilitate command and control of the company assets and to maximize BCT S-2 support. The military intelligence company command post includes the company headquarters element, the analysis and integration platoon, the UAS platoon, and the ground collection platoon. During brigade operations the situation and target development section and ISR requirements section are typically under OPCON of the BCT and HUMINT collection team of the ground collection platoon operate under direct support of maneuver battalions and the reconnaissance squadron or even their subordinate companies and troops.

## Command and Control Communications

**F-44.** The military intelligence company operates on several communications and processing nets. Communications redundancy ensures that support to brigade operations will not be severely disrupted by the loss of any one system or command post. The military intelligence company assets use three basic communications nets: the operations and intelligence nets, command nets, and a discipline-specific technical net. Depending on their mission and battlefield location, the company or subordinate elements may also need to monitor the fire support element (FSE), aviation, or air defense artillery (ADA) communications nets.

- Operations and intelligence nets or DCGS-A links the intelligence collectors and producers to the consumers of the intelligence information. They are used to pass information of immediate value to the affected unit and to analytical elements at the supported unit.
- Command nets link the superior headquarters with its subordinate elements. Normally a unit will operate on two command nets; the one that links that unit to its higher headquarters and the one that links that unit to its subordinate elements.
- Technical nets link the control team to subordinate collection teams and to the centers or organizations that provide the databases and technical guidance necessary for single discipline collection and analysis.

**F-45.** TROJAN SPIRIT communication systems are organic to the MICO. Through the DCGS-A network centric enterprise the intelligence analysts assigned to the TROJAN SPIRIT access the dedicated multilevel security, high-capacity communication link between BCT CPs, national centers, and other intelligence organizations outside the BCT's AO to pull intelligence products, receive and analyze routed direct downlinks, and access external databases to fuse with organically collected information. The TROJAN SPIRIT also provides access to the JWICS through its Joint Deployable Intelligence Support System (JDISS).

## Company Intelligence Support Team

**F-46.** The maneuver company has an intelligence support team that assists the commander in processing and analyzing combat information provided by its platoons and integrating intelligence developed by higher and adjacent units.

**F-47.** The COIST is equipped with intelligence processors that allow data sharing with all echelons. The current intelligence processor used by the COIST is the Tactical Ground Reporting System (TIGR). TIGR is a multimedia reporting system for soldiers at the patrol level, allowing users to collect and share information to improve situational awareness and to facilitate collaboration and information analysis among junior officers. TIGR is fully accredited to operate on SIPRNET and NIPRNET. It is optimized for use in low bandwidth environments. TIGR is web-based and interoperable with the DCGS-A, the combined information data network exchange (CIDNE), the command post of the future (CPOF), and the Force XXI Battle Command Brigade and below (FBCB2) system.

**F-48.** Though the COIST can access the tactical internet, it normally does not establish a Web site. This is due to the fact that it operates in a low bandwidth environment and belongs to a headquarters that normally does not operate from a fixed location. The theater, corps and division G-2 can access the reporting generated by the COIST through DCGS-A. Figure F-10 illustrates COIST integration into the Army intelligence enterprise.

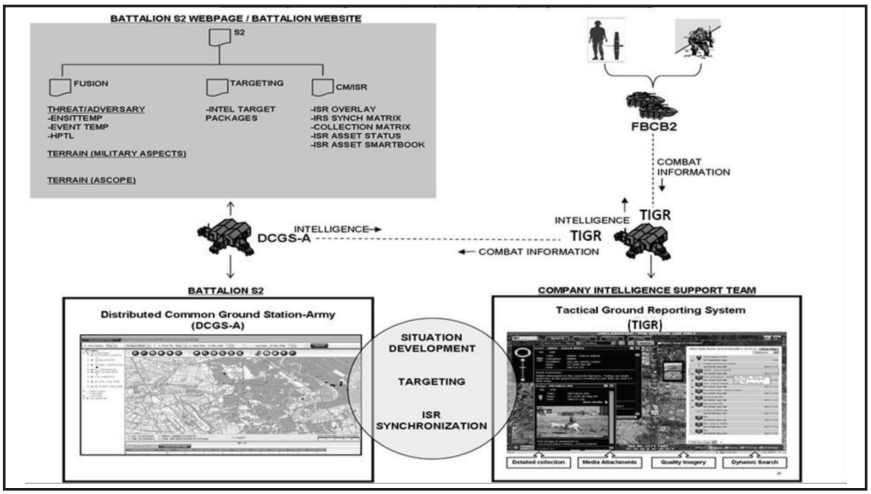



**Figure F-10. The Army intelligence enterprise (company to battalion)**

**F-49.** COISTs fuse intelligence and operations within a designated AO. The COIST uses information derived from all intelligence disciplines to determine changes in enemy capabilities, vulnerabilities, and probable COAs. The initial analysis of the area of responsibility is provided to the company by the battalion or brigade S-2 section. The COIST refine these products based on knowledge gained from assets performing missions in the assigned company area of responsibility. Table F-1 reflects the responsibilities of the COIST members.

**Table F-1. Responsibilities of COIST members**

| Position | Duties and responsibilities |
|---|---|
| COIST OIC<br>Officer in charge | Overall responsibility for COIST mission accomplishment and Soldiers.<br>Ensures COIST members are tasked appropriately and priorities of work are indentified.<br>Communicates with the battalion to ensure all intelligence and collection assets are available to the company and that tasked appropriately and effectively. |
| COIST NCOIC<br>Noncommissioned Officer in charge | The NCOIC ensures all priorities of work are completed and the analysts have the time and the appropriate area to conduct their work. The NCOIC provides guidance and support when needed. The NCOIC is the primary liaison between the COIST and the companies to ensure the analysts are not distracted from the day to day operations and they are able to conduct their work without outside interference.<br><br>• Performs duties of COIST analysts.<br>• Provided guidance to subordinate Soldiers.<br>• Supervises the receipt, analysis, dissemination, and storage of intelligence information.<br>• Supervises the IPB process.<br>• Provides quality control analysis performed by subordinates.<br>• Assists in the preparation of indicators to satisfy priority intelligence requirements.<br>• Provides current situation briefings to subordinates.<br>• Receives, produces, and disseminates intelligence reports containing information obtained from all sources.<br>• Supervises intelligence operations within the company.<br>• Acts as liaison between COIST and higher echelon S-2 sections. |

**Table F-1. Responsibilities of COIST members (continued)**

| Position | Duties and responsibilities |
|---|---|
| COIST Analysts | The Soldiers filling the analyst role in the COIST carry out the majority of the COIST duties. They are responsible for reading, interpreting, researching, and analyzing all available information in the company AOR or that may affect the company AOR. The analyst is usually the most knowledgeable and most informed member of the COIST because of their workt and the amount of time spent on their tasks. The primary duties of the analyst are:<br><br>• Prepare intelligence products to support the company commander.<br>• Assist in establishing and maintaining systematic, cross-referenced intelligence records and files.<br>• Receive and processe incoming reports and messages.<br>• Assist in determining significance and reliability of incoming information.<br>• Assist in integrating incoming information with current intelligence holdings.<br>• Prepare and maintain the situation map.<br>• Assist in the analysis and evaluation of intelligence holdings to determine changes in enemy capabilities, vulnerabilities, and probable courses of action.<br>• Assist in the preparation of threat characteristics using information from all sources and in the preparation of estimates of enemy units and organizations strengths, capabilities, and TTP.<br>• Assist in identifying information gaps.<br>• Assist in preparing and submitting requests for information (RFIs) to adjacent/higher units.<br>• Assemble and proofread reports and assists in consolidating them into military intelligence.<br>• Prepare IPB products.<br>• Assist in the preparation of reports on captured enemy material.<br>• Draft periodic and special intelligence reports, plans, and briefings.<br>• Assist in preparing collection requirements for unit patrols.<br>• Brief and debrief patrols. |

**F-50.** Many units use the fire support officer (FSO) to lead the COIST. FSOs and fire support noncommissioned officers (NCO) often assume responsibilities at the company level for performing or coordinating the following:

- Targeting.
- Air-ground integration.
- Information engagement related operations.
- Coordination of civil-military operations related operations.
- Coordination of Psychological Operations (PSYOS) with the first attached or assigned PSYOPS officer or NCO in the chain of command.
- Employing enablers.
- Public affairs.

**F-51.** The COIST focuses on three areas—processing data, performing pattern analysis, and supporting HUMINT-related operations. Table F-2 illustrates the specifics of processing data and performing pattern analysis, and table F-3 illustrates the specifics of support to HUMINT-related operations.

Table F-2. COIST focus

| Process data and conduct pattern analysis. | |
|---|---|
| **Task** | **Description** |
| ***Assist in developing the commander's priority intelligence requirements (PIRs).*** | Well-written PIRs meet the following criteria:<br>• They provide intelligence required to support a single planning task, decision, or action.<br>• They ask only one question.<br>• They focus on a specific fact, event, or activity.<br>• They can be satisfied using available assets or capabilities. |
| ***Conduct intelligence preparation of the battlefield (IPB) for company operations.*** | The COIST—<br>• Follows the four step IPB process<br>• Receives IPB products from the battalion.<br>• Refines the higher echelon IPB products to the company's specific AOR.<br>• Adds information such as changes in infrastructure, identification of local leaders, and the identification of criminal and adversarial groups in the AOR.<br>***Note:*** Company level IPB products should be synchronized with higher and lateral echelons to improve the overall intelligence picture. |
| ***Manage the patrol pre-brief/ debrief process.*** | The ***pre-brief*** is given to the patrol leader prior to departure and consists of events that occurred in the AOR over the past 12 to 24 hours, such as:<br>• Route status.<br>• ISR collection assets in use throughout the unit's operating environment.<br>• Specific intelligence requirements tasked to answer.<br>• Other units operating within the AOR.<br>• Be on the lookout (BOLO) lists.<br>• Predictive analysis based on analysis of events.<br>The mission ***debrief***—<br>• Reviews the route traveled.<br>• Reviews the collection objectives of the patrol.<br>• Reviews methods employed by patrols.<br>• Captures information the patrol was to collect.<br>• Captures any other information and observations the patrol made concerning the AOR.<br>• Collects any fliers, pamphlets, media, or pictures the patrol found or obtained.<br>The COIST uses the applicable information from the debrief to update any assessments, matrices, or databases which may have changed due to the information obatined by the patrol. |


FOR OFFICIAL USE ONLY

Table F-2. COIST focus (continued)

| Task | Description |
|---|---|
| ***Maintain intelligence board for outgoing patrols.*** | Contents of the intelligence board include—<br>• CCIRs.<br>• PIR.<br>• Friendly force information requirements (FFIR).<br>• Essential elements of information (EEFI).<br>• Maps.<br>• Link analysis charts.<br>• Recent enemy tactics, techniques, and procedures (TTP).<br>• Trend analysis.<br>• BOLO lists.<br>• Significant activity (SIGACTS).<br>• Light and weather data.<br>• Battle damage assessments (BDA), including detainee status. |
| ***Track and analyze all significant activities (SIGACTS).*** | The COIST conducts event analysis in order to determine patterns of enemy events, for example, time, place, and type of activity. The two predominant tools for event tracking are the—<br>• Analysis time event wheel.<br>• Graphic map display which can be a physical map, computer map, or a combination of both, which is the preferred method. |
| ***Conduct local intelligence analysis and forecast enemy actions.*** | Pattern analysis is conducted to identify the activity and TTP that enemy forces employ by careful observation and evaluation of patterns in their activities. The primary tool is the pattern analysis plot sheet, which can illustrate timeframes of enemy activity such as—<br>• Bombings occur in the early morning.<br>• Ambushes are an evening event.<br>• Kidnappings take place very late at night. |
| ***Database information.*** | The COIST is responsible for collecting and archiving data at the company for use at all echelons. Examples of local databases include—<br>• Enemy activities matrix.<br>• Personality tracker.<br>• Mug shot file. |


FOR OFFICIAL USE ONLY

Table F-2. COIST focus (continued)

| Task | Description |
|---|---|
| ***Display AO and AOI information graphically.*** | Another COIST task is to graphically display each enemy activity or significant event that takes place within the company's AOR in a format that is easy to display, update, and transmit. One way is to use an enemy activities overlay. Another is to use special assessments or storyboards, which should contain, the following:<br>• Detailed summary of the event if required for clarification.<br>• WHO—Unit reporting the significant activity and the intelligence sources.<br>• WHAT—Description of the activity.<br>• WHERE—Location: zone/neighborhood with grid.<br>• WHEN—DTG of the activity.<br>• WHY—Assessment - near term analysis of threat intent and activity.<br>• Map or imagery with callouts or symbols that depict where the event occurred.<br>• May be grouped by unit, activity, timeframe, or operation (situation dependent). |

Table F-3 Support HUMINT related operations

| Task | Description |
|---|---|
| ***Assist management of bilateral and leadership engagement.*** | The COIST maintains all known information of community leaders to assist Soldiers and unit leaders in planning engagements. For example, information about the individual's—<br>• Position in the community.<br>• Family.<br>• Personality.<br>• Links to other individuals.<br>• Historical activities.<br>Once the engagement is complete, the files should be updated to maintain the most current information. |
| ***Assist with detainee operations.*** | The COIST—<br>• Ensures departing patrol units are armed with complete blank detainee packets and the knowledge to properly complete the forms.<br>• Maintains copies of complete packets and tracks current location and status of the company's detainees. |
| ***Manage walk-in informants.*** | If no HUMINT collection team (HCT) personnel are available, COIST personnel assist in screening walk-ins. |

## INTELLIGENCE COLLECTION OPERATIONS

**F-52.** The COIST is responsible for analyzing information collected from—

- Patrols.
- Raids.
- Interacting with the local population (bilateral and leader engagements).
- Site exploitation (SE).
- Tactical questioning.
- Civil Affairs and PSYOPS reports which may provide information on the local politics, economy, demographics, perceptions, and infrastructure.
- Coalition partners.
- Contracting officers.
- Multinational operations centers.
- Nongovernment organizations.
- Special Forces reporting.
- U.S. civilians, such as contractors or journalists, who offer information. For legal reasons, it is important to understand regulations regarding intelligence-related information collected from U.S.

## BATTLEFIELD SURVEILLANCE BRIGADE INTELLIGENCE SECTION

**F-53.** The BFSB collects combat information and intelligence using UASs, ground-based signals intelligence sensors, HUMINT collection teams, long range surveillance teams, and ground reconnaissance assets.

**F-54.** This information and intelligence is transmitted from the sensor to the BFSB to the BFSB S-2 over the BFSB's digital battle command network. This information is also forwarded to the G-2 staffs of supported corps or division headquarters.

**F-55.** BFSBs are equipped with Web-based intelligence processors that allow data sharing with all echelons. These processors are connected to JWICS, SIPRNET, and NIPRNET. These processors are interoperable with all ABCS and can share data with all organizations in the Army and defense intelligence enterprises as well as those nonmilitary members of the intelligence community that use JWICS, SIPRNET, and NIPRNET. Figure F-11 illustrates BFSB integration into the Army intelligence enterprise.

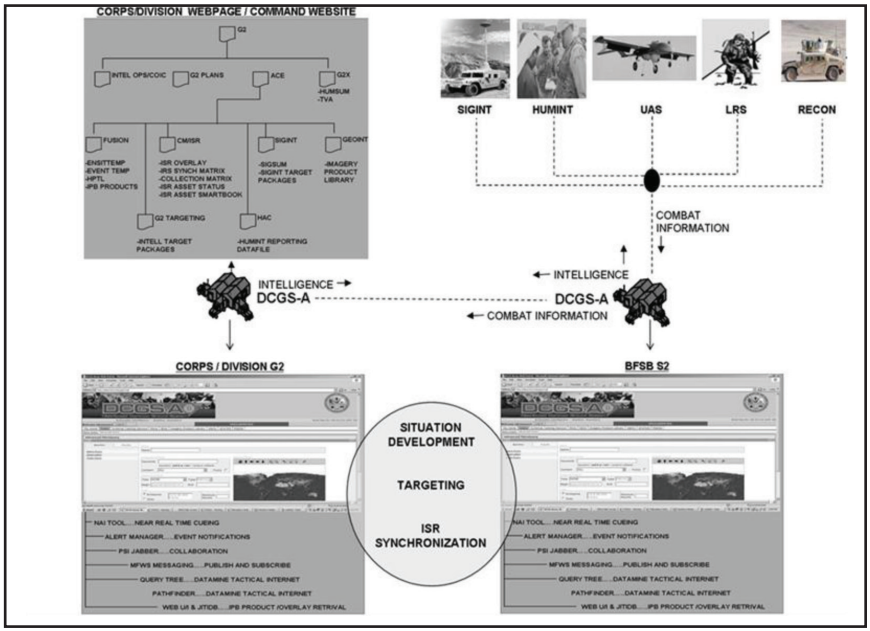



**Figure F-11. The Army intelligence enterprise (BFSB)**

## Every Soldier is a Sensor

**F-56.** Every Soldier is responsible for detecting and reporting threat activities, dispositions, and capabilities. The Army's Every Soldier is a sensor program was established through Soldier surveillance and reconnaissance to help commanders to get combat information and reports. See FM 2-91.6 for a detailed discussion about Soldier surveillance and reconnaissance.

# Appendix G

# The Military Intelligence Career Fields

## INTRODUCTION

**G-1.** The military intelligence (MI) career field consists of branch officer areas of concentration (AOCs), branch officer functional areas (FAs) (see DA Pam 600-3), warrant officer AOCs, and enlisted military occupational specialties (MOSs). Various intelligence disciplines are represented in these fields:

- All-source intelligence.
- Counterintelligence (CI).
- Human intelligence (HUMINT).
- Geospatial intelligence (GEOINT).
- Imagery intelligence (IMINT).
- Signals intelligence (SIGINT).
    - Communications intelligence (COMINT).
    - Electronic intelligence (ELINT).
    - Foreign instrumentation signals intelligence (FISINT).

## BRANCH OFFICER AREAS OF CONCENTRATION

**G-2.** All-source intelligence officer (AOC 35D) duties include the following:

- Directs, supervises, and coordinates the planning, collection, evaluation, fusion, analysis, production, and dissemination of all-source intelligence and CI at any echelon.
- Performs multidiscipline intelligence, surveillance, and reconnaissance (ISR) requirements, coordinates surveillance and reconnaissance activities, and provides advice on the use of intelligence resources at all echelons.
- Supervises and performs intelligence preparation of the battlefield (IPB) and uses automated intelligence data processing systems.
- Advises commanders and subordinate units on the threat, terrain and weather, and civil considerations.

**G-3.** CI officer (AOC 35E) duties include the following:

- Plans, directs, manages, coordinates, and participates in the collection, production, and dissemination of CI information and the conduct of CI investigations and operations.
- Provides CI input and assistance to protection planning and execution by limiting the effectiveness of foreign multidiscipline collection directed against Army operations, activities, technology, and personnel at all echelons, including joint, interagency, and multinational forces.

**G-4.** HUMINT officer (AOC 35F) duties include the following:

- Plans, directs, manages, coordinates, and participates in controlled collection operations to obtain intelligence information in support of Army and Department of Defense (DOD) requirements.
- Develops and approves interrogation plans, document translations, and missions.
- Advises the supported element on the best employment of HUMINT collection assets.
- Coordinates closely with other intelligence and nonintelligence agencies regarding interrogation and military source operations (MSO). Writes, reviews, and approves interrogation and intelligence reports that include document translations and limited technical intelligence (TECHINT) reports.

**G-5.** IMINT officer (AOC 35C) duties include the following:

- Performs and supervises the exploitation and analysis of optical, infrared, and radar imagery using techniques of photogrammetry and terrain analysis.
- Uses electronic, mechanical, and optical devices to support tactical and strategic reconnaissance and surveillance operations.

***Note.*** In October 2009, AOC 35C was phased out and replaced with skill identifier (SI) 1D. All officers currently trained in this SI fall under AOC 35D. On 30 September 2011, all officers currently classified as AOC 35C will be recoded as AOC 35D1D. At the same time, modified tables of organization and equipment (MTOEs) that show AOC 35C will change to reflect the new code.

**G-6.** SIGINT/Electronic warfare (EW) officer (AOC 35G) duties include the following:

- Plans, directs, manages, coordinates, and participates in the collection, production and dissemination of SIGINT (COMINT, ELINT, and FISINT) at the tactical, operational, and strategic levels including joint, interagency, and multinational forces.
- Performs reporting in accordance with SIGINT directives to produce combat information and intelligence.
- Establishes priorities of intercept missions for acquisition of desired traffic.
- Coordinates SIGINT analytical projects.
- Advises and assists commanders and staff officers in planning for SIGINT activities.

## BRANCH OFFICER FUNCTIONAL AREAS

**G-7.** Strategic intelligence officer (FA 34A) duties include the following:

- Coordinates, supervises, and participates in all-source current intelligence indications and warning, threat analysis, and general military intelligence activities focusing on the intentions, geography, and military capabilities of foreign nations, with primary focus on the ground forces.
- Develops collection and production requirements and oversees acquisition of information and intelligence including targeting strategic- and theater-level threat collection resources.
- Evaluates, interprets, analyzes, and produces general intelligence products in support of DOD and combatant commander requirements.
- Supervises and performs IPB and uses automated data processing systems.
- Advises commanders and subordinate units on the threat, terrain and weather, and civil considerations.

## WARRANT OFFICER AREAS OF CONCENTRATION

**G-8.** All-source intelligence technician (AOC 350F) duties include the following:

- Develops all-source intelligence products through the fusion of data accumulated from maps and intelligence information derived from a variety of sources.
- Makes reliability assessments of information received by comparing it with previously evaluated information on hand.
- Maintains close liaison with other staff elements and specialized intelligence activities, including CI, IMINT, HUMINT, measurement and signature intelligence (MASINT), SIGINT, and language interpretation units.
- Ensures compliance with computer interface and operating procedures, concepts, and principles as applied to automated data processing in the development and maintenance of intelligence databases.
- Develops and maintains situation maps, overlays, and reports to provide complete and accurate intelligence information to users.

- Establishes and maintains files as a basis for information to support commanders' decisions.
- Maintains current information concerning friendly and threat characteristics.
- Develops and prepares threat vulnerability studies and evaluates their significance for use in predicting probable threat courses of action (COAs) in terms of disposition, capabilities, and intentions.
- Supervises intelligence production operations and ISR activities.

**G-9.** CI technician (AOC 351L) duties include the following:

- Conducts investigations and operations by applying sound judgment and analytical reasoning methods to detect and prevent acts of espionage, sabotage, and terrorism directed against Army activities.
- Supervises investigative, operational, and administrative personnel. Manages investigative and operational elements of varying sizes commensurate with skill and experience level.
- Prepares, reviews, and approves investigative and operational reports of investigations and inspections.
- Performs terrorism counteraction analysis and threat analysis. Investigates national security crimes of Army interest as defined by regulation, the Uniform Code of Military Justice, or applicable sections of the United States Code.
- Conducts and supervises both overt and covert investigations. Supervises the technical performance of subordinate military and civilian personnel in related job skills. Develops, evaluates, and manages sources and informants of military intelligence. Develops and approves investigative plans.
- Obtains and executes arrest and search warrants in coordination with the Criminal Investigation Command or the Federal Bureau of Investigation. Interviews and interrogates witnesses, suspects, and subjects and obtains written statements executed under oath.
- Represents the Army's interests in investigations conducted collaterally with DOD, Department of Justice, and other federal, state, or local investigative agencies.

**G-10.** HUMINT collection technician (AOC 351M) duties include the following:

- Interrogates, debriefs, translates, and interprets as defined by regulation the Uniform Code of Military Justice, and other applicable regulations and agreements.
- Conducts and supervises both tactical and strategic HUMINT- and interrogation-related duties, including MSO.
- Supervises the technical performance of subordinate military and civilian personnel in related job skills.
- Develops and approves interrogation plans, document translations, and missions.
- Advises the support element on the best employment of HUMINT collection assets.
- Coordinates closely with other intelligence and nonintelligence agencies regarding interrogation and MSO. Writes, reviews, and approves interrogation and intelligence reports that include document translations and limited TECHINT reports.
- Performs language support in the form of translation or interpreter duties when required.

**G-11.** IMINT technician (AOC 350G) duties include the following:

- Directs, supervises, and performs the planning, collection, exploitation, and dissemination of initial to comprehensive GEOINT reports, briefings, and products.
- Leads imagery analysis elements and manages imagery systems, files, and databases within DOD, Joint Chiefs of Staff (JCS), combatant commands, and Army organizations.
- Validates imagery collection and exploitation strategies in support of operations.
- Synchronizes and cues tactical, theater, and national imagery ISR.
- Supports the planning process on targeting and battle damage assessment efforts.
- Provides technical expertise on IMINT architecture, integration of new technologies and equipment, and future intelligence activities.
- Provides GEOINT input to tactics, techniques, and procedures.

**G-12.** Attaché technician (AOC 350Z) duties include the following:

- Meets with foreign and U.S. visitors, guests, and government representatives at highest levels of government and civilian structure; must be capable of discussing matters of national-level policy interest.
- Coordinates operations and operational support of the defense attaché office.
- Applies regulations, directives, and procedures necessary for managing HUMINT collection operations.
- Correlates information regarding operational travel, fiscal matters, personnel and materiel resources, collection strategies, and HUMINT requirements into a tactical collection management plan.
- Serves as a principal advisor to the defense attaché in matters involving the Defense Intelligence Agency (DIA), Department of State, Army, Navy, Air Force, and Marine Corps, and deals with policies and procedures of other agencies in the operations and operational support arenas.
- Advises other defense attaché office personnel and visitors regarding matters of security, protocol, military courtesies, and public affairs.
- Reads, interprets, and prepares intelligence information reports, technical reports, electrical communications, and other information.
- Authenticates budgets, purchase orders, obligation liquidation documents, requests for supplies, and any other correspondence necessary to ensure office support.

**G-13.** SIGINT analyst (AOC 352N) duties include the following:

- Manages personnel and equipment to collect, process, locate, identify, and analyze SIGINT intercepts.
- Performs reporting in accordance with SIGINT directives to produce combat information and intelligence.
- Establishes priorities of intercept missions for acquisition of desired traffic.
- Coordinates SIGINT analytical projects.
- Advises and assists commanders and staff officers in planning for SIGINT activities.

**G-14.** Non-Morse intercept technician (AOC 352S) duties include the following:

- Manages personnel and equipment assets in establishing and employing non-Morse intercept activities.
- Plans, coordinates, and supervises activities of personnel engaged in non-Morse operations, establishes work schedules and priorities, and evaluates performance of subordinates.
- Coordinates collection activities with applicable traffic analysis and cryptonalysis personnel.
- Plans and coordinates procedures for the performance of maintenance, calibration, adjustment, and test of non-Morse intercept personnel and equipment.
- Establishes, directs, and evaluates qualification training programs for non-Morse operations.

**G-15.** Intelligence EW systems maintenance technician (AOC 353T) duties include the following:

- Manages intelligence EW equipment maintenance activities at organizational, direct support, and general support levels.
- Manages intelligence EW maintenance training program, the prescribed load list, repair parts stockpile levels, and the essential repair parts stockage list.
- Manages and supervises maintenance and supply personnel.
- Manages the equipment improvement report program and quality assurance program for the maintenance facility.
- Monitors the modification work order program and ensures the work is completed.
- Monitors maintenance requests and the maintenance request register for the maintenance facility.
- Monitors supply/parts requisitions and the document register.
- Maintains the updating of maintenance historical data records in the maintenance facility.
- Assists in the preparation of or prepares the material readiness report. These duties may be

assigned to the contracting officer representative or assistant contracting officer representative for the maintenance facility.

## ENLISTED MILITARY OCCUPATIONAL SPECIALTIES

**G-16.** Intelligence analyst (MOS 35F) duties include the following:
- Prepares all-source intelligence products to support commanders.
- Assists in establishing and maintaining systematic, cross-referenced intelligence records and files.
- Receives and processes incoming reports and messages.
- Assists in determining the significance and reliability of incoming information.
- Assists in the analysis and evaluation of intelligence holdings to determine changes in threat capabilities, vulnerabilities, and probable COAs.
- Assembles and proofreads intelligence reports and assists in consolidating them into Army intelligence.
- Stores and retrieves intelligence data using computers.

**G-17.** CI agent (MOS 35L) duties include the following:
- Provides CI services and support to force protection operations at all echelons.
- Performs CI support to counterterrorism operations.
- Prepares and operates recording and photographic equipment.
- Processes CI evidence and evaluates sources of information.
- Prepares and disseminates CI reports.
- Assists in nontechnical surveillance.
- Collects and compiles open-source material of CI interest.
- Conducts liaison with U.S. agencies.
- Maintains CI files and databases.

**G-18.** HUMINT collector (MOS 35M) duties include the following:
- Assists in the screening of HUMINT sources and documents.
- Conducts debriefings and interrogations of HUMINT sources in English and foreign languages.
- Translates written foreign material and captured documents into English.
- Prepares and edits appropriate intelligence and administrative reports.
- Utilizes CI and HUMINT reporting and communications equipment.
- Conducts MSO as appropriate.

**G-19.** Imagery analyst (MOS 35G) duties include the following:
- Identifies, analyzes, and reports on targets observed on imagery from satellite and airborne systems.
- Produces GEOINT supporting operations by analyzing still and motion imagery and geospatial data.
- Plans and recommends the use of imaging sensors for ISR missions.
- Identifies conventional and unconventional activity, installations, facilities, weapons systems, order of battle, military equipment, and defenses.
- Determines target coordinates for accurate location of imagery analysis findings.
- Identifies and analyzes military installations and lines of communications.

**G-20.** Common ground station (CGS) operator duties (MOS 35H) include the following:
- Deploys and redeploys the CGS in a tactical environment.
- Analyzes moving target indicator (MTI), synthetic aperture radar (SAR), radar, infrared, and visible imagery.
- Drafts and disseminates intelligence reports in support of Soldiers' requirements and to cue other

intelligence collectors or consumers.
- Correlates intelligence obtained from other sources.
- Analyzes and correlates the Joint Surveillance Target Attack Radar System (JSTARS) near real-time radar imagery data, SIGINT data, and the Secondary Imagery Dissemination System (SIDS) products.
- Performs maintenance on the prime mover and the CGS mission equipment.

**G-21.** SIGINT analyst (MOS 35N) duties include the following:
- Analyzes foreign communications intercepts and isolates intelligence information.
- Studies radio signals to understand the tactics and organization of foreign military forces.
- Locates the sources of foreign radio signals.
- Maintains databases and prepares intelligence reports based on signals intercepts.
- Keeps logs of signals interceptions.

**G-22.** Cryptologic linguist (MOS 35P) duties include the following:
- Translates, transcribes, or produces summaries of foreign language transmissions in English or target languages.
- Identifies languages spoken in an assigned geographic area.
- Scans written foreign language material for key words and indicators.
- Provides records of foreign intercepted communications.
- Operates communications equipment for SIGINT tasking, reporting, and coordination.
- Translates written and spoken foreign language material to and from English, making sure to preserve the original meaning.
- Records foreign radio transmissions using sensitive communication equipment.
- Translates foreign books and articles describing foreign equipment and construction techniques.

**G-23.** Signals collector/analyst (MOS 35S) duties include the following:
- Deploys, installs, and operates ELINT collection systems.
- Searches the radio frequency spectrum to collect, identify, and record target communications and selected categories or classes of electro-optic or foreign instrumentation signals.
- Operates communications equipment for SIGINT reporting and coordination.
- Performs basic signals analysis to determine signal parameters for identification and processing.
- Operates SIGINT equipment and prepares logs and technical reports.

**G-24.** MI systems maintainer/integrator duties (MOS 35T) include the following:
- Maintains, tests, and repairs communications equipment.
- Installs and repairs circuits and wiring.
- Calibrates and aligns equipment components.
- Strings overhead communications and electric cables between utility poles.
- Prepares maintenance forms and records.
- Works with oscilloscopes, signal generators, spectrum analyzers, and wire diagrams.

**G-25.** Interpreter/translator (MOS 9L) duties include the following:
- Prepares nontechnical translations into the target language and performs on-site translations from a target language into English.
- Performs oral interpretation functions.
- Assists a military contracting officer with local purchases and provides interpretation support at military traffic control points.
- May assist security personnel in screening the local population at military checkpoints.
- Other duties may include providing interpretation assistance for the public affairs office during local media events and translation of local newspapers or pamphlets.

# Appendix H

# Intelligence-Related Contact Information

## INTRODUCTION

**H-1.** This appendix contains contact information for some of the topics covered in this reference guide. Many of the links are for Web sites accessed with an Army Knowledge Online user name and password or common access card.

## U.S. ARMY INTELLIGENCE CENTER OF EXCELLENCE

**H-2.** https://icon.army.mil/APPS/IKN_WEBSITE/INDEX.CFM?ORGANIZATION=g3#.

## OFFICE OF THE CHIEF, MILITARY INTELLIGENCE (MI)

**H-3.** https://icon.army.mil/anon/ikn_website/index.cfm?organization=gomi#
ocmi@conus.army.mil.

## TRAINING

### 111th MI Brigade (Fort Huachuca, Arizona)

**H-4.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=111th%20mi%20bde#.

### 304th MI Battalion

**H-5.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=304th%20mi%20bn#.

### 305th MI Battalion

**H-6.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=305th%20mi%20battalion#.

### 309th MI Battalion

**H-7.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=309th%20mi%20battalion#.

### 344th MI Battalion (Goodfellow Air Force Base, Texas)

**H-8.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=344th%20mi%20bn#.

### Noncommissioned Officer's Academy

**H-9.** https://icon.army.mil/APPS/IKN_WEBSITE/INDEX.CFM?ORGANIZATION=ncoa#.

## JOINT INTELLIGENCE COMBAT TRAINING CENTER

**H-10.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=jictc#.

## FORT HUACHUCA RESERVE FORCES OFFICE

**H-11.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=rfo#.

## U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

**H-12.** INSCOM Training and Doctrine Support (ITRADS) Detachment
https://icon.army.mil/apps/ikn_website/index.cfm?organization=itrads#.

**H-13.** FOUNDRY
https://icon.army.mil/cfportal/sectors/news/trainingtoolkit/projectfoundry/projectfoundry.htm.

## LANGUAGE TRAINING

**H-14.** The Defense Language Institute Foreign Language Center
http://www.dliflc.edu/index.html.

**H-15.** 229th MI Battalion (Monterrey, California)
https://icon.army.mil/apps/ikn_website/index.cfm?organization=229th%20mi%20bn#.

**H-16.** Rosetta Stone
http://usarmy.rosettastone.com/.

## DISTRIBUTED COMMON GROUND SYSTEM-ARMY

**H-17.** https://icon.army.mil/apps/ikn_website/index.cfm?organization=dcgs#.

## HUMAN INTELLIGENCE TRAINING-JOINT CENTER OF EXCELLENCE (FORT HUACHUCA, ARIZONA)

**H-18.** http://www.us.army.mil/suite/page/612679.

# Appendix I

# Handheld, Manned, and Unmanned Collection and Sensor Systems

## INTRODUCTION

**I-1.** Collection and sensor systems gather information that is processed into intelligence. A collection asset or sensor is a system, platform, or capability that is supporting, assigned, or attached to a particular commander.

**I-2.** This appendix provides details of collection and sensor systems and capabilities in the following categories: unattended ground sensors, handheld collection systems, manned ground collection systems, unmanned aircraft systems, manned aircraft systems, airborne moving target indicator (MTI) systems, and electronic support systems. The systems discussed are annotated with their appropriate status in the acquisition process—quick reaction capability, developmental, prototype, or program of record.

## UNATTENDED GROUND SENSORS (UGS)

Figure I-1. OmniSense unattended ground sensor.

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**OmniSense.
**FUNCTION—**Electro-optical (EO)/Infra-red (IR) cameras and activity-cueing sensors (acoustic, magnetic, and seismic).
**DESCRIPTION—**Integrated system of hand-emplaced, unattended ground sensors, imagery devices, and satellite communications terminal. OmniSense was the first of the new generation of ground imagers with cueing sensors. It set the standard for PED in sanctuary. OmniSense established a near real time (NRT) viewing of the product within the area of operational responsibility (AOR). It is a fully capable player in a layered approach (short range). It has combat proven modalities. It leverages reach analysts for long term/trend products & dissemination. It has low power utilization with extended life beyond 90 days. It uses satellite communications (SATCOM) based communications. Reach, persistence, and agility enable unattended surveillance of a variety of locations beyond the area of operations or in unassigned areas. Beyond line-of-sight (BLOS) communications enable sensors to interact over a wide area network that provides dispersed forces with the timely, relevant, and accurate fused data. Access to common data enables joint, interagency, intergovernmental, and multinational (JIIM) users to construct a tailorable, relevant picture of the operational environment that facilitates situational awareness and decisive action. Mapping functions embedded in SADU software display locations of systems. Future integration in Distributed Common Ground Station-Army (DCGS-A) includes OPUS software for mission planning. Meets overhead imagery requirements in OIF/OEF for emplacement and recovery mission planning purposes.
**SYSTEM SELECTION CRITERIA—**Short range EO/IR cameras are easily concealed, and effective to approximately 200 meters. Best used when imagery is required, but terrain and foliage considerations dictate emplacement within 200 meters of the named area of interest (NAI).
**BASIS OF ISSUE—**Theater-provided equipment.
**STATUS—**

Figure I-2. Scorpion unattended ground sensor.

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Scorpion.
**FUNCTION—**EO/IR cameras and activity-cueing sensors (acoustic, magnetic, passive IR, and seismic).
**DESCRIPTION:** A ground imager with cueing sensors. It supports the community standard for PED in sanctuary. It supports NRT viewing of product within the AOR. It is a fully capable player in layered approach (mid to long range). Scorpion has combat proven modalities. It leverages reach analysts for long term/trend products and dissemination. It has low power utilization with extended life beyond 90 days. It uses SATCOM-based communications. Reach, persistence, and agility enable unattended surveillance of a variety of locations beyond the area of operations or in unassigned areas. BLOS communications enable sensors to interact over a wide area network that provides dispersed forces with the timely, relevant, and accurate fused data. Access to common data enables JIIM users to construct tailorable, relevant picture of the operational environment that facilitates situational awareness and decisive action.
**SYSTEM SELECTION CRITERIA—**Long range EO/IR cameras are more difficult to conceal, but are effective to approximately 800 meters. Best used when imagery is required, and terrain considerations allow stand off from the NAI.
**BASIS OF ISSUE—**Theater-provided equipment.
**STATUS—**

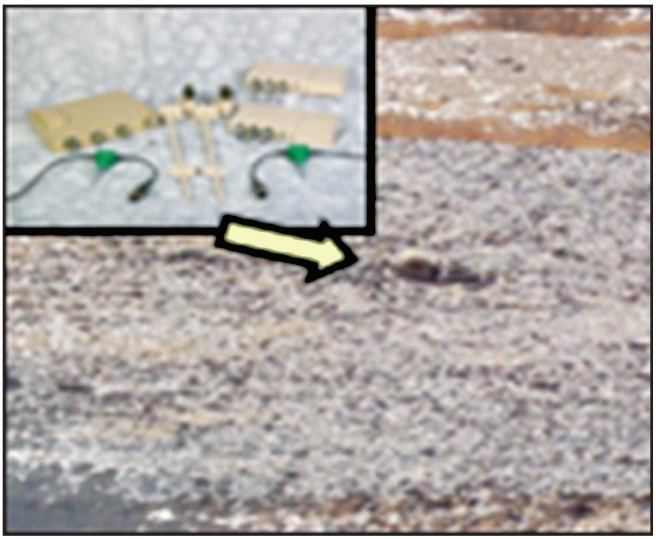


Figure I-3. SilentWatch unattended ground sensor.

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**SilentWatch.
**FUNCTION—**Activity sensors (passive infrared & seismic).
**DESCRIPTION:** Part of the new generation of ground sensors. It supports the community standard for PED in sanctuary. It supports NRT notification of product within AOR. It is a fully capable player in layered approach (activity and cueing). Combat proven modalities. Leverages reach analysts for long term and trend products and dissemination. Uses a qualification, filtered and unfiltered mode to minimize false alarms SATCOM-based communications. Reach, persistence, and agility enable unattended surveillance of a variety of locations beyond the area of operations or in unassigned areas. BLOS communications enable sensors to interact over a wide area network that provides dispersed forces with timely, relevant, and accurate fused data. Access to common data enables Joint, interagency, Intergovernmental, and Multinational (JIIM) users to construct tailorable, relevant picture of the operational environment that facilitates situational awareness and decisive action.
**SYSTEM SELECTION CRITERIA—**This system is more power-efficient than comparable systems, allows longer deployments, and is capable of being buried almost completely, allowing excellent concealment. Best used when imagery is not required and greater concealment and duration are desired.
**BASIS OF ISSUE—**Theater-provided equipment.
**STATUS—**

Figure I-4. Expendable unattended ground sensor.

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Expendable UGS (E-UGS).
**FUNCTION—**Seismic sensor.
**DESCRIPTION—**Hand-emplaced seismic-only sensor. Detects and classifies personnel or vehicle. It protects the force in counterinsurgency operations by providing route monitoring and early warning capabilities. Complements existing ISR capabilities, augmenting higher-fidelity systems with numerous sensor points of presence. E-UGS provides sufficient data to establish traffic patterns and movement trends. Minimal training required. Establishes a NRT (< 4 seconds) visualization of detections within the AOR. E-UGS provides unattended monitoring of a variety of locations beyond the area of operations or in unassigned areas. LOS communications enable sensors to interact over a wide area network that provides forces with the timely, relevant, and accurate detection. Supports the commander's ability to anticipate and react to a wide range of protection threats and situations. Small (2.6" diameter X 2.2" height) and light weight (8.5 oz per sensor), E-UGS operates on batteries. Battery life is two to four months. LOS radio range is 2-60KM. Low cost.
**SYSTEM SELECTION CRITERIA—**Seismic-only sensors are low-fidelity, very small, easily emplaced, and report to a stand-alone laptop. This system is best used within range of a fixed location to provide cueing and early-warning.
**BASIS OF ISSUE—**Theater-provided equipment.
**STATUS—**

Figure I-5. RF-5408 Falcon Watch remote imager.

**NOMENCLATURE—**RF-5408.
**PROJECT NAME—**Falcon Watch.
**FUNCTION—**IR and daylight images (paired with SilentWatch).
**DESCRIPTION—**Remote Intrusion Detection and Surveillance System, RF-5408, remote imager, mid-range dual IR and visible imager. Falcon Watch systems are wireless sensors, remote, battery-operated products that provide operators with critical surveillance data on a 24 hour basis. The Falcon Watch remote surveillance system is fully integrated with FALCON II radios and is ideal for monitoring high-value assets. No predeployment or deployment configuration required. It is easy to aim and focus. Existing SilentWatch sensors can be used as cueing devices. It can capture vehicles at 400 meters (800 meters day time) and personnel at 200 meters (400 meters day time). Falcon Watch provides advanced image capturing. It provides automatic target tracking, processes, and tracks targets through the field of view. Both IR and daylight images are captured for more accurate analysis. It has efficient transmission of images. Its power-efficient architecture extends battery life. It is designed to minimize false alarms by filtering out naturally occurring phenomena. It has a removable electric viewfinder (sighted through the IR imager) aligned from the factory. It is a plug and play operation into the Harris Intelligent Gateway. Only one imager unit to carry, emplace, aim, and camouflage. It is small (7.5”L x 8.0”W x 4.5” H) and lightweight (~5 lbs).
**SYSTEM SELECTION CRITERIA—**The mid range, medium-sized EO/IR imagers can be employed against targets at ranges up to 800 meters (day) or 400 meters (night.) Best used when imagery is required, and terrain considerations dictate emplacement between 200-400 meters from the NAI.
**BASIS OF ISSUE—**Theater-provided equipment.
**STATUS—**

SYSTEM SUMMARY

FEATURES—

- Unattended sensors.
- Acoustic mortar detection system that detects points of origin and points of impact by triangulating the lines of bearing developed by each UTAMS array.
- Detect pin-point improvised explosive device explosions and small arms and rocket propelled-grenade fires.

**Figure I-6. Unattended transient acoustic MASINT sensor (UTAMS).**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Unattended transient acoustic MASINT sensor (UTAMS).
**FUNCTION—**UTAMS is an acoustic localization system based on classic sound-ranging principles with advanced and unique signal processing techniques. It can detect and isolate transient events such as mortar or rocket firings, munitions impacts, and other explosive events.
**DESCRIPTION—**UTAMS comprises two to four sensor arrays linked via radio to a base station. The system provides line of bearing (LOB) from each array on the base station's map display. Each sensor station comprises a four-microphone acoustic array, Global Positioning System (GPS) antenna, radio with antenna, humidity sensor, signal processing box, and power box. The base station comprises a laptop, radio, and antennas. Configuration of UTAMS is three to five sensor arrays linked via radio to a base station.
**CAPABILITIES—**

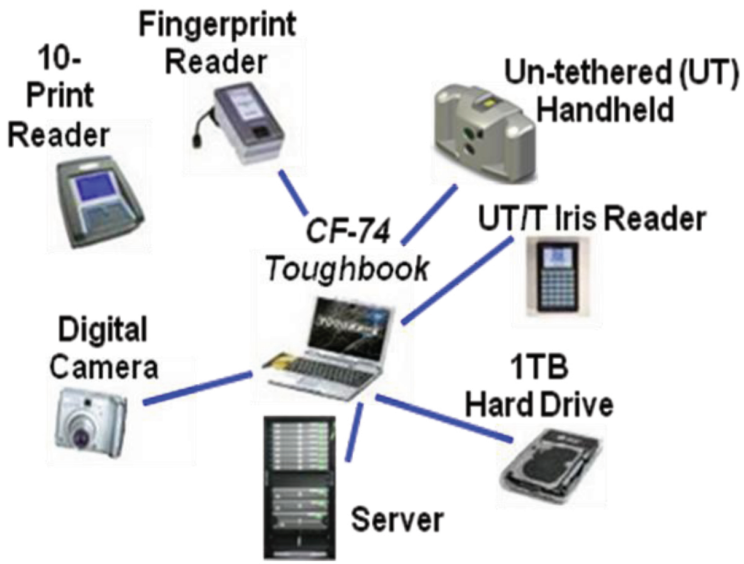
- Each array consists of a tripod, four acoustic microphones, a GPS antenna, a temperature sensor and an electronics unit. Once the arrays are set up, the microphone with north-seeking arrow on each array is aligned either at true north or at a known distant aiming point. Although its main use is for acquiring indirect fires, it also can pinpoint improvised explosive device (IED) explosions and small arms and rocket-propelled grenade (RPG) fires. The UTAMS has detected points of origin up to 10 km out.
- Provides LOB from each array on the map display of the base station.
- In its current configuration, each of the UTAMS acoustic sensor arrays independently processes the detected events based on statistics from the signal content against the background noise, computes LOB to the firing locations, and sends the LOB information to a central base station laptop computer via a radio frequency (RF) radio link. The base station performs source localizations via correlation and triangulation techniques. Due to the short and accelerated schedule, only a crude transient classifier was implemented in UTAMS. The Army Research

Laboratory is currently developing a more robust classifier that further differentiates between mortar, rocket, RPG, and small arms fire events.

**OPERATING ENVIRONMENT—**UTAMS continues to support both OIF and OEF, outperforming the AN/TPQ-36 (Fire Finder radar system) in tracking mortar and RPG events to points of origin. The system is also used effectively to track other events (for example, gunfire or IED), often locating these events before reports are received from troops on the ground. UTAMS is being tested as a payload for the persistent threat detection system, and has been designated a complementary cueing device by counter-rocket, artillery, and mortar (C-RAM). The system is being spiraled as a part of the C-RAM comprehensive force protection initiative.

**OPERATOR/MANTAINER—**Not MOS-specific; specialized training required; field service representative.

**STATUS—**UTAMS' status as a quick response capability (QRC) program will terminate at the conclusion of OIF and OEF.




SYSTEM SUMMARY

FEATURES—

- Collects, stores, and matches biometric data to satisfy stakeholders' requirements in friendly, threat, and neutral domains.
- Multi-modal biometric capability for fingerprints, iris images, facial photos, contextual and biographic data.
- Ruggedized laptop with biometric enabling software suite.
- Peripherals resist weather, heat, cold, dust; adaptable to most environmental conditions.
- Identifies, enrolls, and tracks persons of interest.
- Handheld device used as an untethered component of capability and database for tactical, squad level, operations.
- GPS connectivity capable.
- Lightweight, sustainable; man-portable, self-contained equipment packaging.
- Low power consumption; AC 110/220 volt; can operate up to four hours on laptop battery.
- Badge and identification badge printer capability.
- Assigns a geographic unique identification number to each dossier or record.
- Iris image reader may operate in tethered or untethered modes.
- Digital camera used in the tethered or untethered mode to record facial images, body images, evidentiary photographs of persons, scenes, or materials for attachments to records or dossiers.
- Optical or capacitive fingerprint readers for single, slap, multi-print capture, or rolled fingerprint image capture.
- Lightweight, sustainable.
- Adaptable to most environmental conditions.

Figure I-7. Biometrics Automated Toolset—Army.

**NOMENCLATURE—**None designated.
**PROJECT NAME—**Biometrics Automated Toolset-Army (BAT-A).
**FUNCTION—**The Biometrics Automated Toolset–Army's primary function is to ascertain and establish the identities of individual against claimed identities. The BAT-A capability provides the force the ability to make rapid hold, detain, or release decisions for persons of interest encountered on

the battlefield. It matches encountered individuals to identified individuals with known or suspected involvement with terrorism, criminal activity, or other persons of national security interest. The BAT-A can provide positive identification of local nationals and locally-employed persons requesting base access. It can be used as a means of verification of privileges for individuals requesting services.
**DESCRIPTION—**The BAT-A capability consists of four basic components—A BAT-A laptop and peripheral biometric collection hardware, the handheld device, the server, and the software. The laptop and peripheral hardware collect and store biometric information and can match biometric records to a record in its stored data. Peripheral hardware may consist of optical fingerprint readers, iris scanners, digital cameras, tripods, badge printers, barcode scanners, signature pads, port replicators, and external hard drives. The BAT-A includes a software suite resident on a ruggedized, Windows-based, laptop computer. Allows U.S. Forces and their allies to identify personnel, thus increasing the automation and reliability of HUMINT reporting, and enabling cross functional analysis with information from other intelligence and non-intelligence domains. It enhances the Army's ability to establish and maintain identity superiority by establishing the true identity of an individual and a knowledge base associated with that identity. The BAT-A can be used across the force to strengthen and improve physical security, access control, force protection, and the following operational missions:

- Identify an individual during tactical operations. Users can rapidly determine whether to detain or release an individual who is encountered during an operation.
- Conduct military operations among indigenous populations. Users can identify and manage indigenous populations during operations, including local foreign national employees and those needing humanitarian assistance.
- Track a person of interest (POI). Users can identify a POI and log the location(s) where biometrics data were collected from an individual in order to track a subject's movements.
- Conduct detention operations. Users can identify and track detainees from capture to release. Users can associate detention information, including interrogation reports, to a detainee's biometric file.
- Control or authorize physical access (entry control point). Users can authorize individuals to receive access and subsequently verify, for each request, the identity and authorization of those attempting to gain access.
- Protect/secure operationally critical installations and systems (access control point). Users can control access to military facilities and bases by using biometrics to authenticate identity.
- Match forensic evidence. Users can conduct biometric matching from forensic evidence.
- Conduct watch list operations. Users can create and disseminate regional and national level biometrically-based watch lists.
- Share identity information across the netcentric environment. Share identity information with U.S. government agencies, allies, and other partners or communities of interest.

In peacetime, the BAT-A can be used for training, intelligence support, and supporting real-world stability operations.
**POWER SOURCE—**Multisource— can be configured to use AC 110/220 volt, battery, or vehicle conversion kit power. Rechargeable batteries can be used on the laptop, untethered handheld collection device, and the iris image capture device. Digital cameras can use AC 100v or can use rechargeable or disposable AA batteries. The optical fingerprint sensors vary from USB powered to AC 110v power.
**OPERATOR/MANTAINER—**Not MOS specific, but specialized training is required. Field service representative (FSR) training required for server and equipment support.
**REFERENCES—**BAT-A capability production document, BAT-A training needs analysis, BAT STRAP, BAT-A training circular.
**STATUS—**

SYSTEM SUMMARY

FEATURES—
- Includes a camera for site documentation and LP photography.
- Includes a Metal-TEC 1400 that silently detects metal objects to include SIMM cards.
- Bag and Tag items for preservation and transfer of material off-site.
- Includes light sources for oblique lighting of biological stains, LPs, blood, hair, fibers, and chemicals.

**Figure I-8. Latent print collection kit.**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Not applicable.
**FUNCTION—**Provides the tools needed to process and lift latent fingerprints (LPs) on different textures—both porous and non-porous surfaces.
**DESCRIPTION—**

- Condor deployment bag
- 2 oz Black Fluor Powder
- 1 oz Black Fluor Magnetic Powder
- Tactical fiberglass fingerprint brush
- Regular magnetic applicator
- 2" clear fingerprint lifting tape
- Latent printed backing cards
- White 6" photographic scale
- White 2cm adhesive photographic scales
- FBI/CJIS Arrest and Institution Fingerprint Cards CRIMINAL
- Postmortem fingerprinting strips
- Postmortem fingerprinting strip holder—metal spoon
- Material field collection bags—SNG 9" x 12"
- Material field collection bags—SNG 12" x 16"
- Black Magic ceramic sm retg
- Black Magic ceramic lg retg
- X-large black nitrile gloves
- Sterile water ampoules
- DNA buccal Integriswab—sterile, 100/per pack
- Mini evidence envelope self-seal SNG 4" x 6"
- Canon Powershot D10—4X Zoom, 12 Megapixels
- SanDisk 2G memory card
- 12' metal measuring tape—substitute 16'
- Disposable tweezers

**CAPABILITIES—**

- Latent fingerprint collection.
- Post-mortem print collection.
- Live print collection.
- Capture latent on camera.
- Collect latent DNA.
- Collect forensic materials.

**POWER SOURCE—**Not required.
**OPERATOR/MANTAINER—**Not MOS specific; specialized training required; FSR.
**STATUS—**

SYSTEM SUMMARY

FEATURES—
- Provides the tools needed to process and lift LPs on different textures–both porous and non-porous surfaces.
- Includes a camera for site documentation and LP photography.
- Bag and tag items for preservation and transfer of material off-site.

**Figure I-9. Weapons intelligence team CSI bag**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Not applicable.
**FUNCTION—**Collect latent fingerprint and forensic materials, including post mortem collection.
**DESCRIPTION—**The CSI bag contains the following:

- ACU pattern bag.
- Fingerprint and information cards (big).
- Evidence bags.
- Fingerprint cards (small).
- Reversible latent print backing cards
- Semi-inkless fingerprint pad (2.25" X 1.75" X 0.5").
- Semi-inkless fingerprint pad (5" X 2.5").
- Adhesive-backed photo scales.
- Post-mortem card holder.
- Hinged print lifters (white backing cards—2" X 4").
- Silver/black dual-purpose latent print powder.
- Transparent latent print lifting tape in tube.
- Camera for site documentation and LP photography.
- Bag and tag items for preservation and transfer of material off-site.
- Straight black & white ruler.
- Pair of gloves.
- Whisper latent print brush.
- Tape measure.
- Twin Tip Sharpie.
- Reversible L-shaped Black & White.
- Ruler, reversible.

**CAPABILITIES—**Collect latent fingerprints; photograph latent fingerprints; collect post mortem fingerprints, and collect forensic materials.
**OPERATOR/MANTAINER—**Not MOS specific; specialized training required; FSR.
**STATUS—**



SYSTEM SUMMARY

FEATURES—

- Process takes less than 90 seconds
- Uniquely identified by barcode
- Can be used on all surfaces including human skin.

**Figure I-10. Explosives, chemical, toxins, narcotics trace detection kit**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Not applicable.
**FUNCTION—**Uses on-the-spot testing to detect the presence of trace forensic material of explosives and propellants, dangerous chemicals or toxins, and narcotics.
**DESCRIPTION—**This is a self-contained kit that is portable, disposable, low-cost, reliable, robust, and easy-to-use. The device is sensitive to a broad range of explosives, hazardous chemicals and toxins, and narcotics. It has built-in chemistry tests. The kit has hand-held chemical and biological agent sensors utilizing the latest technologies available including gas chromatography, spectroscopy and other spectral-scanning techniques. These sensors have novel algorithms embedded, so that the presence of individual agents can be detected quickly.
**CAPABILITIES—**The kit is capable of detecting all TNT explosives, PETN, RDX, HMX, inorganic explosives, gunshot residue, and is sensitive to anagram levels. Could be projected into an area.
**POWER SOURCE—**Not applicable.
**OPERATOR/MANTAINER—**Not MOS specific; specialized training required; FSR.
**STATUS—**


SYSTEM SUMMARY

FEATURES—

- Data Acquisition.
- Hard drives.
- CDs/DVDs/Floppies.
- Flash media.
- Cell phones/SIM cards.
- PDAs.
- Internationalized text / encoding schemes.
- Document / data format conversion.
- Graphic images.
- Known good/bad content identification.
- Rapid analysis.
- Steganalysis.

**Figure I-11. System for triaging key evidence (STRIKE)**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**STRIKE.
**FUNCTION—**To quickly assess whether digital media such as hard drives, CDs/DVDs/Floppies, flash media, cell phones/SIM cards, and PDAs contain tactical intelligence of benefit to the warfighter.
**DESCRIPTION—**STRIKE is a media exploitation device (MEDEX). It is portable, small (10.6”x 7.2”x 1.65”), light weight (3.7 lbs.), and easy to use. The basic device is an Itronix GoBook Tablet PC with a 933 MHz low voltage mobile Intel PIII CPU. It contains 640 MB of SDRAM with a shock-mounted 40 GB HDD. Communications are 10/100 MbitBase-T LAN GPRS/CDMA/EDGE/802.11b WLAN/ Bluetooth. The display is an 8.4”SVGA TFT outdoor transmissive display. The STRIKE provides the following interfaces: PC Card slot for one Type I or II card with 32 bit card bus 2.1 interface; a compact flash slot for one Type I or II card; two USB 2.0 connectors; and a connector for an expansion battery.
**CAPABILITIES—**STRIKE performs live media examinations and is a role-based system using advanced rules and automation.
**POWER SOURCE—**Smart 3600 mAH (40W) lithium-ion battery pack.
**OPERATOR/MANTAINER—**Not MOS specific; specialized training required; FSR.
**STATUS—**


Portable Barcode Scanner

Portable Biometrics

Internet Protocol (IP) Handheld Exploitation Device

SYSTEM SUMMARY

FEATURES—

- MEDEX tools—ENCASE, FTK, D2C, STRIKE, ADF, and others.
- DOCEX tools—DHDS T, DHDS CT, and DHDS.
- Site Scene—Documents, drawings, ID cards, blueprints, maps, and other printed media.
- PEDEX tools—Mobile Edit, CALYX, and others.
- Biometrics tools—HIIDE, BAT, and others.

- Quickly assess (within 30 min.) whether a media device has potential intelligence value based on the unit's PIR and assist the decisionmaker in determining whether to further exploit and confiscate the target device.
- Site or scene documentation tool.
- Mobile telephone forensics device.
- Portable biometrics device.

**Figure I-12. Tactical site exploitation toolkit (TSET)**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Not applicable.
**FUNCTION—**The Tactical Site Exploitation Toolkit (TSET) is a modular computer forensics front end tool designed to rapidly collect, sort, and disseminate collected data. The TSET is intended for use by both trained and untrained personnel at multiple echelons in support of a site exploitation mission. This mission includes media exploitation (MEDEX), Document Exploitation (DOCEX), personal

electronic device exploitation (PEDEX), site scene documentation and exploitation, and biometrics.
**DESCRIPTION—**The TSET must include a forensic software package that has the ability to compare electronic media against known target lists (PIR/IR). The software must also port the data hits into the target's native language and run a small PDA/OKO. The device shall have an Intel Duo Core 1.2 GHz Atom processor, up to 4GB memory, a WSVGA with passive touch screen display, a touch screen display and stylus user interface, rugged solid state drive storage, comply with MIL-STD-810F and IP-67, a Windows XP Professional operating system, wireless Bluetooth 2.0, be Wi-Fi b/g and 3G/4G capable, SATCOM capable, and contain a GPS. Three variants must be available—site or scene documentation tool, mobile telephone forensics device, and a portable biometrics device (optional).

- **Site or scene documentation tool.** This tool will provide a capability to document and capture site or scene data in any situation. The device must be ruggedized, and include integration of Bluetooth, 802.11, GPS, camera, barcode scanner, and USB and host and client ports as well as have a high resolution screen and a minimum and 806Mhz processor. The camera must have 9 million pixels and 3X Optical Zoom (up to 600 DPI), GPS position and track log, shock, dust and water resistance compliant with military specifications, a real-time MGRS Display, a barcode scanner, still mode, video mode, scene mode, sound mode, Bluetooth, and 802.11b/g—security-enabled WEP (64/128bit). An integral laser range finder must be Bluetooth enabled with a range of 0 to 1000m to an accuracy of +/- 1 ft at an inclination of +/- 90 degrees.
- **Mobile telephone forensics device.** The mobile telephone forensics device will provide a standalone field expedient capability to extract data from common models of telephones sold worldwide. The device must capture vital data such as phonebooks, pictures, videos, text messages, call logs, ESN, and IMEI information. The system must also support CDMA, GMS, IDEN, and TDMA communications technologies and be compatible with any wireless carrier.
- **Portable biometrics device (optional).** The portable biometrics device must provide a tactical extension to the BAT-A that can enroll, match or verify using three primary biometrics modalities—iris image, fingerprint and facial image. The device must operate independently from the host PC while deployed and include a state-of-the-art lens technology for both iris and facial image capture; the fingerprint capability must be compliant with IAFIS and have a capacity 500 DPI.

**CAPABILITIES—**Perform computer analysis in under 30 min; satisfy site or scene exploitation; be an IP-enabled personal electronic exploitation device; be inoperable with biometrics collection capability; and must be Wi-Fi, Bluetooth, 3G/4G capable.
**POWER SOURCE—**Not determined.
**OPERATOR/MANTAINER—**Not MOS specific; specialized training required; FSR.
**STATUS—**

## Manned Aircraft System

SYSTEM SUMMARY

Sensor Descriptions—

- MX-20 EO/IR sensor.

  - IR w/ high magnification 4-step zoom.
  - Color day camera w/ continuous zoom lens.
  - Night (mono) camera.
  - Laser illuminator.
  - Laser rangefinder.
- Multi-mode synthetic aperture radar/ ground moving target indicator (SAR/GMTI).
- COMINT.
- Onboard collection, analysis, sensor cross-cueing and real time dissemination.

Aircraft—DHC-7—

- Ceiling—20,000 ft. (MSL)
- Endurance—eight hrs.
- Loiter speed—140 knots.
- Gross wt.—47,000 lbs.
- Data link range—180 nautical miles (nm).
- Crew—two pilots, four operators.

**Figure I-13. RC-7B, Airborne Reconnaissance–Low (ARL)**



**NOMENCLATURE—**RC-7B, Airborne Reconnaissance–Low (ARL).
**PROJECT NAME—**RC-7B, (ARL).
**DESCRIPTION—**ARL improves commanders' situational awareness and contributes to their understanding of the environment by providing day and night, near all-weather, near real-time airborne communications and imagery intelligence collection and designated area surveillance.
**CAPABILITIES—**ARL provides the commander with a multi intelligence collection capability to accurately detect, identify, track, and report on targets of interest in near real time. The platform provides COMINT intercept, DF, and special signals exploitation capabilities. It finds, fixes, and identifies targets of interest, and provides actionable intelligence direct to BCT. It also provides full-motion video (FMV) feed to the tactical commander. It provides broad-area surveillance and focused stare on target areas of interest (AO)—both point and area targets. It is capable of tactical over-watch of ongoing operations, and provides real-time down-link of MTI data to the CGS at the BCT up to echelons above corps level. There are four mission workstations onboard.
**POWER SOURCE—**Aircraft-generated power.

**OPERATOR/MAINTAINER—**Pilots–15C/155E; operators/analysts—352N/352P/350G/35N/35P/35G/35H; maintainers—contractor.
**REFERENCE—**ARL Program Summary.
**STATUS—**Fielded.

SYSTEM SUMMARY

Sensor descriptions—

- PenRad 7 UHF-Band SAR

  - SAR resolution of 1 meter.
  - On-board image processing.
  - Nominal swath width of 3 km.
  - Side-look aperture (left/right/both).
- MX-15 EO/IR sensor.

  - IR w/ high magnification four-step zoom.
  - Color day camera w/ continuous zoom lens.
  - Night (mono) camera.
  - Laser illuminator.
  - Laser rangefinder.

Aircraft—King Air A200T (C-12 equivalent).

- Ceiling—31,000 ft. (MSL).
- Endurance—4.5 hrs.
- Loiter speed—160-180 knots.
- Data link range—100 nm.
- Crew—two pilots, two or three operators.

**Figure I-14. Desert Owl**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Desert Owl.
**FUNCTION—**The Desert Owl contractor-owned/contractor-operated (COCO) system provides tactical commanders data to conduct counter-improvised explosive device (C-IED) operations using coherent change detection (CCD).
**DESCRIPTION—**Desert Owl is an airborne ISR system that can simultaneously conduct measurement and signature intelligence (MASINT) and IMINT missions in near all-weather conditions. High-quality SAR imagery and CCD products are collected through a long-range UHF-SAR array. By conducting multiple flights over the same area, the software produces still images that indicate changes on the ground.

**CAPABILITIES—**This system provides the commander an intelligence collection capability to accurately detect, identify, and report changes in the environment. It provides the tactical commander with CCD to assist in CIED operations. Desert Owl provides FMV feeds in EO and IR modes to one system remote video terminal (OSRVT), the Desert Owl ground control station, or through the Task Force (TF) ODIN SIPR architecture. It provides laser illuminator and designator for precision targeting, and feeds the FBCB2 and BFT digital command and control system.
**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MANTAINER—**COCO.
**REFERENCE—**Desert Owl CONOP.
**STATUS—**Fielded as a QRC niche system currently deployed in the Central Command (CENTCOM) AO.

SYSTEM SUMMARY

Sensor descriptions—

- High resolution EO camera.
  - Capable of providing wide format EO-persistent, motion imagery (low frame-rate video).
  - Provides forensic C-IED/VBIED capability.
  - Camera field of collection is 6x6 km area.
  - Provides route mosaics.
  - Collected data processed post-mission.
  - Requires extensive analytical/ processing time.
  - Future systems will add wideband downlink, wider field of view, and night capabilities.

Aircraft—King Air A200T (C-12 equivalent) for OEF theater and the Sherpa/Shorts 360 aircraft for OIF AO.

- Ceiling—16,000 ft. (MSL).
- Endurance— 4.5 hrs.
- Loiter speed—180-220 knots.
- Data link range—Not applicable; must land to exploit data.
- Crew—two pilots, two or three operators.

**Figure I-15. Constant Hawk**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Constant Hawk.
**FUNCTION—**The Constant Hawk is a COCO, aerial ISR system that provides the tactical commander data needed to conduct high resolution imagery forensics to assist in CIED operations.
**DESCRIPTION—**The Constant Hawk is an airborne intelligence system that collects day-only motion imagery for use in forensic backtracking of enemy activity. The system conducts persistent area coverage and uses software to produce motion imagery. These products may be exploited for use in the CIED mission and other spectacular and complex enemy events or attacks.

**CAPABILITIES—**This system provides the commander with a single intelligence collection capability to accurately backtrack enemy events or attacks. The forensic analysis is conducted post-mission. It also provides actionable intelligence derived from vehicle backtracking of vehicle borne improvised explosive device (VBIED) events. The software orthorectifies and georectifies the imagery products for spatial accuracy.
**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MANTAINER—**COCO.
**REFERENCE—**TF ODIN CONOP.
**STATUS—**Fielded as a QRC niche system deployed in CENTCOM AO.

SYSTEM SUMMARY

Sensor descriptions—

- MX-15i EO/IR Sensor.

  - IR w/ high magnification, four-step zoom.
  - Color day camera w/ continuous zoom lens.
  - Night (mono) camera.
  - Laser illuminator.
  - Laser rangefinder.
- COMINT and ELINT intercept capability.
  - Provides DF.
  - Provides precision location.
  - Capable of special signals exploitation.
- Digital framing camera (PeARL).
  - Available on ARMS only in OIF.
  - Sensor consists of four 21 megapixel cameras producing one to eight images.
  - Rapidly provides geo-registered high-resolution color imagery of large areas.

Aircraft—

- ARMS—B-200.
- MARSS—11 aircraft are B-300 (King Air 300), 2 are DASH-7 aircraft, and 2 are B-200 aircraft.
- Ceiling—31,000 ft. (MSL).
- Endurance—5.5 hrs.
- Loiter speed—160-220 knots.
- Data link range—138 nm.
- Crew—2 pilots, 2 operators

**Figure I-16. Medium Altitude Reconnaissance and Surveillance System (MARSS), Airborne Reconnaissance Multi-sensor System (ARMS)**

**NOMENCLATURE—**Not applicable.

**PROJECT NAME—**Medium Altitude Reconnaissance and Surveillance System (MARSS) OEF/ Airborne Reconnaissance Multi-sensor System (ARMS) OIF.

**FUNCTION—**MARSS and ARMS are manned aerial collection systems that perform signals intercept, DF, and precision location, day and night full-motion video. ARMS provides wide area high-resolution still imagery.

**DESCRIPTION—**MARSS provides EO/IR (day/night) FMV to tactical commanders. ARMS can simultaneously conduct SIGINT collection and real-time electronic order of battle (EOB), provide

EO/IR FMV, and collect high-resolution color still imagery. The high-resolution imagery collected on ARMS is stored onboard the aircraft and disseminated and analyzed post-mission.
**CAPABILITIES—**These systems provide the commander with a multi-intelligence collection capability to accurately detect, identify, and report threat targets in near real-time.
**POWER SOURCE—**Aircraft.
OPERATOR/MAINTAINER—

- ARMS: Pilots—15C/155E or contractor-operated; operators—35N/35P or contractor; maintainers—35T or contractor.
- MARSS: Pilots—NG 15C/155E; Operators—35N/35P; Maintainers—35T or contractor.

**REFERENCE—**TF ODIN and ARMS CONOPS.
**STATUS—**Fielded as a QRC niche system deployed in the CENTCOM AO.

SYSTEM SUMMARY

Sensor description—

- SIGINT sensors:
  - Provide COMINT intercept, DF, and special signals exploitation.
  - Data are down linked to a ground station for processing.
- MX-15i EO/IR Sensor.

  - IR w/high magnification, four-step zoom.
  - Color day camera w/ continuous zoom lens.
  - Night (mono) camera.
  - Laser illuminator.
  - Laser rangefinder.

Aircraft—King Air A200T (C-12 equivalent).

- Ceiling—31,000 ft. (MSL).
- Endurance—4.5 hrs.
- Loiter speed—160-220 knots.
- Data link range—BLOS via Ku-Band SATCOM.
- Crew—two pilots, two or three operators.

**Figure I-17. Redridge II**

**NOMENCLATURE—**Not applicable.
**PROJEC NAME—**Redridge II.
**FUNCTION—**Redridge II is a manned SIGINT platform in OEF.
**DESCRIPTION—**The Redridge II QRC is an airborne intelligence collection system that conducts SIGINT and provides FMV.
**CAPABILITIES—**This system provides the commander with an intelligence collection capability that accurately detects, identifies, and reports signals of interest in near real time (NRT).
**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MAINTAINER—**Government owned and contractor operated (GOCO).
**REFERENCE—**Not available.
**STATUS—**Fielded as a QRC niche system deployed in the CENTCOM AO.

SYSTEM SUMMARY

Sensor description—

- High-resolution EO camera system.

  - 2.4-inch resolution from 15K AGL.
  - 10 meter location accuracy and automated, NRT data processing
  - Produces color or grayscale images, but grayscale is currently predominant due to processing times.
  - System can produce 3-D maps and images.

Aircraft—King Air A200T (C-12 equivalent).

- Ceiling—31,000 ft. (MSL).
- Endurance—4.5 hrs.
- Loiter speed—160-220 knots.
- Gross wt.—14,000 lbs.
- Data link range—BLOS via INMARSAT.
- Crew—two pilots, two or three operators.

**Figure I-18. Highlighter**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Highlighter.
**FUNCTION—**The Highlighter COCO system provides the tactical commander the data needed to conduct C-IED operations utilizing change detection. The system performs change detection in a rural to semi-urban environment during daylight hours.
**DESCRIPTION—**The Highlighter is an airborne intelligence system that can simultaneously conduct MASINT and IMINT missions. It is a daylight-only system consisting of a C-12 Aircraft with mission survivability equipment, three high-resolution EO cameras, and computer hardware and software with change detection algorithms. The change detection products provide the tactical commander with high-resolution imagery that is used to depict changes in their area of operation.
**CAPABILITIES—**Still images may be received via the One System Remote Video Terminal (OSRVT). It has an onboard analysis capability with dedicated in-flight operator. Video is disseminated

to ARST via Ku-band data link. Image products are disseminated to ARST via INMARSAT. All products are available via the TF ODIN SIPR architecture.
**POWER SOURCE—**Aircraft.
**OPERATOR/MANTAINER—**COCO.
**REFERENCE—**TF ODIN CONOP.
**STATUS—**Fielded as a QRC niche system deployed in CENTCOM AO.

Night Eagle

Change Detection Display

Night Activity Video

- SYSTEM SUMMARY

Sensor description--

- L-3 Sonoma EO/IR camera system.

  - High-resolution still imagery.
  - EO/IR FMV.
  - Provides a day and night change detection capability.

Aircraft—King Air A200T (C-12 equivalent).

- Ceiling—31,000 ft. (MSL).
- Endurance—5.5 hrs.
- Loiter speed—160-220 knots.
- Data link range—100 nm.
- Crew—two pilots, two operators.

**Figure I-19. Night Eagle**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Night Eagle.
**FUNCTION—**The Night Eagle COCO system provides the tactical commander data needed to conduct CIED operations with amplitude change detection.
**DESCRIPTION—**The Night Eagle is an airborne intelligence system that can simultaneously collect MASINT and IMINT data during ISR missions. High-quality night camera imagery and amplitude change detection products are collected through the electro-optical and infrared camera. The Night Eagle mission profile enables the aircraft to fly the area of interest with multiple looks to facilitate the amplitude change detection.
**CAPABILITIES—**This system provides the tactical commander with day or night change detection to assist in CIED operations and high resolution still-imagery products. EO/IR FMV may be disseminated to OSRVT users. Can target precisely using laser illuminator and designator. All products are available

via the TF ODIN SIPR architecture.
**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MANTAINER—**COCO.
**REFERENCE—**Not available.
**STATUS—**Fielded as a QRC niche system deployed in CENTCOM AO.

SYSTEM SUMMARY

Planned sensor payloads—

- COMINT and ELINT payload.
- EO/IR payload.
- Eye-safe laser rangefinder (ELRF).
- SAR/GMTI payload.

Planned aircraft—King Air B350ER (C-12 equivalent).

- Ceiling—31,000 ft. (MSL).
- Endurance—5.5 hrs.
- Loiter speed—160-220 knots.
- Data link range—BLOS for chat/SIGINT; 138 nm. for FMV.
- Crew—two pilots, two operators.

**Figure I-20. Enhanced-Medium Altitude Reconnaissance and Surveillance System (EMARSS)**

**NOMENCLATURE—**Not applicable.
**PROJEC NAME—**Enhanced-Medium Altitude Reconnaissance and Surveillance System (EMARSS)
**FUNCTION—**EMARSS provides a persistent capability to detect, locate, classify/identify, and track surface targets in day/night, near all-weather conditions with a high degree of timeliness and accuracy. EMARSS aircraft will be located within aerial exploitation battalions (AEBs), which are assigned to the U.S. Army Intelligence and Security Command (INSCOM).
**DESCRIPTION—**EMARSS is a manned, multi-intelligence airborne ISR (AISR) platform. It is designed to provide timely, accurate, assured support to tactical forces in full spectrum operations. The EO/IR payload provides FMV disseminated over a digital data link. The SIGINT payload provides detect, identify, geolocate, and copy with aerial precision guidance capability. The system includes an RC-12 aircraft as the prime mover. The system consists of two onboard sensors and provides cross-cueing intelligence collection of both onboard and off-board sensors.
**CAPABILITIES—**EO/IR, SAR/GMTI, and SIGINT payloads on each airframe provide multi-discipline collection and support. The SAR/GMTI capability provides deep look and advanced threat indication, warning, and adverse weather imaging.
**BATTERY SOURCE—**Aircraft-generated power.
**OPERATOR/MAINTAINER—**Pilots: 15C/155E; operators: 35N/35P/35T.
**REFERENCE—**DA G-3 Directive.
**STATUS—**Currently QRC; first unit equipped is planned for FY12.

SYSTEM SUMMARY

Sensor Descriptions—
- Communications intelligence (COMINT) payload collects, identifies, classifies, and locates radio frequency (RF) signals.
- Guardian Eagle (GE) QRC upgrade provides modern signals and special signals exploitation.
- Line-of-sight and BLOS communications for off-board analysis and reporting.

Aircraft—RC-12X with advanced avionics, GPS, inertial navigation, and color weather radar.
- Ceiling—35,000 ft. mean sea level (MSL).
- Endurance—5.5 hours.
- Loiter speed—210-220 knots.
- Gross wt.—16,200 lbs.
- Data link range—180 nm.
- Crew—2 pilots.

**Figure I-21. RC-12X, GUARDRAIL/Common Sensor (GRCS)**

**NOMENCLATURE—**RC-12X, GUARDRAIL/Common Sensor (GRCS).
**PROJECT NAME—**RC-12X, GRCS.
**FUNCTION—**The GRCS improves commanders' situational awareness and contributes to their understanding of the environment by providing COMINT and ELINT intercept, direction finding (DF), precision geolocation, and special signals exploitation.
**DESCRIPTION—**GRCS is a tactical airborne signals intelligence (SIGINT) collection and precision targeting system. The GRCS consists of seven RC-12X aircraft, a GUARDRAIL Ground Baseline (GGB) exploitation and dissemination center, and a mission operations center. The mission is usually conducted with up to three aircraft in a synchronized constellation to optimize coverage and location accuracies at altitudes up to 35,000 ft MSL for durations of up to five-and-a-half hours. GRCS is managed by the corps it supports, while tasking may include requests from brigade, theater, and national organizations. GRCS may be deployed within hours of being tasked with an urgent/ad hoc mission supporting dynamic tasking in flight. Specific modifications to the GRCS include—
- Enhanced split-based operations.
- Increased COMINT throughput and frequency range.
- Enhanced classification and recognition of modern signals.
- Improved precision emitter geolocation.
- Beyond line-of-sight relay for off-board analysis and reporting.
- Improved ground station, the GGB.

**CAPABILITIES—**GRCS provides the commander with a SIGINT collection capability to accurately detect, identify, track, and report high-value targets in near real-time.
- Detects, intercepts, geolocates, identifies, tracks, exploits and reports COMINT, ELINT, and special signals.




FOR OFFICIAL USE ONLY

- Precision geolocation of COMINT and special signals with rapid reporting to support time-sensitive targeting.
- Beyond line-of-sight processing reduces deployed footprint and sustainment requirements.
- Provides near-national level sensor capabilities tailored for the corps area of operation and threats.
- Reach back capabilities include comprehensive SIGINT analysis.
- The technology is leveraged in the development of the future aerial ISR constellation.

**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MAINTAINER—**Pilots: 15C/155E (Aviation All-source Intelligence Officer/C-12 Pilot warrant officer); Operators/Analysts: 352N/352P/35N/35P; Maintainers: 353T/35T/Contractor.
**REFERENCE—**GRCS Program Summary.
**STATUS—**The GGB has been fielded to all AEBs. The other preplanned product improvements are underway—first unit equipped is expected in 4Q FY10.

SYSTEM SUMMARY

| Payload descriptions— | Platform description— |
|---|---|
| • EO/IR camera.<br>• Optical bar camera.<br>• ASAR.<br>• SIGINT.<br>• Network-centric communication. | • Ceiling—70,000+ ft.<br>• Endurance—12 hours.<br>• Loiter speed—373 knots.<br>• Data link range—8-12 km.<br>• Crew—one air vehicle operator. |

**Figure I-22. U-2S High-altitude reconnaissance aircraft**

**NOMENCLATURE—**U-2S High-altitude reconnaissance aircraft.
**PROJECT NAME—**U-2S.
**FUNCTION—**The U-2 provides high-altitude, all-weather surveillance and reconnaissance, day or night, in direct support of U.S. and allied forces. It delivers critical imagery and signals intelligence to decisionmakers throughout all phases of conflict, including peacetime indications and warnings, low-intensity conflict, and large-scale hostilities.
**DESCRIPTION—**The U-2S is a single-seat, single-engine, high-altitude/near-space reconnaissance and surveillance aircraft providing SIGINT, IMINT, and MASINT. Long and narrow wings give the U-2 glider-like characteristics and allow it to quickly lift heavy sensor payloads to unmatched altitudes, keeping them there for extended periods of time. The aircraft has the following sensor packages: EO/IR camera, optical bar camera, ASAR, SIGINT, and network-centric communication.
**CAPABILITIES—**The U-2 is capable of gathering a variety of imagery, including multi-spectral electro-optic, infrared, and synthetic aperture radar products which can be stored or sent to ground exploitation centers. In addition, it also supports high-resolution, broad-area synoptic coverage provided by the optical bar camera producing traditional film products which are developed and analyzed after landing. All intelligence products, except wet film, can be transmitted in near real-time anywhere in the world via air-to-ground or air-to-satellite data links, rapidly providing critical information to combatant commanders. MASINT provides indications of recent activity in areas of interest and reveals efforts to conceal the placement or true nature of man-made objects.
**POWER SOURCE—**Internal to airframe.
**OPERATOR/MAINTAINER—**One pilot (USAF) from the assigned unit; 5 two-seat trainers and two ER-2s operated by NASA.
**REFERENCE—**U.S. Air Force Fact Sheet.
**STATUS—**Fielded.

# UNMANNED AIRCRAFT SYSTEMS

There are currently four unmanned aircraft systems (UAS) in widespread use by U.S. forces. The aircraft are capable of carrying different intelligence-relevant payloads. Table I-1 provides comparison data for the four UAS presented in this appendix.

**Table I-1. Unmanned aircraft systems comparison chart**

| Specifications/Capabilities | RQ-11B Raven | RQ-7B Shadow | MQ-5B Hunter | MQ-1C Gray Eagle |
|---|---|---|---|---|
| Level of Asset (i.e. BN, BDE, DIV, Corps) | CO / BN | BCT | Corps / DIV | DIV |
| Service Ceiling Altitude | 500 ft - AGL | 14k ft - MSL | 18k ft - MSL | 25k ft - MSL |
| Operational Altitude | 150 - 500 ft - AGL | 6k - 10k ft - AGL | 8k - 12k ft - AGL | 15-20k ft AGL |
| Dash Airspeed | 60 MPH | 110 KIAS | 110 KIAS | 185 KIAS |
| Cruise Airspeed | 40 MPH | 65 - 70 KIAS | 60 - 80 KIAS | 60 - 75 KIAS |
| Max Range (KM) | 8 - 12 KM | 125 KM | 300 KM (Relay) | 300 KM (T) / 500 KM (O) |
| Operational Range (KM) | 3 - 8 KM | 50 KM | 125 KM | 300 KM (T) |
| Max Endurance Time (Hrs) | 1 - 1.5 Hrs | 5 Hrs | 16 - 18 Hrs | 24+ |
| Loiter Time over Target @ Range | .5 - 1 Hrs | 5 Hrs @ 50 KM | 10 - 12 Hrs | 12 Hrs (T) / 24 Hrs (O) |
| Amount of Continuous Coverage Time | Continuous | 20 Hrs / 24 Hr Period | 24 Hrs / 24 Hr Period | 24 Hrs Coverage |
| Threshold Payloads | EO or IR | EO/IR | EO/IR | EO/IR w/LRF/LD |
| | | | Greendart | SAR/MTI (when available) |
| | | | | SIGINT (when available) |
| | | | | WCP (when available) |
| | | | | Weapons (HELLFIRE) |
| Objective Payloads | | SAR/MTI | CRP | HS/US |
| | | CRP-Light | Viper Strike | MET |
| | | HS/US | TSP | SIGINT/EA |
| | | MET | | ASTAMIDS |
| | | SIGINT/EA | | NBC Detection |
| | | ASTAMIDS | | Surety Material Sampling |
| | | NBC Detection | | LIDAR |
| | | Surety Material Sampling | | PSYOPS LRBS |
| | | LIDAR | | |
| | | PSYOPS | | |

SYSTEM SUMMARY

| Payload description— | Platform description— |
|---|---|
| • Primary payload is the EO or IR sensor.<br>• EO and IR payloads are non-gimbaled.<br>• EO payload—Front and side looking.<br>• IR payload—Front or side looking; laser illuminator. | • Ceiling—1000 ft. (MSL).<br>• Endurance—60-90 minutes.<br>• Loiter speed—40 knots.<br>• Data link range—8-12 km.<br>• Crew—one air vehicle operator. |

**Figure I-23. RQ-11B, Raven Small Unmanned Aircraft System (SUAS)**

**NOMENCLATURE—**RQ-11B, Raven Small Unmanned Aircraft System (SUAS).
**PROJECT NAME—**Raven SUAS.
**FUNCTION—**The RQ-11B Raven SUAS provides the small unit with an organic capability to perform "over the next hill" reconnaissance, surveillance, and target acquisition (RSTA).
**DESCRIPTION—**The RQ-11B Raven SUAS is a hand launched, auto land or manual recovery system. It incorporates an auto-navigation feature using military P(y)-code GPS. The system can be flown actively or through set waypoints with options of either an EO or IR camera allowing both day and night operations. The aircraft allows rapid to assembly (< 3 minutes) and is man portable and back packable. The RQ-11B Raven SUAS consists of one ground control station, three aircraft with payloads, lithium ion batteries with rechargers, and spare parts.
**CAPABILITIES—**The RQ-11B Raven SUAS provides reconnaissance and surveillance (R&S), as well as remote monitoring, with day and night imagery The RQ-11B Raven SUAS operates at the company level while performing R&S missions, convoy security to protect friendly forces, and/or real time BDA.
**POWER SOURCE—**Airframe and ground control station both use lithium ion batteries.
**OPERATOR/MAINTAINER—**Two operators from the assigned unit—not MOS specific.
**REFERENCE—**Rucksack Portable UAV ORD submitted by Special Operations Command (SOCOM).
**STATUS—**Over 1000 systems fielded.


SYSTEM SUMMARY

Payload description—-

- Primary payload is the POP 300 (EO/IR).

  - Color EO.
  - Laser target marker and illuminator, or laser designator and rangefinder.
- May employ communications relay payload-light (CRP-L).

Platform description—

- Ceiling—15,000 ft. (MSL).
- Endurance—5+ hrs.
- Loiter speed—80 knots.
- Data link range—67 nm.
- Crew—one air vehicle operator, one payload operator.

**Figure I-24. RQ-7B, Shadow Tactical UAS (TUAS)**

**NOMENCLATURE—**RQ-7B, Shadow Tactical UAS (TUAS).
**PROJECT NAME—**Shadow TUAS.
**FUNCTION—**The RQ-7B Shadow TUAS is an airborne intelligence, surveillance, and reconnaissance (AISR) capability to provide BCT-level commanders with a persistent capability to detect, locate, identify, and track surface targets in day and night conditions with a high degree of timeliness and accuracy.
**DESCRIPTION—**RQ-7B Shadow TUAS conducts battlefield surveillance using its multimission optronic payload. The payload broadcasts its data to mission monitoring stations and OSRVTs. The RQ-7B Shadow TUAS consists of launch and recovery equipment; two ground control stations; remote video terminals; and four aircraft with payloads.
**CAPABILITIES—**The RQ-7B Shadow TUAS is capable of performing focused operations in a brigade's operational environment and covers the dead space by extending the ground reconnaissance capability. The RQ-7B Shadow TUAS, including its POP 300 EO/IR payload data, is interoperable with other C4ISR systems. The POP 300 EO/IR payload provides a multi-mode payload with resolution sufficient to detect and recognize light pick-up truck-sized targets from operational altitudes and survivable standoff ranges (~3km to 5km) from the imaged target. It has a laser target marker and illuminator and a laser designator and range finder. It gathers ISR and battle damage information in real time, then relays it via video link to commanders and soldiers on the ground.
POWER SOURCE—Payload power supplied by airframe; operator workstation power supplied by generator.

**OPERATOR/MAINTAINER—**Pilot: MOS 150U (UAS Warrant Officer); Operator: MOS 15W; Maintainer: MOS 15G/J.
**REFERENCE—**TUAV operational requirements document (ORD).
**STATUS—**Fielded as a QRC niche system deployed to BCTs in CENTCOM AO.

SYSTEM SUMMARY

Payload description—-

- Primary payload is the MOSP 770 (EO/IR/LD).

  - FMV.
  - Color EO.
  - Multiple-mission configurations.
  - Currently tri-sensor (EO/IR/LD) transitioning to quad-sensor (EO/IR/LD/LRF).
- May employ Greendart payload.
- May employ communications relay payload (CRP).
- May employ VIPER STRIKE.

Platform description—

- Ceiling—18,000ft (MSL).
- Endurance—21 hrs.
- Loiter speed—80 knots.
- Data link range—67+ nm. (w/o relay); 107+ nm. (w/ relay).
- Crew—one air vehicle operator, one payload operator.

**Figure I-25. MQ-5B, HUNTER UAS**

**NOMENCLATURE—**MQ-5B, Hunter UAS.
**PROJECT NAME—**Hunter UAS.
**FUNCTION—**The MQ-5B Hunter provides division and corps commanders a persistent capability to detect, locate, identify, and track surface targets in day and night conditions with a high degree of timeliness and accuracy.
**DESCRIPTION—**MQ-5B Hunter is an AISR system supporting tactical forces in full spectrum operations. It carries IMINT and SIGINT payloads The EO/IR payload provides FMV, while the SIGINT payload provides precision geolocation of intercepted modern signals. There is an armed MQ-5B HUNTER variant equipped with VIPER STRIKE munitions currently operated by GOCO units. It provides multidiscipline collection and support, and is a multimission, medium-altitude and endurance UAS.
**CAPABILITIES—**Hunter conducts battlefield surveillance using its electro-optical and infrared payload. It also communicates AISR and battle damage assessment information in real-time by relaying payload data via the digital data link to tactical commanders and Soldiers on the ground.
**POWER SOURCE—**Payload power supplied by airframe; ground station power supplied by generator.
**OPERATOR/MAINTAINER—**Aerial exploitation battalion (AEB) personnel; Pilot—MOS 150U; Operator—MOS 15W; Maintenance—MOS 15G/J; GOCO personnel— contractor operated and maintained.
**REFERENCE—**UAV-SR ORD.
Fielded to three AEBs (15th MI BN, 224th MI BN, and 1st MI BN) plus training base; one GOCO unit (partial system).

SYSTEM SUMMARY

Payload description—-

- Greendart.

  - Special purpose payload on the MQ-5B, Hunter UAS.
  - Provides APG targeting support to BCT.
  - Uses MOSP 770 EO/IR/LD payload as confirmation and overwatch capability.
  - Requires separate Greendart workstation located in SCIF.

Platform description—

- The MQ-5B HUNTER UAS is the baseline platform.
- Greendart payload does not degrade flight characteristics of MQ-5B, Hunter UAS.
- Uses interchangeable payload package for simple aircraft modifications based on mission needs.

**Figure I-26. Greendart on MQ-5B, Hunter UAS**

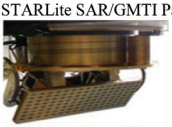
**NOMENCLATURE—**Greendart on MQ-5B, Hunter UAS.
**PROJEC NAME—**Greendart.
**FUNCTION—**Provides aerial precision geolocation (APG) to the warfighter.
**DESCRIPTION—**The Greendart is a special purpose payload that can be installed on the MQ-5B, HUNTER UAS. It consists of hardware (payload chassis, antennas, encryption and decryption boxes, and a separate operator workstation) and software. The Greendart incorporates a separate communications relay channel enabling the Greendart and MQ-5B, HUNTER UAS payload operators to communicate directly with the supported signal terminal guidance (STG) teams. The Greendart shares the same data links, logistical support, and baseline of equipment as other MQ-5B, HUNTER UAS payloads.
**CAPABILITIES—**The Greendart payload operates in dense signals environments against modern threat emitters. It provides precision geo-location of intercepted signals. The onboard MOSP 770 EO/IR payload provides confirmation and an overwatch capability once it is passed to the STG teams.
**POWER SOURCE—**Greendart payload power is supplied by MQ-5B airframe; GREENDART payload operator workstation power supplied by standard power sources in a SCIF.
OPERATOR/MAINTAINER—GOCO.
**REFERENCE—**Greendart CONOP.
**STATUS—**The capabilities of Greendart were evaluated by the Capabilities Development for Rapid Transition (CDRT) Board resulting in the decision to migrate its capabilities into the Tactical SIGINT Payload (TSP) POR.

SYSTEM SUMMARY

Payload descriptions—

- Common EO/IR/LD Sensor Payload.

  - Color television with B/W mode.
  - Image Intensified ($I^2$) TV.
  - Laser rangefinder/laser pointer.
  - Laser designator and spot tracker.
  - Fused/blended imagery.
  - The gimbal is stabilized w/integrated IMU for precise targeting.
  - Provides FMV imagery to detect, recognize and identify multiple moving and stationary targets.
  - Provides common user interface for Gray Eagle and armed scout helicopter (ASH); reduces CAB logistical burden.
  - Planned enhancements include high definition (HD), increased target location accuracy (TLA), and 3rd Generation IR.
- STARLite SAR/GMTI Payload.



*Antenna Assembly*

  - Provides a Ku Band multi-mode radar capability in near-all battlefield conditions (day/night, adverse weather/atmospheric conditions) to collect imagery and target data.
  - Produces SAR strip mode and wide area surveillance products.
  - The SAR spot mode provides higher resolution.
  - Change detection capability compares and highlights changes in imaged areas over time.
- Tactical SIGINT Payload.

  - Provides a modular COMINT payload.
  - Provides advanced APG capabilities.
  - Provides improved access to low-power targets.
  - Provides advanced digital beam forming antenna array to mitigate co-channel interference.

Platform description—

- Ceiling—25,000 ft. (MSL).
- Endurance—24-30 hrs.
- Loiter speed—90 knots.
- Data link range—67+ nm. (w/o relay), 160+ nm. (w/ relay); SATCOM capable.
- Crew—one air vehicle operator, one-two payload operators.

**Figure I-27. MQ-1C, Gray Eagle UAS, Extended Range Multi-Purpose (ERMP)**

**NOMENCLATURE—**MQ-1C, Gray Eagle UAS, Extended Range Multi-Purpose (ERMP).
**PROJECT NAME—**MQ-1C, Gray Eagle.
**SENSOR NAMES—**Common Sensor Payload (CSP), STARLite SAR/GMTI Payload, and TSP.
**FUNCTION—**The MQ-1C, Gray Eagle UAS, while using the CSP, STARLite, and/or TSP, will provide the division and military intelligence brigade (MIB) with improved situational awareness to permit forces to maneuver from a position of advantage with greater speed and precision.
**DESCRIPTION—**The MQ-1C, Gray Eagle UAS, consists of launch and recovery equipment; five ground control stations; and twelve aircraft with payloads. This system is also SATCOM and Air Data

Relay (ADR) capable to support BLOS operations. The CSP is an EO/IR/LD sensor that provides full motion video capability. The STARLite SAR/GMTI payload provides a near all-weather still imagery and moving target indicator capability. The TSP provides precision geo-location of intercepted modern signals capability. The TSP is a complementary and evolutionary SIGINT capability to GRCS, ARL, EMARSS, and the AISR Constellation, and provides additional dimension to manned-unmanned (MUM) teaming by covering SIGINT gaps. The MQ-1C, GRAY EAGLE UAS, also has external hard points that are capable of supporting payload pods or weapons.

**CAPABILITIES—**The MQ-1C, Gray Eagle UAS, uses IMINT and SIGINT payloads to provide multi-intelligence collection and support to the brigade combat team (BCT).

**OPERATOR/MAINTAINER—**Operator: MOS 15W (UAS operator, CSP and STARLite payload operator); MOS 150U (UAS technician); MOS 35N/35P (SIGINT mission); maintainer: MOS 35T (SIGINT payload) and MOS 15G/J.

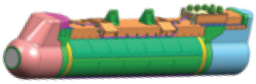
**POWER SOURCE—**Payload power supplied by airframe; operator workstation power supplied by generator.

**REFERENCE—**ERMP CPD.

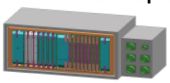
**STATUS—**QRC 1 fielded in FY09; first unit equipped (FUE) is scheduled for FY11.

## AIRBORNE MOVING TARGET INDICATOR











SYSTEM SUMMARY

Sensor description—

- This is a tactical radar for direct support of a BCT capable of detecting, recognizing and tracking target types of dismounts, and vehicles.
- VADER is a day/night/near all weather airborne dismount/ground (vehicle) moving target indicator (D/GMTI) SAR with advanced active electronically scanned array (AESA) antenna.
- Can be integrated on multiple platforms, e.g., Twin Otter, A-160 Hummingbird, Long Endurance Multi-INT Vehicle (LEMV), and ERMP UAS.
- Produces GMTI, SAR, FMV and annotated imagery.
- Provides FMV EO/IR/illuminator multi-lens camera to assist classifying and identifying targets and provides additional tracking.
- Capable of limited identification of humans, animals and limited vehicle signatures.
- VADER Exploitation Ground Station (VEGS) allows unique forensic analysis of detections, tracking and recognition processing.
- Sensor weight is 400 lbs. and uses 2500 watts.

Aircraft—Twin Otter surrogate during the development of the system. Planned upgrades to the platform include the A-160 Hummingbird Vertical Takeoff and Landing UAS and the MQ-9 Reaper.

**Figure I-28. Vehicle and dismounts exploitation radar (VADER)**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Vehicle and dismounts exploitation radar (VADER).
**FUNCTION—**VADER detects the IED chain/phases of operation and is able to conduct unique forensic analysis.
**CAPABILITIES—**VADER is a hybrid advanced kinematic/multiple hypotheses MTI tracker. Wide area coverage can cover a major portion of a BCT AOR with the electronic scanning providing moving vehicle detections. Smaller areas of search are used to focus the AESA antenna energy to detect moving dismounts. The operator can zoom via the radar's modes to improve resolution and target details including accurate target location coordinates. Using the dismount characterization analysis and MTI detections, the operator can cue the FMV imagery providing additional recognition and identification of the target and provide NRT entity analysis for separate reporting of unique information. It is designed for target validation and annotated SAR.

- GMTI data of both dismounts and vehicles are reported via the STANAG 4607 format allowing

DCGS-A and other MTI application workstations to process data.

- SAR is reported in national imagery transmission format (NITF) 2.1 standard format that is usable by DCGS-A workstations to conduct recognition of targets, metallic detections, terrain disturbances, and feature changes with common detection and coherent change detection processing.
- The ground control station and peripherals are configured for system management, sensors control, telemetry instrumentation, weather tracking, airspace control interface, and mission management.

**POWER SOURCE—**Aircraft-generated power.
**OPERATOR/MAINTAINER—**VADER is a government owned, contractor operated (GOCO) and contractor-maintained program. No transition plan is intended in the near future.
**STATUS—**QRC; advanced concept technology demonstration ACTD.

SYSTEM SUMMARY

FEATURES (E-8C)—

- MTIs.
- SAR/FTI Imagery.
- Joint Tactical Terminal.
- 18 Work Stations.
- Joint Air Crew.

FEATURES (CGS/JSWS)—

- NRT Multi-Sensor ISR Display.
- Operations on the move (OTM) (CGS) Joint Tactical Terminal Direct Simulation Interface.
- GOTS/COTS Equip (CHS II Compliant).
- Color Photo Printer.
- E-Maps/Digital Terrain Data.
- GPS.

INTEROPERABILITY/INTERFACE (E-8C)—

- CGS/JSWS.
- Airborne Warning Control System (AWACS).
- Intel Broadcasts.
- Air-Air/Air-Ground Fighters.
- RC-135V/W Rivet Joint.

INTEROPERABILITY/INTERFACE (CGS)—

- Advanced Field Artillery Tactical Data System (AFATDS).
- All Source Analysis System (ASAS).
- UAS/UAV.
- GRCS.
- ARL-M.
- U-2.
- Apache LONGBOW.
- Secondary Imagery Systems.
- MSE/ATCCS/ABCS LANS.
- TROJAN.
- Intel Broadcasts (SIGINT).
- DIS/HLA Simulations.
- Other CGS/JSWS.

OPERATIONS (CGS/JSWS)—

- Correlate, display, and manipulate multi-sensor data.
- Remote workstation (CGS).
- Color/black and white hardcopy imagery/reports.
- Mission history replay.
- Graphics, targeting, tracking display, storage & target files.

TABULATED DATA (E-8C)—

- Coverage—Army corps AOI.
- Aircraft range—8 to 20 hrs.

**Figure I-29. Army Common Ground Station (CGS) and the Air Force Joint Surveillance Target Attack Radar System (JSTARS)**

**NOMENCLATURE—**AN/TSQ-179(V) 2.

**PROJECT NAME—**Army Common Ground Station (CGS) and the Air Force Joint Surveillance Target Attack Radar System (JSTARS).

**FUNCTION—**JSTARS is a joint Army/Air Force wide area ISR program that provides NRT information to all levels of command and services. When the E-8C is in direct support of the Air





FOR OFFICIAL USE ONLY

Force, its primary role is battle management, vectoring ground attack aircraft to targets, and situational awareness. The Army crew on board ensures ground commanders are supported and de-conflicts priority of radar service requests. The CGS provides support to the commander for real-time battlefield surveillance, situation awareness, battle management, combat assessment, target development and direct targeting, battlefield visualization, and limited theater missile defense support. The CGS acquires, processes, displays, stores, and disseminates MTD, FTD, and SAR images from the Air Force E-8C airborne sensor, as well as multiple real-time sensors including UAS and MTI imagery, Intelligence Broadcast System (IBS) SIGINT display and correlation, GRCS (SIGINT), Apache LONGBOW FCR and position data, U-2R E-MTI, ARL (MTI), Secondary Imagery Dissemination System, and ASTOR (MTI and SAR).

**DESCRIPTION—**The E-8C aircraft is a militarized Boeing 707-300 series aircraft. It carries a flight and mission crew of three Army and 18 Air Force personnel. It operates at an altitude of 30,000 feet with a planning endurance time of 11 hours (20 hours with in-flight refueling). The crew can be expanded to 35 personnel for extended missions. A normal mission profile provides for eight hours of on-station time with two hours' total transit time to and from the orbit area. The E-8C radar is capable of looking deep into hostile and potentially hostile areas to detect, locate, and track a variety of targets. It can be operated in two basic radar modes-- MTI and SAR. A 5-channel intercommunications system, which links all workstations and flight-crew positions, provides the internal communications for the E-8C. The external communications provide voice and data transmissions for LOS and non line-of-sight (NLOS) communications. SATCOM provides capability for BLOS communications to joint command and control targeting nodes, and to CGSs beyond aircraft surveillance and control data link (SCDL) LOS. E-8C operators can pass information to other Air Force platforms and command and control nodes, such as AWACS. The CGS is a secret collateral system that is designated to support commanders and staff at all echelons with battlefield visualization in NRT. Is designed to operate on-the-move to keep situational awareness for the commander. It interfaces with ACE, TOC, aviation, and artillery nodes. The CGS has a robust suite of modern communications, which include SATCOM. The Joint Stars work station (JSWS) is a standalone CGS workstation that has the same capability and software as a CGS. It will be located at fixed joint intelligence facilities, bunkers, battle labs, battle simulation centers, and select EAC units. The CGS uses commercial computer, servers, workstations, networking, and industry standard interfaces. It can pass information to its supported units, to the E-8C aircraft, or other CGSs via voice, TACLAN, UHF, VHF, mobile subscriber equipment, FAX, hard copies, SCDL, SATCOM, landline, Army Battle Command System (ABCS) LAN and STU-III/STE. Operators may request images of a specific area through voice/digital communication with the E-8C, voice communication with ARL-M aircraft, or from tactical/strategic IPLs. JSWS can use the same communications as CGS. The CGS system is configured with two operator workstations in the CGS, one CGS remote work station, one CGS remote cab display located in the vehicle cab, and two printers, one color photo capable, one black and white. CGS and JSWS provide the commander with a fully adjustable, deployable, mobile, and responsive ISR processing capability to present a correlated multi-sensor picture of the battle to commanders at all echelons. The CGS and JSWS software are based on a real-time open system architecture using modules or engines. The surveillance control data link (SCDL) is pictured in figure I-29.

**POWER SOURCE—**Aircraft-generated power. The CGS operates on 115-VAC, 50/60 Hz, 3-phase power provided by towed 10 kW tactical quiet generators or the TOC power grid. It can also operate on 200-VAC, 50/400 MHz, 3-phase commercial power or other unit power generation equipment. The JSWS operates on 115-VAC, 60 Hz, 3-phase power. It can also operate on 200-VAC, 50 MHz, 3-phase commercial power.

**OPERATOR/MAINTAINER—**MOS 35H, 35T.

**REFERENCES—** FM 3-09.60; FM 6-60; ST 6-60-30; TM 11-5865-299-BD; CGS DTT, November 2000.

**STATUS—**The CGS is an Army POR and the JSTARS is an Air Force POR, as separated by the Army Acquisition Authority.

## ELECTRONIC SUPPORT SYSTEM

**Figure I-30. Prophet Electronic Support (ES), Spiral I (Detecting System Countermeasures)**

**NOMENCLATURE—**AN/MLQ-40 (V 4).
**PROJECT NAME—**Prophet Electronic Support (ES), Spiral I (Detecting System Countermeasures).
**FUNCTION—**Prophet provides commanders the ability to perform electronic intelligence preparation of the battlefield, battlefield visualization, target development, and force protection. It has the ability to detect, locate, collect, exploit, and electronically attack selected emitters in areas where ground reconnaissance assets cannot penetrate or cover.
**DESCRIPTION—**Prophet is the Army's brigade combat team (BCT)- and battlefield surveillance brigade (BFSB)-dedicated, ground-based SIGINT and electronic attack (EA) system, and is an integral part of the Army's new modular design. Prophet operates in direct support to division BFSBs, BCTs, Stryker brigade combat teams (SBCTs), and armored cavalry regiments (ACRs). A Prophet system comprises two or more Prophet sensors (depending on the echelon of assignment) and Prophet control (PC), a command and control (C2) system containing the resources and activities required to plan, execute, and control Prophet's operational functions and to access the Global SIGINT Enterprise (GSE). Prophet ES Spiral I, AN/MLQ-40 (V4), is an advanced SIGINT system with organic wideband LOS communications equipment, special sensor capability (SSC), independent server, and dual CF-29 laptops running Single SIGINT Software Baseline (S3B) software. The system is transported within an environmentally controlled, three-seat, fully up-armored M1165A1(B3) (HMMWV) to improve survivability and sustainment. The M1165A1 (B3) pulls a trailer containing an AN/PRD-13(V2) man-pack ES subsystem, AN/PRC-19 man pack Single Channel Ground and Airborne Radio System (SINCGARS), Soldier-equipment, and sure-power unit. The following are its characteristics:

- Dedicated, all weather, 24/7 tactical COMINT and EW system integral to the expeditionary Army SIGINT.
- Enhanced ground-based, man-pack, dismounted capability to detect, identify, locate, and exploit enemy communications while at-the-short-halt.
- High-speed wideband BLOS data communications provide NSAnet/GSE access at point of collect that enables processing, collaboration, and dissemination of intelligence.
- Collaborative audio and data file-sharing via the RTRG.
- Up-armored and environmental controls improve sustainability and survivability.
- Scalable, flexible, open architecture, and TI to counter dynamic threat.

**Prophet System Variants**

- Prophet ES Spiral I plus AN/MLQ-40 (V5) (P3I).
  - Replaces AN/VRC-99 with WB BLOS communications on Prophet ES Spiral I.
  - Fielded to OEF.

- TRITON III (QRC).
  - Advanced SIGINT sensor on a Cougar medium mine resistant ambush protected (MRAP) vehicle.
  - Adds WB BLOS communications.
  - Fielded QRC to support OIF.

- Prophet Enhanced ISR Surge, AN/MLQ-44 (QRC).
  - Advanced SIGINT sensor on a Panther/XM-1229 medium MRAP vehicle.
  - Adds dismounted and man pack capability.
  - Adds WB BLOS communications.
  - S3B v2.
  - Fielded to OEF.

- Prophet Enhanced program of record (POR), AN/MLQ-45 (P3I).
  - Adds dismounted and man pack capability to POR.
  - Adds WB BLOS communications.
  - To be fielded FY2011.

**CAPABILITIES**

- Exploits signals internals for intelligence and immediate combat information in support of stability operations.
- Provides near real time (NRT) protection of the force, situational awareness, and actionable intelligence to the BCT, SBCT, ACR and BFSB maneuver elements.
- Organic communications jamming.
- Supports high-value target/high-value individual (HVT/HVI) targeting.

**BASIS OF ISSUE—**

| | |
|---|---|
| • BCT | 2 Sensors, 1 control with T-LITE. |
| • SBCT | 3 Sensors, 1 control with T-LITE. |
| • ACR | 4 Sensors, 1 control with T-LITE. |
| • BFSB MI BN | 4 Sensors, 2 controls each with T-LITE. |
| • TRADOC | 6 Sensors, 3 controls each with T-LITE. |

**POWER SOURCE—**Self-contained, sure-fire power unit.
**OPERATOR/MAINTAINER—**
**REFERENCE—**
**STATUS—**Status of Prophet depends on the variant; variants exist as QRC and PORs. Prophet has been fielded to the active component (AC) and the reserve component (Active Reserve and National Guard). In the future, PC will be re-designated Distributed Common Ground System–Army (DCGS-A) and receive the same functionality as other SIGINT enclaves.

# Appendix J

# Processing Systems

## INTRODUCTION

**J-1.** A processing system is designed to convert raw data into useful information. The systems discussed in this appendix are currently in use in Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF), and elsewhere.

### Distributed Common Ground System-Army Weather Services

**SYSTEM SUMMARY**

| FEATURES— | TABULATED DATA— |
|---|---|
| • Receives digitized weather data from satellites, local and remote weather sensors, artillery meteorological (ARTYMET) systems, U.S. Air Force (USAF) Weather Centers and Squadrons. | • Prime mover—High-mobility multipurpose wheeled vehicle (HMMWV). |
| • Processes and displays satellite weather imagery, upper air data, surface weather reports, manual and automated weather forecasts. | • Power—115-variable AC (VAC), single phase, 60 hertz (Hz). |
| • High resolution satellite photographs. | • Power source—Standard 10 kW generator. |
| • Supports IPB and terrain analysis. | • Command Post and Light Configurations—TBD. |
| • Provides tactical decision aid (TDAs) to the commander. | |
| • Disseminates forecasts and TDAs to all users. | |

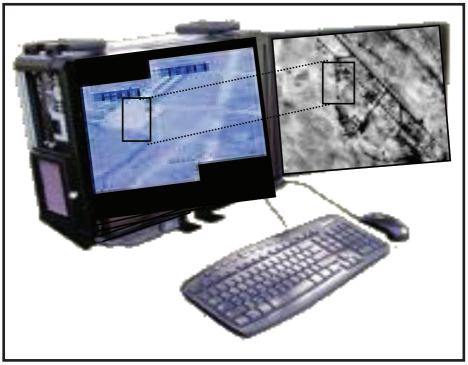
**Figure J-1. Distributed Common Ground System-Army weather service**

**NOMENCLATURE—**AN/TMQ-40A, Integrated Meteorological System IMETS, Block II.
**PROJECT NAME—**Distributed Common Ground System-Army Weather Services (DCGS-A WS).
**FUNCTION—**The DCGS-A WS is the meteorological component of the intelligence, surveillance, and reconnaissance (ISR) sub-element of the Army Battle Command System (ABCS). DCGS-A WS provides commanders at all echelons with an automated weather system to receive, process, disseminate weather observations and updated forecasts. The system also processes weather and environmental effects to aid all intelligence operating systems which provide data to support air defense, fire support, and ISR.
**DESCRIPTION—**DCGS-A WS is an HMMWV-mounted tactical DCGS-A WS receives weather information from polar orbiting civilian and defense meteorological satellites, Air Force Global Weather Center, artillery meteorological teams, remote sensors, and civilian forecast centers. DCGS-A WS processes and collates forecasts, observations, and climate data to produce timely and accurate weather products that are tailored to the needs of the supported commander. It is staffed and operated by USAF weather personnel and maintained within the scope of existing Army support principles. It is deployed at combatant command, corps, and division aviation brigades, division armored cavalry regiments (ACR), separate brigades, Special Operations Forces (SOF) Groups, ranger regiments, and special operations aviation regiments, psychological operations groups, and transportation groups. Communications included in DCGS-A WS are meteorological satellite (Sea Space), single-channel, ground and airborne radio systems (SINCGARS), tactical anti-jam secure voice/data radio, and digital subscriber voice terminal. DCGS-A WS generates the following United States message text format (USMTF) standard reports, standard weather products, and special weather products as follows:

- **AO—**Typically issued every six hours and tailored to the mission. Valid for 24 to 72 hours for a specific AO.
- **WEATHER EFFECT MATRIX—**Issued every six hours with forecast; valid 24 hours or beyond.
- **NVG/LIGHT DATA—**Issued daily with forecast; valid for the entire forecast period.
- **WEATHER OVERLAYS/GRAPHICS—**Issued when requested or required by supported unit; valid for specified time, location, and criteria.
- **EO FORECAST—**Issued when requested or required by supported unit; valid for specified time, location, and weapons system.
- **FLIGHT, MISSION, AND STAFF BRIEFINGS—**Issued when requested or required by supported unit; valid for specified time and location.

DCGS-A WS is deployable on C-130, C-17, and C-5 aircraft, maritime transport, and rail. It is self-deployable on the HMMWV and can be hand carried by an operator. One version of the system resides in a Standardized Integrated Command Post System shelter mounted on the M-1097 HMMWV. Command post and man-portable units are transportable on troop transports.
**POWER SOURCE—**Requires 115-VAC, 60 Hz power provided by the system 10 kW tactical generator, commercial power, or other unit power generation equipment. The light configuration processor operates from internal rechargeable batteries, in addition to commercial and generator power.
**OPERATOR/MAINTAINER—**USAF weather personnel.
**REFERENCE—**FM 34-81.
**STATUS—**No longer in the inventory; however, its capabilities will be merged into a new program of record (POR) under DCGS-A.

## Imagery Workstation (IWS)



**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • Capable of exploiting full motion video, national technical means, and theater imagery data. | • 250GB of storage. |
| • Capable of performing "chat" sessions. | • Capable of Ethernet and fast Ethernet connectivity. |
| • White board capable over the SECRET Internet Protocol Router Network (SIPRNET). | • Disseminate or receive documents using a push/pull capability. |

**Figure J-2. Imagery Workstation**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Imagery workstation (IWS).
**FUNCTION—**Provide Army combat units at brigade with capabilities to exploit full motion video (FMV), national technical means, and theater imagery data. The IWS receives, stores, exploits, and disseminates imagery and products from organic and non-organic sources; receives, stores, analyzes, and disseminates FMV data; and exploits or cues using moving target indicator (MTI) data. As a precursor to the BCT DCGS-A platform, provides all the initial capabilities listed within the operational needs statement (ONS), as well as additional capabilities for enhanced targeting and MTI, not found within the initial DCGS-A platform. With the IWS, the brigade combat team (BCT) can conduct intelligence functions within the task, post, process, and use chain with limited to no external support, narrowing the timeline for true actionable intelligence.
**DESCRIPTION—**The IWS Server (a MaxPac 8219XR Dual XEON 3.2 GHZ, 1MB Cache 4GB random access memory [RAM]) hosts the IMINT processing software and database and provides exploitation support to the workstation clients. The IWS has 250 gigabytes worth of storage. The IWS employs an imagery exploitation package (Remote View, Multimedia Analysis and Archive System (MAAS), moving target information exploitation (MTIX), and precision strike suite for special operations forces (PSS-SOF) and is capable of formatting all images into NITF 2.0 format for storage and dissemination. The IWS connects to other intelligence nodes through the SIPRNET LAN at the collateral level. The IWS performs "chat" sessions and white board discussions over SIPRNET. It can also disseminate or receive documents using a push/pull capability. The IWS possesses Ethernet (10BaseT-- 10 Mbps), and Fast Ethernet (100BASE-X—100 Mbps) connectivity. The system server

provides an interface port supporting X.25 and TCP/IP. Products can be pushed to or pulled by customers.
**CAPABILITIES—**The IWS will receive imagery to include FMV through the LAN. Products from exploitation are imagery-derived products; an IPIR, targeting graphics or UAS FMV exploit products which are disseminated over the LAN. Performs full motion video exploitation for Hunter, I-GNAT, and Shadow TUAS. Additionally capable of performing imagery exploitation of national, theater and tactical EO, infrared, and SAR. IWS provides full research integration capabilities to NGA IPL, WARP, and JWAC. It enables precision geo-location to under 6 meters using DPPS. It can also import MTI using MTIX software pulling from MTIX servers or received from PC-based CGS.
**OPERATOR/MAINTAINER—**35G; contractor support.
**STATUS—**QRC.

## All-Source Analysis System Family of Systems

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • All-source intelligence fusion, analysis and dissemination system. | • Immediate high-payoff target (HPT)/ high-value target (HVT) alarming and reporting. |
| • Integrates collection management functionality. | • Automated and interactive database correlation. |
| • Intelligence systems technical control system. | • Supports jump, degraded, and split-based operations. |
| • Common ABCS hardware/software. | • Communicates via Army common user system (ACUS)—satellite communications (SATCOM), mobile subscriber equipment high-capacity line-of-sight (MSE-HCLOS), joint network node (JNN), tri-Service tactical communications (TRI-TAC), automatic digital network (AUTODIN), and Defense Secure Network (DSNET). |

| FEATURES— | |
|---|---|
| • Processes/disseminates collateral and sensitive compartmented information (SCI) reports. | • Integrates message processing with graphical, National Geospatial-Intelligence Agency (NGA) digitized terrain data. |
| • Rapidly processes large message volumes. | • Direct data exchanges with joint and national databases. |

**Figure J-3. All-Source Analysis System**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**All-Source Analysis System (ASAS).
**FUNCTION—**The ASAS is the intelligence and electronic warfare (IEW) component of the Army Tactical Command and Control System (ATCCS). It is an automated intelligence fusion system that supports the commander in rapidly gathering, recording, analyzing, and disseminating the high volume of intelligence data processed during wartime and other military operations. The system supports the G-2 and the S-2 and the analysis and control element (ACE) in directing ISR operations and producing intelligence that meets the commander's needs. It provides connectivity between sensors and intelligence activities at multiple echelons.
**DESCRIPTION—**The ASAS is a tactically deployable, ruggedized, and automated information system. It consists of evolutionary computer hardware, software, and associated secure communications systems that support the execution of ISR tasks, analysis, and dissemination. The ASAS consists of two blocks—ASAS Block I systems and ASAS Block II systems. The ASAS Block II family of systems consists of five major systems (see figure J-4). The SCI ACE subsystems include the ASAS Fusion System, Single Source Workstations, Trusted Workstation, and Trusted Guard Suite. The collateral ASAS systems include the ACT-E, ASAS-IFS, and ASAS-L. The fifth major system, the communications control set (CCS), is the collateral/SCI bridge between the ACE and collateral ASAS systems. The ASAS is fielded to Army units from EAC to ECB. It can be found in the Military Intelligence (MI) brigade ACE, corps ACE, division ACE, ACR, brigade S-2, battalion S-2, and Special Forces. ASAS, having no organic communications, relies on communications provided by the unit—for example, TROJAN SPIRIT or ACUS. The ASAS can either be deployed as part of a larger command post, or separately as a division intelligence support element to sustain a variety of training and real-world missions. When deployed in this manner the ASAS should co-locate with an available signal unit and communications node for communications support, logistics, and mutual security.

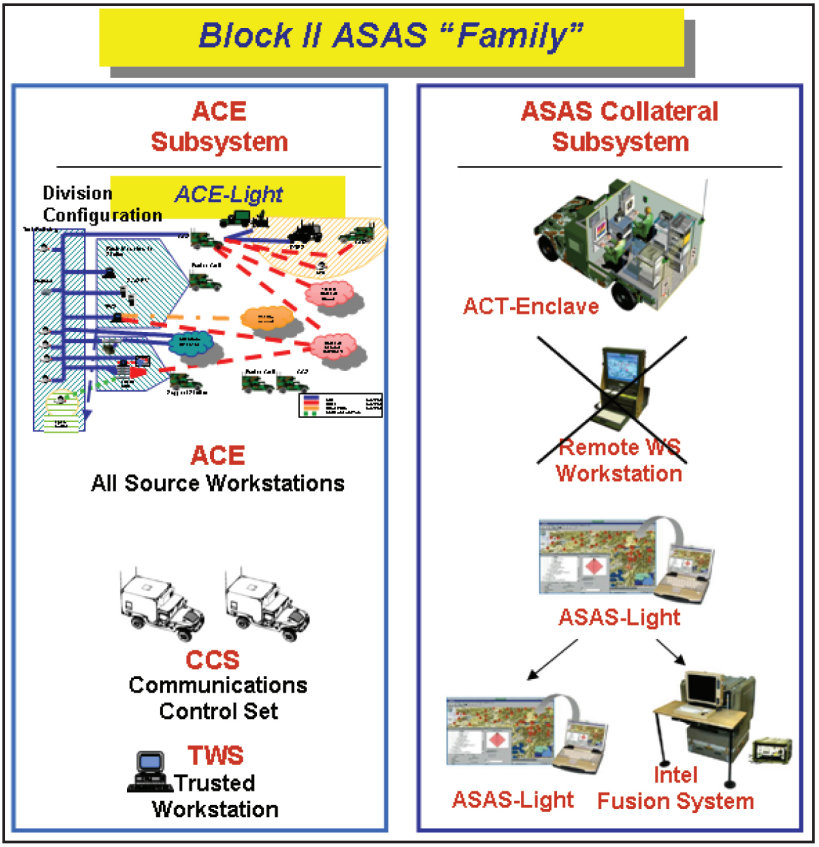



**Figure J-4. Block II ASAS family**

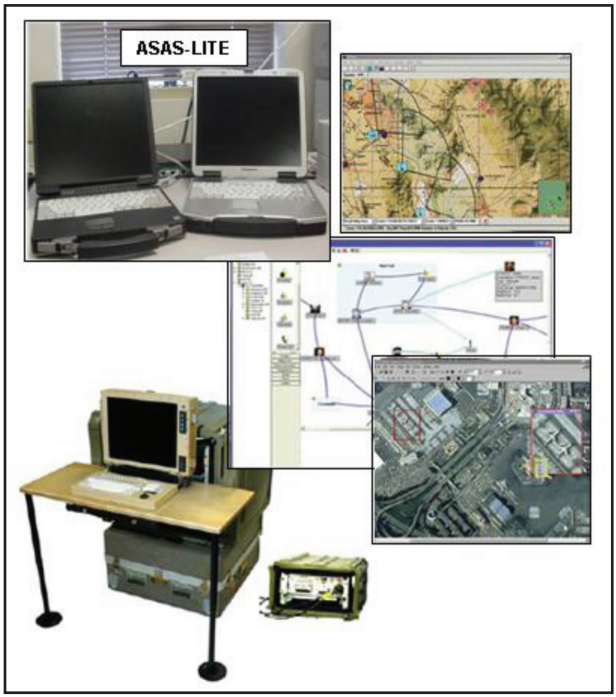
**POWER SOURCE—**Requires 115 VAC, 60 Hz power. The ACE and ACT-E have organic 30kW or 10 kW tactical generators. Other ASAS systems rely on commercial power or other unit power generation equipment.

**OPERATOR/MAINTAINER—**35F, 350F, 35N, 352N, 35G, 350G, 35L/M, 351L/M, 35T.

**REFERENCES—**

**STATUS—**With the exception of a few Block I ACE systems, most of the Block I systems are no longer in the Army's inventory. ASAS capabilities are now DCGS-A-enabled.

## All Source Analysis System-Lite and All Source Analysis System-Intelligence Fusion Station




**SYSTEM SUMMARY**

| FEATURES— | TABULATED DATA: |
|---|---|
| • All-source intelligence fusion, analysis and dissemination system. | **ASAS-L—** |
| • Integrates collection management functionality. | • Item Name—Notebook. |
| • ISR systems technical control system. | • Computer part number—NCU/CF-73 Dell M90. |
| • ABCS interoperable. | • Fast Ethernet—10/100 PCMCIA card. |
| • Processes/disseminates collateral reports. | • Removable hard drive—2 ea x 20 GB. |
| • Alerts criteria/event detection of inbound message traffic. | • CD-ROM drive—CF-VCD721. |
| • Integrated map functionality. | • Drive—superdisk, LS-120, CF-V0 lbs. |
| • Access to national, joint, and theater intelligence databases. | **ASAS-IFS—** |
| • Configurable to operate as a stand-alone system. | • Item Name—Desktop. |

| FEATURES— | TABULATED DATA: |
|---|---|
| | • Computer part number—3U RX. |
| | • Removable hard drive—two each x 20 GB. |

**Figure J-5. All Source Analysis System-Lite and All Source Analysis System-Intelligence Fusion Station**

**NOMENCLATURE—**AN/TYQ-93A(V)3 and AN/TYQ-93B(V)2.
**PROJECT NAME—**All Source Analysis System-Lite (ASAS-L) and ASAS-Intelligence Fusion Station (ASAS-IFS).
**FUNCTION—**The ASAS-L and ASAS-IFS provides an automated intelligence analysis capability to the lowest tactical echelon. The ASAS-IFS is provided to select collateral intelligence work centers having a requirement for significantly more processing power and storage capacity than those delivered by the laptop. ASAS-Lite and the ASAS-IFS are fully compliant and interoperable with the ABCS.
**DESCRIPTION—**The ASAS-L system was developed for the battalion S-2 located in the maneuver battalion tactical operations center (TOC), but the system has since been fielded to all Army echelons. The ASAS-L is lightweight, and scalable. The system can be hosted on a number of hardware platforms and consists of a core set of data processing, analysis, visualization, intelligence production, and dissemination tools designed for stability operations and civil support operations and force-on-force combat operations.
ASAS-L incorporates Microsoft technologies (Microsoft Windows XP and Server 2003) to provide Soldiers a common set of automated intelligence processing, analysis, and reporting tools at all Army echelons from battalion to corps. ASAS-L software is hosted on ruggedized, commercial laptops and servers. The ASAS-L RELKOR version of software enables tactical units to process information up to and including SECRET at Mission Assurance Category II. ASAS-L can receive and parse individual, event, organization, place, unit, equipment, and facility data into its databases via eXtensible Markup Language (XML) messages, the PASS, USMTF, and other standard data exchange formats. The ASAS-L is also used to transmit critical battlefield messages such as the size, activity, location, unit, time, and equipment (SALUTE), tactical report (TACREP), and target intelligence data (TIDAT). Most tools are web-enabled allowing Soldiers to browse other systems' Web pages and share critical intelligence via familiar user-friendly interfaces. The ASAS-L is interoperable with a number of joint and Army systems including ABCS and non-ABCS systems. It is the primary intelligence processing system used by the Army to maintain the battalion-level situational awareness. ASAS-L has full interoperability with ASAS-IFS and ASAS Blocks I and II. ASAS-L and IFS platforms capable of hosting DCGS-A v3 software that have not already been upgraded will be upgraded as part of a unit's reset, ramp-up for deployment, or as a regularly scheduled hardware refresh.
**OPERATOR/MAINTAINER—**MOS and AOC 35F, 350F, 35T.
**REFERENCE—**
**STATUS—**ASAS-L is an ASAS Block II program under the direction of the program manager for intelligence fusion. ASAS-L and IFS capabilities are now DCGS-A-enabled.

## Analysis and Control Team-Enclave, AN/TYQ-103.

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • Self-contained system. | • Built-in e-mail, FTP, web services. |
| • Disseminates near real time (NRT) current threat situational awareness. | • Allows analysts to browse other systems' web pages. |
| • Rapidly processes large volumes of information. | • Sends and receives NITF imagery, graphic INTSUMs, and overlays. |

**Figure J-6. Analysis and Control Team-Enclave**

**NOMENCLATURE**—AN/TYQ-103.
**PROJECT NAME**—Analysis and Control Team-Enclave (ACT-E).
**FUNCTION**—The ASAS ACT-E (hereinafter called the ACT-E) is designed to provide a brigade combat team (BCT) with a self-contained system capable of receiving, processing, and disseminating NRT current threat situational awareness needed for commanders to view the operational environment and plan and execute the battle. The ACT-E rapidly processes large volumes of intelligence and sensor information. It is capable of operating across the entire spectrum of conflict.
**DESCRIPTION**—The ACT-E is a tactically deployable, integrated, shelterized, intelligence system mounted on a HMMWV. The ACT-E is the nexus of intelligence operations within the BCT, integrating intelligence, surveillance, and reconnaissance (ISR) information received from CGS, Prophet-Control, ASAS ACE, other sensor and collectors, and battlefield systems via two on-board ASAS-IFS. The on-board ASAS IFS provide common map products, databases, and communications to provide a COP, planning and execution tools, common operations or intelligence database, and data exchanges to higher and lower echelons. The ACT-E shelter houses two ASAS-IFS hosted on the 3U RX Common Hardware Platform. Communications support consists of two SINCGARS AN/VRC-92F(C) and an Enhanced Position Location Reporting System (EPLRS) AN/VSQ-2(V), data converters, router and peripheral devices. A planned DCGS-A v3 technical insertion will outfit the ACT-E with two rack-mounted workstation suites. Each DCGS-A v3 Work suite consists of a Dell Poweredge 1850 and 2850 server, four monitors, a switch, and keyboards. The ACT-E operates at the security level appropriate to the organization it supports. As with the ASAS-IFS and ASAS-L, the ASAS-L normally operates at the SECRET security level. Planned improvements to DCGS-A will give the ACT-E both

an SCI and collateral capability. The ACT-E is interoperable with other ASAS systems (ASAS ACE, ASAS-IFS, and ASAS-L), CGS, Prophet control, IMETS, ABCS via the Battle Command PASS and select messages, and with other Army and Joint command and control (C2) systems via ACUS. It uses standard IP e-mail communications for inbound/outbound messages through the CMP to send and receive USMTF and VMF messages. Interoperability with the Block II ACE includes graphic and imagery exchanges, select message exchanges, as well as database population, to support the full range of military operations. Dissemination of intelligence is made possible by the on-board EPLRS and SINCGARS radios which give the ACT-E the ability to pass digital data over ACUS or by tying directly in to the TOC LAN and using TOC communications. With built-in-email, FTP, and web services, the ACT-E can send and receive a variety of tactical intelligence reports and products such as ASAS EDC messages. In addition, ACT-E also enables two-way communication of critical operational environment messages such as TACREP and TIDAT messages. The ACT-E also allows analysts to browse other systems' Web pages, send and receive NITF imagery, graphic INTSUMs, and overlays. ACT-E is assigned per BCT or battlefield surveillance brigade (BFSB).

**POWER SOURCE—**Power is supplied by 15-kW generator.

**OPERATOR/MAINTAINER—**35F, 350F, 35T.

**STATUS—**ACT-E is an ASAS Block II program under the direction of the program manager for Intelligence Fusion.

## All-Source Analysis System Block II Analysis and Control Element


**SYSTEM SUMMARY**

| FEATURES— | TABULATED DATA— |
|---|---|
| • All-source intelligence correlation, fusion, analysis and dissemination system. | **AFS—** |
| • Single-source signals intelligence (SIGINT) correlation, net/node/link analysis, TACREP generation. | • ISS component. |
| • Single-source (CI/HUMINT) net/node/link analysis. | • Item name—server. |
| • Limited imagery intelligence (IMINT) capability. | • Computer part number—Sun Fire v480/v490. |
| • Integrates collection management functionality. | • ASWS component—laptop. |
| • All-source and single-source data repositories. | • Computer part number--Dell M90, Bull Frog. |
| • Processes/disseminates SCI and collateral reports. | **ASAS-SS—** |
| • Alerts criteria and event detection of inbound message traffic. | • Item name—desktop computer part number: RUX3, Dell 2650. |
| • Integrated map functionality. | • Item Name—laptop. |
| • Access to national, Joint, and theater intelligence databases. | • Computer part number— Dell M90, CF-73, Bull Frog. |

| FEATURES— | TABULATED DATA— |
|---|---|
| • Configurable to provide a split-based capability. | **TWS and GUARD SUITE** |
| | • Item—laptop. |
| | • Computer part name—Bull Frog, Tadpole. |

**Figure J-7. All-Source Analysis System Block II Analysis and Control Element**

**NOMENCLATURE—**
- ACE-EAC, AN/TYQ-91.
- ACE-Corps, AN/TYQ-92.
- ACE-Division or ACE-ACR, AN/TYQ-89.
- ACE-SOF, AN/TYQ-90.

**PROJECT NAME—**Army Tactical Light Analysis System; All-Source Analysis System Block II (ASAS Block II) Analysis and Control Element (ACE).

**FUNCTION—**The ASAS Block II ACE (hereafter called ASAS ACE) is a tactically scalable system that provides a robust SCI automated intelligence analysis capability at theater, corps, division, ACR, and the Special Forces Group. The ASAS ACE is the 'fusion' engine for the intelligence mission area. As such it serves as the Army's premier integrated data repository for all-source correlated information. It supports the commander's all source intelligence and targeting requirements and is the focal point for IEW/ISR management and synchronization.

**DESCRIPTION—**The ASAS ACE is a shelterized system that consists of COTS common hardware and software (CHS) equipment and selected items of Government furnished equipment (GFE) integrated to comply with the ASAS capability production document (CPD). The ASAS ACE is fully compliant and interoperable with the ASAS-IFS and ASAS-L. The ASAS ACE serves as the primary all-source processing, analysis production, and dissemination C2 intelligence system. The ASAS ACE provides relevant information about threats and the battlefield that is used to plan and execute battles, engagements, and other missions across the full spectrum of operations. It consists of three modules—analytic workstation module comprised of all-source, single-source and open source intelligence (OSINT) terminals; the system administrator/server module consisting of the Intel Server Suite; and a communications/firewall module which includes the Trusted Workstation, Trusted Guard Suite, and the CCS. The communications/firewall module collectively serve as an internal communications support assembly package and provides a communications front-end for messaging, access to communications networks including Joint Worldwide Intelligence Communications System (JWICS), SECRET internet protocol router network (SIPRNET), and connection to multiple sensors and collectors. The ACE-AFS provides all-source analysis and fusion of single-source data received in the Block II ACE. The ACE-AFS consists of the intelligence shared server (ISS), and the ASWS. The ISS is a server class machine executing the all-source fusion processing maintained in a single database. It provides a web-based capability for operators to monitor, view, and access selected capabilities and data on the ISS. One ASAS ACE is assigned to each regional operations company within the MI Operations Battalion of the MI Brigade, one per corps/division main, one per MI Company of the ACR, and one per SF Group. The ACE-AFS includes database capabilities that provide full support for individuals, events, and organizations (IE&O), including criteria alert development; mapping capabilities that include automatic/interactive correlation and normalization, and entity operations that provide the ability to select and process entities directly from the Joint mapping toolkit (JMTK). The ACE-AFS message processing capabilities including automatic receipt, parsing and distribution of USMTF 2000 messages inbound and outbound processing of XML data, and automatic transmission of critical data based on user-set criteria. User utilities include a web-based query of database information that includes crosslinks to multimedia files, Visual Links to display relationships between entities, and GPS Time—Defense advanced GPS receiver (AGR). The ASWS is a client workstation. Analysts control and monitor the all source fusion executing on the ISS. It also provides an extensive tool suite for viewing and analyzing fusion results. The ASAS single-source (ASAS-SS) subsystem automates the

processing and analysis of intelligence data from individual intelligence and battlefield information sources. ASAS-SS is a tactically deployed, automated intelligence system. It supports Army SIGINT analysts at the ACE, intelligence units at EAC, corps, and divisions. Analysts receive SIGINT data through message traffic and augment reporting through access to IMINT reports. As the ASAS component for processing single-source intelligence received from other preprocessors and/or directly from collection assets via the ASAS CCS, the ASAS-SS subsystem receives SIGINT information and processes it into multi-source intelligence products. After processing received information, the ASAS-SS workstation delivers NRT SIGINT updates to the ASCDB in the ASAS all source (ASAS-AS) workstation. The ASAS-SS also provides detailed technical support information back to tactical SIGINT sensors. The ASAS-SS is capable of extracting information from national level databases to support contingency planning or tactical operations. ASAS-SS capabilities and products include fully integrated digital terrain elevation data (DTED)-/digital feature analysis data (DFAD)-based system maps, integrated Oilstock mapping application, integrated Joint Deployable Intelligence Support System (JDISS), communications support via Ethernet, transmission control protocol/internet protocol (TCP/IP), and asynchronous/synchronous serial. Automatic conversion of selected messages to TACREPs, based on MIL-STD 6040, USSID-369, and IEW COMCAT standards, validates all fields rather than selected fields of each message type and parses communications intelligence (COMINT), electronics intelligence (ELINT), measurement and signature intelligence (MASINT), HUMINT, and IMINT messages. Interactive COMINT and ELINT correlators, and Office automation tools complete the ASAS-SS software application. The Sysadmin/Server module and communications/firewall module are housed in shelters mounted on HMMWVs. Depending upon the echelon assigned, up to two light medium tactical vehicles (LMTV) and three cargo trailers provide lift for workstations and peripheral devices. ASAS Fusion and IMINT associated laptops use the UNIX-based Tadpoles or Bull Frogs laptops. Collection management, SIGINT, and HUMINT positions are supported by laptops and desktops, which are a combination of Panasonic Toughbook, Tadpole or Bull Frog laptop computers, or even Dell desktop systems running Windows XP. Depending upon the echelon, up to two fusion shelters mounted on HMMWVs are assigned to the ACE. Each houses two UNIX-based Intel shared servers (Sun Fire V480/490 server with two 73 GB hard drives and a Sun StorEdge 3310/3320 with twelve 147 GB hard drives using the Sun Solaris 2.8 OS in 64-Bit Mode and Oracle 8.1.7.4. RDBMS, along with a Trusted Workstation (Tadpole) and a desktop Dell single-source workstation. A Fusion Support Shelter, also mounted on a HMMWV, contains various Tadpoles and Bull Frogs that make up the Trusted Guard suite along with an optional Tactical Exploitation range instrumentation systems (RIS) server. The client side of the ACE-AFS configuration consists of 1-16 ASWS laptops fielded on the Tadpole 6500 platform with 30 GB hard drives. The laptops run either Unix or Windows XP operating environment. The ASWS may also be fielded on the Tadpole VigraBook.

**POWER SOURCE—**Power is supplied by two generators—a 15 kW and either a 30 kW or a 60 kW.

**OPERATOR/MAINTAINER—**35F, 350F, 35N, 352N, 35L/M, 351L/M, 35G, 350G, 35T.

**STATUS—**ASAS ACE is an ASAS Block II program under the direction of the program manager for Intelligence Fusion.

## JOINT DEPLOYABLE INTELLIGENCE SUPPORT SYSTEM (JDISS)

**SYSTEM SUMMARY**

| FEATURES— | TABULATED DATA— |
|---|---|
| • Accesses theater, Service, and national intelligence databases. | • Software—UNIX OS. |
| • Transmits (TX) and receives (RX) specific requests for intelligence. | • Hardware—CHS II. |
| • Supports digitized imagery exchange. | • Power—110-240 VAC, 3-phase, 60 Hz, and 28 VDC. |
| • Accesses automated record message processing systems, indications and warning (I&W) systems, and collection management systems. | |
| • E-mail/chatter. | |
| • Word processing and message generator. | |
| • Imagery manipulation. | |
| • Communications interfaces/map graphics. | |
| • Briefing tools/utilities. | |
| • Multimedia applications—desktop video and voice, voice electronic publishing, and video teleconferencing. | |

**Figure J-8. Joint Deployable Intelligence Support System**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Joint Deployable Intelligence Support System (JDISS).
**FUNCTION—**The JDISS allows for connectivity and interoperability with the intelligence systems needed to support forces in an operational environment. It provides the joint intelligence center (JIC), joint task force (JTF), and operational commanders with the automation support and the connectivity necessary to execute the intelligence mission. JDISS supports Army, Air Force, Navy, and Marine Corps commanders.
**DESCRIPTION—**JDISS is a non-developmental (NDI), unit-purchased, Government-off-the-shelf

(GOTS) desktop computer and set of applications that provide the deployed joint task force (JTF) commander critical intelligence support to combat operations. It provides timely, secure, direct access to theater and national intelligence assets, as well as standard office automation and support functions. It consists of an integrated set of COTS software including word processing, e-mail, chatter, graphics, imagery manipulation, and remote database access. JDISS supports the unit's intelligence mission in garrison as well as during forward-deployed operations. The small physical profile of the system makes it ideal for operations requiring tailored, deployable intelligence support elements. The system comes without dedicated transport or operators; therefore, units must incorporate into their SOPs the necessary provisions for who will operate the system and how it is to be deployed.

**POWER SOURCE—**110- to 240-VAC, 60 Hz power is provided by commercial power or unit-owned power generation equipment.

**OPERATOR/MAINTAINER—**35F, 35L, 35M.

**REFERENCES—**JDISS Joint Program Office web pages.

**STATUS—**U.S. Navy POR.

## Counterintelligence and Human Intelligence Automated Reporting Collection System

**SYSTEM SUMMARY**

| FEATURES: | |
|---|---|
| • Provides mission automation CI/HUMINT collection, interactive analytical, report writing, dissemination, and asset management tools. | • The current CHARCS system (Increment 1) provides HUMINT and CI collectors with the ability to collect, analyze, and report intelligence information. Although the current system provides robust reporting capabilities, OIF experience has identified a gap in the capability to fully exploit CI and HUMINT collection opportunities. The current CHARCS system will interface with a number of communication systems, but has no communication system of its own. |
| • Provides seamless linkage for the flow of CI/HUMINT data to and from tactical, strategic, and Joint/National levels. | • CHARCS is accredited to operate at the SECRET level. |
| • The CHARCS family of systems comprises the following--Counterintelligence and Human Intelligence Automated Reporting Collection System (CHARCS), Team Leader Set, Individual Tactical Reporting Tool (ITRT), Collection-Peripherals, Sets, and Kits (C-PSK), and mission specific PSKs. | • Future Capability (Inc 2) - Mission Specific PSKs issued 1 per OMT, Biometric PSK, CHDDD PSK, DOMEX PSK. |

**Figure J-9. Counterintelligence and Human Intelligence Automated Reporting Collection System**

**NOMENCLATURE—**Counterintelligence (CI) human intelligence (HUMINT) automated tool set (CHATS), AN/PYQ-3(V)3; Individual Tactical Reporting Tool (ITRT), AN/PVQ-8; and collection peripherals, sets, and kits (C-PSK).
**PROJECT NAME—**Counterintelligence (CI) and Human Intelligence (HUMINT) Automated Reporting Collection System (CHARCS).

**FUNCTION—**CHARCS primary purpose is to allow commanders to connect to communications devices for immediate transmission of CI and HUMINT intelligence reports and to receive tasking and requests for information (RFI). CHATS also provides CI and HUMINT personnel the ability to gather and maintain intelligence and rapidly transmit and receive information via electronic means. The ITRT is the entry-level device into the CHARCS architecture. Its primary function is to report intelligence of immediate tactical value to other CHARCS for the commander. The C-PSK enhances the collection and reporting capability of the CI and HUMINT teams.

**DESCRIPTION—**A complete CHARCS configuration consists of CHATS, ITRT, and C-PSK. The numbers of each component depend on the distribution, composition, and echelon of engagement. The CHARCS team kit bag comprises a digital camera, digital video camera, digital voice recorder, global positioning system (GPS) with maps, biometrics collection device, two mini-USB thumb drives (1GB each), infrared mark-light strobe (four per kit), and a pelican case with cut foam. The CHARCS team leader set comprises a 19" flat panel monitor; all-in-one printer, scanner, copier; full size keyboard, and an optical mouse.

- **CHATS—**commercial-off-the-shelf (COTS) equipment housed in three airline-approved carrying cases(two hard and one soft). (See figure J-9.)CHATS two subsystems are:
  - Hardware—laptop computer with internal power-management capability, printer, scanner, digital camera, secure telephone, cables and adapters to ensure ease of use in different environments. Hardware turnover occurs every three years to accommodate technology updates.
  - CHATS all-source integration system (CHASIS) software—consists of Windows 95 software and includes other COTS software applications such as Microsoft Plus/Office PRO 95, Quarterdeck PROCOMM Pls, NETSCAPE Navigator, Photosuite V 8.0, Pagescan V.1.2, Photoenhancer V.2.1, Hardlock V.4.1, Norton Utilities, and WINZIP. In addition, government-developed CI and HUMINT utilities provide mission-specific functionality.
- **ITRT—**COTS. (See figure J-10.)

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • The ITRT is the entry-level device into the CHARCS architecture. Its primary function to report intelligence of immediate tactical value to other CHARCS for the commander. | • The ITRT provides CI and interrogation Soldiers with the capability to collect, process and disseminate intelligence information obtained through investigations, interrogations, collections, operations, and document exploitation. |

**Figure J-10. Individual Tactical Reporting Tool, AN/PVQ-8**

**C-PSK—**Assortment of tools that enhances CI/HUMINT team collection and reporting capability; tools include digital imaging, biometric collection, document and media exploitation. (See figure J-11.)

**Figure J-11. Collection Peripherals, Sets, and Kits**

**CAPABILITIES—**CHARCS provides CI and HUMINT collection teams (HCT)automated capabilities to collect, report, and answer the commander's intelligence requirements, particularly with respect to high-value individuals and high-value targets. Provides CI and HUMINT collection teams increased capability to disseminate information and intelligence products at point of collection via

beyond-line-of-sight communications. Supports protection, interrogation operations, document and media exploitation (DOMEX), and source operations. Enhances the commanders ability to anticipate and react to a wide range of threats and situations. The basis of issue for the CI team and HCT is one each CHARCS, two each ITRTs, one each C-PSK, and one team leader set. The operational management team is issued one each CHARCS and mission-specific PSKs.
**OPERATOR/MAINTAINER—**Operators: counterintelligence (35L, 351B, 35E) and HUMINT collector (35M, 351B, 35F); maintainer: field support representatives.
**STATUS—**POR.

## Tactical Exploitation System-Forward

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • SIGINT processing and correlation. | • Moving target indicators (MTI) from Joint STARS, U2 and Global Hawk. |
| • National and theater imagery products. | • Receives Predator and other UAS feeds. |
| • Tracks 200 signals of interest (SOIs). | • Global Broadcast Service (GBS)-enabled. |
| • Tracks 500 active and 1,000 inactive imagery targets. | • Organic communications (Trojan Lite). |

**Figure J-12. Tactical Exploitation System-Forward, AN/TSQ-219(V1)**

**NOMENCLATURE—**Tactical exploitation system-forward, AN/TSQ-219(V1).
**PROJECT NAME—**Tactical exploitation system-forward (TES-F).
**FUNCTION—**TES-F is a SIGINT and IMINT processing system that incorporates a cross-discipline integration, cueing, and data presentation work environment to produce intelligence products providing critical intelligence to commanders.
**DESCRIPTION—**TES-F is able to receive, process, exploit, store, and disseminate imagery from the national sources, the U2, Predator UAV, Global Hawk (electro-optical (EO)/synthetic aperture radar (SAR)/MTI), shared reconnaissance pod (SHARP) sensor, F-16 gun camera, Joint STARS MTI and fixed target indicators (FTI), and selected commercial imaging satellites. It also receives, processes, exploits, stores, and disseminates SIGINT from national sources and the IBS network. The organic Trojan Lite and GBS receiver suite provides the TES-F with high data rate receive and broadcast capabilities. TES-F consists of six HMMWVs containing ten UNIX and five PC workstations for SIGINT and IMINT analysis. A digital "library" allows supported entities to retrieve the data at a time convenient to them. TES-F tracks up to 200 SOIs and up to 500 active and 1,000 inactive imagery targets. It uses a peer-to-peer (P2P) architecture to allow the dissemination of intelligence products and collaboration of analysts between systems and echelons. TES-F is a deployable, highly-flexible modular system configured to provide the commander the option to use split-base operations. It provides quick set up and tear down for rapid deployment and drive-on and drive-off capability on the C-130 military aircraft. Set-up time for TES-F is two hours. TES-F uses common hardware and software and standard protocols compliant with DOD and national architectures to support joint and combined operations.
**CAPABILITIES—**TES-F is the objective tactical exploitation of national capabilities program (TENCAP) preprocessor for national and theater SIGINT and IMINT data.
**OPERATOR/MAINTAINER—**35G, 35N, 35T, 350G, 352N, 353T, 35B, 35C. Operators and maintainers must attend the TES analyst course.
**STATUS—**DCGS-A-enabled POR.

## Distributive Tactical Exploitation System

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • SIGINT processor and correlator. | • Receives MTI, FTI, and SAR data directly from Joint STARS or over the LAN. |
| • National and theater imagery products. | • Receives data over the organic Low Cost S-Band Receiver (LSR). |
| • Receives the IBS. | • Receives video over GBS receiver suite. |

**Figure J-13. Distributive Tactical Exploitation System, AN/TSQ-219(V3)**

**NOMENCLATURE—**AN/TSQ-219(V3).
**PROJECT NAME—**Distributive-Tactical Exploitation System (D-TES).
**FUNCTION—**The D-TES is a division-level intelligence system that receives, processes, exploits, and disseminates intelligence data from Joint STARS (MTI and FTI data), UAS full motion video (FMV), relayed SIGINT and MASINT products via IBS, TES-F, and National Mission Ground Stations (MGSs) using the Low-Cost S-Band Receiver (LSR), and Imagery-Derived Products (IDPs) through SIPRNET, JWICS, and GBS. The D-TES can be augmented with TES-F components to increase its capability. The D-TES has the same operational, communications, and support capabilities as the TES-F node.
**DESCRIPTION—**The D-TES comprises two HMMWV-enhanced capability vehicles (ECV) mounted with Wolf Coach modified Gichner (GSS-1497) shelters. The D-TES consists of only the FCV, Gen30, and RET. This repackaging effort will allow the D-TES to operate at the SECRET Collateral level only, reducing the transportation requirements and providing a smaller operations footprint. The D-TES has an organic GBS receiver suite and a LSR. The D-TES communications subsystems connect to other nodes of the TENCAP and intelligence communities. It incorporates a UHF SUCCESS DAMA radio, a TCSP for connection to AUTODIN (R and Y routers). The DMS Server interfaces with the DMS, STE, MSE, and other Defense and intelligence communications networks. The D-TES also has an organic LSR to receive unexploited products from national MGSs. The D-TES has integrated an organic GBS suite for receiving large data files such as National or commercial imagery, and topographic products. D-TES has two UNIX and two PC workstations; it can support up to a total of six. The D-TES components and multi-function workstations (MFWS) are synchronized to the GPS for the time and geographical accuracy. The D-TES MFWSs are the interface in which the operator performs functions including SIGINT analysis, mission management, dissemination, and fault detection/fault isolation (FD/FI). Each MFWS is packaged in two transit

cases and is easily detached for transport between the D-TES shelters and a remote TOC. The MFWSs are remotely connected to the shelters via the RNB. The MFWS can be located up to 100 ft. from the forward communications vehicle (FCV) and communications support vehicle (CSV) shelters. The keyboard, video, and mouse (KVM) switch transmitter and receiver interfaces to the remote distribution nodes (RDN) with the system servers for remote control of the servers. The RDNs can be located up to 100 ft. from the FCV and CSV shelters. An uninterruptible power supply (UPS) is integrated into the MFWS central processing unit (CPU) transit case to provide emergency backup power in case of power failure and to perform a safe shutdown of the MFWS CPU. The on-the-move (OTM) operations capability enables the operator to receive, display, and update the system database via a notebook computer mounted in the FCV cab. The OTM notebook running Gale Lite (SIGINT) and Remote View (IMINT), and cross-intelligence disciplines enable the operator to correlate and display SIGINT data and to receive SIDS data received via the UHF radio. The SUCCESS DAMA UHF radio operates in the receive mode and transmits on one link. The UHF radio receives UHF signals such as IBS, Record Message Traffic (RMT), and IDPs. It also transmits RMT and IDPs via the Hemispheric UHF Antenna. The FCV can process and display IBS, RMT, and IDP products while OTM. For OTM operations, the Hemi Antenna is mounted on the front of the shelter, providing UHF signals reception. The operator uses the OTM notebook running Gale Lite and Remote View to store and process the data received for transfer into the system server databases once the FCV is set up for normal operations. OTM power is provided by a 400A alternator mounted in the engine compartment and is connected to the HMMWV's battery. Two 24-VDC to 120-VAC power inverters provide the power conversion to operate the modified AC unit, UHF radio (1 link transmit), limited crypto, TCSP, printer, KY-99, modems, system server (SS) #2 w/RAID, Interop Server, DMS Server, router, OTM hub and the OTM notebook during OTM operations. UPS protection is provided for the equipment during OTM operations. No other system equipment is operated during OTM operations including the MFWS and RDN.

**CAPABILITIES—**The D-TES controls and supports exploitation by handling cross-cues from SIGINT/IMINT/MTI and other sources of SIGINT data. D-TES employs an imagery exploitation package and is capable of formatting all images into NITF 2.0/2.1 format for storage and dissemination. System Server #2 has integrated Ethernet (10BaseT—10 Mbps), and Fast Ethernet (100BASE-X—100 Mbps) data ports. Internal to the server is an 8-mm tape drive for uploading software updates. The SS #2 provides an interface port supporting X.25 and TCP/IP transmission protocols.

**POWER—**Vehicle-generated power.

**OPERATOR/MAINTAINER—**35G, 35N, 35T, 350G, 352N, 353T, 35B, 35C. Operators and maintainers must attend TES analyst course.

**STATUS—**DCGS-A-enabled POR.

## Tactical Exploitation System-Lite

**SYSTEM SUMMARY**

| FEATURES— | |
|---|---|
| • SIGINT processor and correlator. | • Receives MTI data over LAN. |
| • National/theater imagery products. | • Receives data over the organic Low Cost S-Band Receiver (LSR). |
| • Receives the IBS Broadcast. | |

**Figure J-14. Tactical Exploitation System-Lite, AN/MSW-24**

**NOMENCLATURE—**AN/MSW-24.
**PROJECT NAME—**Tactical Exploitation System-Lite (TES-L).
**FUNCTION—**The TES-L provides timely intelligence and information in support of tactical operations, terrain and obstacle analysis, target development and acquisition, and post-strike combat assessment to tactical commanders in multiple areas of interest. The TES-L supports the commander in executing battle command functions and planning future operations across the full spectrum of conflict. The TES-L provides processed imagery (IMINT), processed MASINT, and SIGINT data to the supported echelon or element. It utilizes SIGINT, IMINT, and MASINT data and products internally for multidiscipline analysis.
**DESCRIPTION—**The TES-L is a portable workstation utilizing a UNIX and PC baseline. The D-TES consists of two HMMWV, ECVs, mounted with Wolf Coach modified Gichner shelters. The D-TES consists of only the FCV, Gen30, and RET. This repackaging effort will allow the D-TES to operate at the SECRET Collateral level only, reducing the transportation requirements and providing for a smaller operations footprint. The TES-L is a highly mobile, scalable, and modular intelligence processing system capable of receiving, processing, exploiting, analyzing, and disseminating preprocessed national (TENCAP) and selected theater and organic data, to include imagery-derived products in a timely manner for tactical commanders and other users at Division and below. The TES-L is a module of the TES enhanced to meet the additional requirements unique to lower echelons such as ACRs, Separate Brigades, and Army Special Operations Forces Regiments or Groups. The TES-L communications subsystems connect to other nodes of the TENCAP communities, but only at the collateral level. The TES-L incorporates a UHF embedded receiver to receive the IBS broadcast. The DMS Server provides the interface to the DMS. The TES-L components and workstation is synchronized to the GPS for the time and geographical accuracy. The TES-L System Server hosts the SIGINT processing and provides support to the workstation clients for overall control of the UHF receiver, as well as planning, mission monitoring and control, exploitation, and FD/FI. A small, SECRET Collateral Imaging storage capability is hosted in the system with four GB of RAM, and

two 36 GB hard drives. The TES-L controls and supports exploitation by handling cross-cues from SIGINT, IMINT, and other sources of SIGINT data. TES-L employs an imagery exploitation package and is capable of formatting all images into NITF 2.0 format for storage and dissemination. The system server has integrated Ethernet (10BaseT—10 Mbps), and Fast Ethernet (100BASE-X—100 Mbps) data ports. The system server provides an interface port supporting X.25 and TCP/IP. The TES-L multi-function workstation (MFWS) are the interface in which the operator performs functions including SIGINT analysis, mission management, dissemination, and FD/FI. The TES-L is packaged in two transit cases and is easily detached for transport between the D-TES shelters and a remote TOC. The MFWSs are remotely connected to the shelters via the RNB. The MFWS can be located up to 100 ft from the FCV and CSV shelters. The KVM switch transmitter and receiver interfaces the RDN with the system servers for remote control of the servers. The RDNs can be located up to 100 ft from the FCV and CSV shelters. A UPS is integrated into the MFWS CPU transit case to provide emergency backup power in case of power failure and perform a graceful shutdown of the MFWS CPU. On-the-move (OTM) operations capability enables the operator to receive, display, and update the system database via a notebook computer mounted in the FCV cab. The OTM notebook running Gale Lite (SIGINT) and Remote View (IMINT), and cross-intelligence disciplines enables the operator to correlate and display SIGINT data and to receive SIDS data received via the UHF radio. The SUCCESS DAMA UHF radio operates in the receive mode and transmits on one link. The UHF radio receives UHF signals such as IBS-S and IBS-I, RMT, and SIDS. It also transmits Record Message Traffic and SIDS via the Hemi Antenna. The FCV can process and display IBS, RMT, and SIDS products while OTM. For OTM operations, the Hemi Antenna is mounted on the front of the shelter providing UHF signals reception. The operator uses the OTM notebook running Gale Lite and Remote View to store and process the data received for transfer into the system server databases once the FCV is set up for normal operations. OTM power is provided by a 400A alternator mounted in the engine compartment and is connected to the HMMWVs battery. Two 24-VDC to 120-VAC power inverters provide the power conversion to operate the modified AC unit, UHF radio (one link transmit), limited crypto, TCSP, Printer, KY-99, modems, SS #2 w/RAID, Interop Server, DMS Server, router, OTM hub and the OTM notebook during OTM operations. UPS protection is provided for the equipment mentioned above during OTM operations. No other system equipment is operated during OTM operations including the MFWS and RDN.

**CAPABILITIES—**The TES-L receives SIGINT information using the ENTR. The SIGINT information is broadcast from National (IBS-S) or theater (TIBS-I). The TES-L operator sets filters within the ENTR radio, filtering out messages that do not pertain to the commander's PIR. Once data is received over the broadcast through the receiver, the operator can set parsing instructions to either store data in the database; display data on the monitor; or immediately resend the message to ASAS or other ABCS terminals, or a combination of all these features. The value-added is that the TES-L correlates messages of similar parameters, either manually or automatically, reducing the message flow to ASAS and other IEW and ABCS systems. The organic LSR can also be used to receive unexploited SIGINT data for integration into the TES-L database. Once received, the data can be exploited supporting the units' mission. The TES-L receives imagery through the LAN. The operator pulls imagery into the system and begins the exploitation process. Products from exploitation are either IDP or an IPIR, or both, and they are disseminated in several ways. During the exploitation phase, the analyst has the capability to overlay SIGINT data on the image to assist in exploitation. The analyst also has the basic exploitation software necessary to exploit handheld or airborne imagery. The organic LSR can also be used to receive unexploited IMINT data for integration into the TES-L database. Once received, the data can be exploited supporting the units' mission.

**POWER—**Power is provided by the vehicle.

**OPERATOR/MAINTAINER—**35G, 35N, 35T, 350G, 352N, 353T, 35B, 35C. Operators and maintainers must attend the TES analyst course.

**STATUS—**DCGS-A-enabled POR.

# Appendix K

# Communications and Communications Support Systems

## INTRODUCTION

**K-1.** Communications networks and information services enable joint and multinational warfighting capabilities (JP 6-0). This appendix is an overview of the principal communications systems used to support Army intelligence. It also contains details on a number of the communications and communications support systems outlined briefly below. The more detailed descriptions contain the name of the system, picture of the system (where available), system summary, function and description of the system, its power source, what personnel operate and maintain it, references to the sytem, and the status of the system in the acquisition chain.

### Army Communications Framework

**K-2.** The following is an overview of the Army Commun User System (ACUS), combat network radio (CNR), and aviation digital data service (ADDS). Together, these systems provide the Army communications support to Army Battle Command System. Along with the joint communications systems, they provide the framework for joint and Army split-based intelligence support to forward-deployed combat forces.



#### Army Common User System

**K-3.** The ACUS is a multi-user, common-user area system for high-volume command and control, operations, intelligence, administrative, and logistics communications. It consists of a series of nodal switching centers in a grid-like network connected by terrestrial line-of-sight (LOS) multichannel radio systems. ACUS provides an integrated switching system from battalion through theater Army or task force (TF) headquarters. It also provides interface points with access to strategic and sustaining base environments.

#### Mobile Subscriber Equipment

**K-4.** MSE is the backbone of the ACUS communications system at the corps and division levels. It is the primary system supporting analysis and control element (ACE) operations and all-source analysis system (ASAS) connectivity outside the corps or division TOC. By providing digital communications from the corps sustainment area forward to the maneuver battalions, MSE extends the ASAS systems interoperability from theater Army or TF headquarters to forward combat information collectors. MSE communications include telephone; facsimile, mobile radiotelephone, data transmission, and CNR network access. In addition, MSE normally operates at security level capable of handling transmissions no higher than the SECRET collateral level. However, communications at security classification levels as high as sensitive compartmented information (SCI) are possible with the use of an additional communications security (COMSEC) variable applied through a digital subscriber voice terminal (DSVT):

- CCS connects to the MSE network through a force entry switch, SEN or an LEN. Network access is established from a DSVT via wireline through a J-1077 junction box at the CSS. The incoming MSE signal is initially routed into the communications control set (CCS) where communications software converts it into a compatible protocol format.
- After conversion, all messages are automatically routed to the appropriate workstation or database based on PLAs and RIs applied to each message.

### Combat Net Radio

**K-5.** The CNR provides a secondary means of data communications for the CCS. It covers a broad spectrum of single-channel radio systems used for immediate command and control (C2). The CNR architecture consists of VHF FM radios, HF AM radios, and UHF TACSAT systems. The CNR systems are designed to meet the requirements of speed, reliability, and security on the battlefield.

### Improved High Frequency Radio

**K-6.** IHFR is the family of secure tactical HF AM radios replacing systems such as the AN/PRC-7, AN/GRC-165, and the AN/GRC-106. The IHFR extends and complements VHF FM communications networks in the corps and division. The IHFR is configured as the AN/GRC-193A (vehicular), AN/GRC-213 (man-pack or vehicular), and the AN/PRC-104 (man-pack). Beginning with ASAS Block II, the CCS will be capable of IHFR communications:

- **SINCGARS—**The Single Channel Ground and Airborne Radio System (SINCGARS) is the family of VHF FM radios that have replaced older FM radio equipment on a one-for-one basis. It provides secure voice and data transmission, a broad frequency spectrum and a frequency-hopping capability. With an integrated COMSEC capability, it secures data to the SECRET level and provides low probability of intercept when operated in the frequency-hopping mode. The CCS contains four SINCGARS transceivers operated in the single-channel mode for both voice and data communications. These radios are primarily used for voice and data communications with supporting ISR assets. If necessary, they can provide access to the MSE network or, if the MSE is not available, provide an alternate means of data communications to support ASAS.
- **TACSAT—**The TACSAT (AN/TSC-85B and AN/TSC-93B) provides secure long distance SHF voice and data SATCOM. It can interface and provide an internodal link between widely separated MSE node centers or a gateway link between NCSs. The system provides a communications link with higher echelons or forward elements to support ASAS operations in a split-based environment.
- **ADDS—**The ADDS is an integrated C2 communications system providing NRT transmission capabilities to support high volume data networks. In addition, it provides precise position, location, navigation, identification, time of day, and reporting information for units on the battlefield. ADDS meets the needs of the users for a high speed, high volume, secure communications system to convey sensor traffic for evaluation and firing data for target engagement. The system is secure, jam-resistant, and automatically relays data in a manner that is transparent to the user. The EPLRS, MPN, and the AFATDS are examples of ADDS.
- **EPLRS—**The CCS will eventually support an Enhanced Position Location and Reporting System (EPLRS) capability. The EPLRS is a computer-based communications system designed to provide secure, jam-resistant, contention free, NRT data transmission, and distribution to a wide array of subscribers. In addition, it provides unit identification, navigational aids, and automatic location reporting of tactical units. The EPLRS uses integral dual-level (CONFIDENTIAL and SECRET) COMSEC with over-the-air rekeying, frequency-hopping, and error correction encoding as protection from EA.

### Defense Communications System

**K-7.** The DCS is a composite of certain DOD communications systems and networks. The system provides long distance, point-to-point, and switched network telecommunications. The DISA provides centralized management for C2 systems of the DCS. The Army Signal Command is the Army's executive agent for DISA. The communications networks supported by DISA are discussed below:

- **DSN—**The DSN is the principal common user, switched, nonsecure voice communications network within the DCS. It consists of a worldwide network of commercial leased and government-owned facilities. Tactical DSN subscribers normally gain access through the TCS using the AN/TTC-39 circuit switch. The TCS provides circuit or message switches and direct access to many worldwide DOD networks.
- **DISN—**DISA consolidated the DDN packet switched networks under the DISN. DISN provides DOD worldwide packet switched data communications through three separate networks.

Consolidation of these networks was accomplished by converting all service and agency multiplexer networks to the same hardware base. While the specifics of the consolidation vary between DISA and the various router network managers, DISA is centrally operating at least two worldwide IP networks. One network is for sensitive but unclassified information known as the NIPRNET, while the other is for SECRET Collateral information and is known as SIPRNET. In addition to NIPRNET and SIPRNET, DISA also operates a data communications "back-bone" network known as the DATM network. DATM is intended to provide unclassified and classified computer networking service for official DOD business. DATM is designed to accommodate data, video, and voice traffic simultaneously and to provide the various levels of service required for each type of data.

### Automatic Digital Network

**K-8.** AUTODIN is the DOD common user store-and-forward message-switching network for all record message traffic. It consists of a network of fixed and mobile ASCs and AUTODIN communications centers. The current AUTODIN system evolved from the consolidation of the DSSCS with the GENSER AUTODIN system in the mid-1970s. While the two independent systems have been merged, each system has retained its own identity and mission functions. GENSER AUTODIN (referred to as the "R" side) handles UNCLASSIFIED through TOP SECRET record message traffic including SPECAT type messages. DSSCS AUTODIN (referred to as the "Y" side) handles record message traffic containing SCI information. DISA is replacing the aged and inefficient AUTODIN with the modern e-mail based DMS.

### Defense Message System

**K-9.** DMS supports two classes of messages—organizational messages (formal record messages) and individual messages (informal e-mail). Its distributed message system supports online message preparation, coordination, and release of organizational messages. The DMS will replace the centralized AUTODIN message system, the DISN e-mail components, and the formats and procedures of the current message distribution baseline.



### Department of Defense Intelligence Information System

**K-10.** DODIIS is the DIA managed program that incorporates the DISN secure networks under a single architecture. DODIIS defines the standards for intelligence systems and applications interoperability. In addition, it provides an integrated strategic to tactical user environment for performing identical intelligence functions on compatible systems. The system's primary components include the SIPRNET, JWICS, and JDISS:

- **SIPRNET—**SIPRNET has matured to be the core of our warfighting C2 capability. Many expeditionary commanders ask for SIPRNET ahead of secure voice when deploying their forces. SIPRNET is fast becoming the de facto standard of preferred data services, even over NIPRNET. The SIPRNET is the new, worldwide router-based network replacing the older X.25-based packet switched network (DSNET1) of the DDN. The initial SIPRNET backbone router network went online 3 March 1994. Subscribers started coming online shortly thereafter. The SIPRNET WAN (as of 31 May 1995) consisted of a collection of 31 backbone routers interconnected by high-speed serial links to serve the long distance data transport needs of SECRET-level DOD subscribers. Additional SIPRNET backbone routers are being planned to meet increased customer requirements. SIPRNET supports the DOD standard TCP/IP protocol service. Subscribers within the DOD and other government agencies are able to use the SIPRNET for passing datagrams at the SECRET-NOFORN classification level.
- **WICS—**JWICS is a 24-hour-a-day network designed to meet the requirements for secure (TS/SCI) multimedia intelligence communications worldwide. JWICS replaces the DDN DSNET3 as the SCI component of the DISN. It provides DODIIS users an SCI level high-speed multimedia network using high-capacity communications to handle data, voice, imagery, and graphics.
- **SPECIAL PURPOSE INTELLIGENCE COMMUNICATIONS—**The following describes the special purpose intelligence communications systems supporting Army ISR operations.

These systems provide intelligence organizations the dedicated and flexible intelligence communications needed to support commanders across the range of military operations.

### Broadcast Systems

**K-11.** A number of broadcast systems support the dissemination of tactical intelligence to commanders at multiple echelons. These systems are usually designed to "push" formatted, time-sensitive information to tactical commanders. The information includes multi-sensor national and theater ELINT and imagery-derived data as well as multi-source fused threat force disposition information. (See figure K-1.) These broadcast systems include—

- Integrated broadcast service-simplex (IBS-S).
- IBS-interactive (IBS-I).
- IBS-LOS.

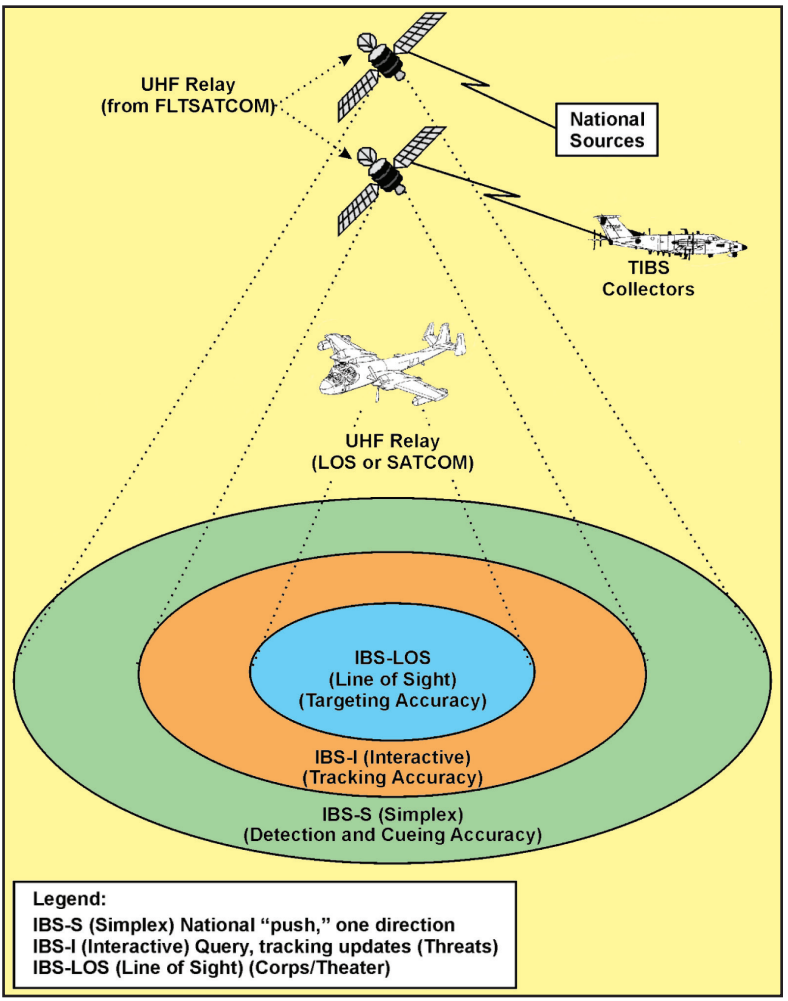



**Figure K-1. Intelligence coverage for UHF broadcast dissemination**

## Joint Tactical Terminal

**K-12.** The JTT is a family of special-application UHF tactical intelligence terminals which provide the capability to disseminate time-sensitive intelligence and battlefield targeting information to tactical commanders. This information is provided in NRT and allows selected collection managers at all echelons a full-duplex capability to dynamically request adjustments to pre-planned tasking. The JTT is integrated in the CCS, the common ground station (CGS), and the Guardrail IPF.

### TROJAN Data Network

**K-13.** The TDN is an internet protocol (IP)-based network that facilitates the exchange of intelligence information among tactical, operational, and strategic intelligence organizations. The TDN is subdivided into three electronically and physically separated networks that correspond to the type and security levels of the information they handle. The TDN is administered by the TROJAN Network Control Center located within the TROJAN Switch Center at Fort Belvoir, VA, and provides configuration control and network management. The three networks of the TDN are:

- **TDN-1.** TDN-1 operates at the SECRET collateral security level and is the gateway to the SIPRNET. It provides data exchange between TROJAN Classic facilities, switch extension, SPIRITs, and other users of the SIPRNET intelligence network.
- **TDN-2.** TDN-2 operates at the TOP SECRET/SCI level. It provides access between selected TROJAN sites and the NSA computer network known as NSAnet.
- **TDN-3.** TDN-3 operates at the TOP SECRET/SCI security level and serves as the gateway to the JWICS computer network.

### TROJAN Special Purpose Intelligence Remote Integrated Terminal II

**K-14.** The AN/TSQ-190(V), TROJAN SPIRIT II, is a corps and division asset that provides dedicated intelligence communications. The TROJAN SPIRIT II is a shelter mounted on two heavy HMMWVs that serves as a tactical mobile switch extension of the TDN. The system is capable of supporting ASAS communications connectivity by providing access to TDN-1, TDN-2, MSE, TPN, and LAN communications support. This capability allows the TROJAN SPIRIT II to serve as a temporary communications set for the ACE during redeployment and split-based operations.

## TROJAN CLASSIC

**SYSTEM SUMMARY**

| | |
|---|---|
| • COMINT intercept collection. | • Interfaces with ASAS and deployed TROJAN Spirit II systems. |
| • Fixed-site, garrison-operated. | • ISR range—Worldwide. |
| • Remotely controlled front-end connectivity. | • Frequency range—HF, VHF, UHF. |
| • Robust communications suite for worldwide TROJAN connectivity. | • Power—115-VAC, 3 phase, 60Hz, and 28 VDC. |

**Figure K-2. TROJAN Classic, AN/FSQ-144**

**NOMENCLATURE—**AN/FSQ-144.
**PROJECT NAME—**TROJAN Classic.
**FUNCTION—**The TROJAN Classic is a fixed facility, operational readiness COMINT intercept, processing, and dissemination system.
**DESCRIPTION—**The TROJAN system includes, but is not limited to, SIGINT collection facilitated by the RCF, COF, and switching center. The TROJAN Classic consists primarily of the following major elements—

- RCF—Data collection for the TROJAN mission is initiated at the remote communications facilities (RCFs) by the remote receiver group (RRG). RRGs are unmanned systems located in secure facilities worldwide. INSCOM TROJAN mission management personnel located in Army technical control and analysis element (TCAE) or echelons above corps (EAC) TCAE organizations control the RRGs.
- Central operations facility—A TROJAN COF provides the storage, control, and analysis capabilities for the TROJAN system.
- Monitor control groups—MCGs are located in COFs at secure MI unit garrison facilities. Each COF consists of four collection positions, four listening posts, an SSC, and associated communications equipment.
- TROJAN Switching Center at Fort Belvoir, VA—TROJAN global communications are focused at the TROJAN switching center, which creates a path between data sources and users of that data.
- Switch extensions—Switch extensions are located in SEF worldwide.

The commander's intelligence requirements drive the tasking of the TROJAN System. Advisory tasking from higher headquarters can be incorporated into the unit's tasking. Reporting is forwarded to the ACE for further dissemination.
**CAPABILITIES—**The AN/FSQ-144 TROJAN Classic is a non-deployable, fixed collection and

processing facility. Deployable associated TROJAN systems can be transported on C-130, C-17, and C-5 aircraft, maritime transport, rail, and unit-owned transportation. The TROJAN Classic has 24-hour mission availability; it is operated in a garrison, fixed-site environment. Associated TROJAN systems provide 24-hour mission availability in a tactical environment. The direct support/general support (DS/GS) maintenance for line replaceable unit (LRU) equipment is resident in supporting the MI unit maintenance section. DS/GS maintenance for contractor-furnished equipment (CFE) is provided by supporting theater maintenance personnel.

**OPERATOR/MAINTAINER—**Not MOS-specific, specialized training required, field service representatives (FSR).

**REFERENCES—**TM 32-5895-400-12&P.

**STATUS—**Fielded.

# TROJAN SPECIAL PURPOSE INTEGRATED REMOTE INTELLIGENCE TERMINAL II

**SYSTEM SUMMARY**

| | |
|---|---|
| • Rapidly deployable worldwide to support the warfighter. | • Frequency bands—C, Ku, and X. |
| • Quick erect, satellite auto-tracking antenna. | • Back-up communications—DSVT (MSE), UHF TACSAT (AN/PSC-5), INMARSAT-M Terminal, JTT. |
| • Robust communications: | • Aggregate data rate—1.2 kbps to 1.544 mbps (T1). |
| • 14 channels digital voice, data. | • Port data rate—50 bps to 512 kbps. |
| • FAX and video (6 collateral, 8 SCI). | • Geolocation Systems—GPS. |
| • Video teleconference (VTC). | • 2.4-meter SATCOM antenna mounted on a trailer. |
| • SID. | • 5.5-meter SATCOM antenna mounted on the X-band trailer. |
| • Heliborne slingload certified (CH-47/53). | |

**Figure K-3. TROJAN Special Purpose Integrated Remote Intelligence Terminal II**

**NOMENCLATURE**—AN/TSQ-190(V).
**PROJECT NAME**—TROJAN SPIRIT II.
**FUNCTION**—The AN/TSQ-190(V), TROJAN SPIRIT II, is an intelligence dissemination satellite terminal that provides access for intelligence processing and dissemination. The TROJAN SPIRIT II provides the commander with imagery, voice, data, e-mail, video transfers, and VTC capabilities. The TROJAN SPIRIT II combines the TROJAN data network (TDN) with mobile switch extensions to offer a worldwide, forward-deployed, quick-reaction reporting and analysis link. This corps and division asset provides dedicated intelligence communications that are intended to augment in-theater communications. It can conduct split-based, inter- and intra-theater operations through the spectrum of conflict.
**DESCRIPTION**—TROJAN SPIRIT II extends the current worldwide TROJAN fixed station architecture to the tactical intelligence force structure in a mobile configuration. TROJAN SPIRIT II is a communications, intelligence C2, and intelligence dissemination and processing system using commercial and DSCS SATCOM for vertical and horizontal intelligence information dissemination

and for accessing databases between echelons. It is mounted in an S-250 communications shelter carried on an M-1097 H-HMMWV, which will be replaced by the M1113 H-HMMWV. A trailer carries a 2.4-meter satellite antenna. A second HMMWV carries maintenance and mission support equipment. The system supports C2 operations for various unmanned aircraft systems (UAS). Processing includes voice at all classification levels and data with interfaces for operations with JWICS and SIPRNET to allow users access to national-level systems as well as vertical and horizontal interchanges of data. The LAN capability of the system allows the operating unit to build an operational information system that can provide direct exchanges of mapping, video, specialized intelligence products, imagery, weather, and a host of related intelligence systems. TROJAN SPIRIT II systems provide a communications interface with the following systems—The ACUS/MSE, MIES, ETRAC, TES, CGS, TRACKWOLF systems, GRCS IPF, CHATS, JOINT STARS CGS, JMICS, and ABCS. TROJAN SPIRIT II uses intelligence special communications systems available to the supported echelon. When necessary, TROJAN SPIRIT will use standard DOD worldwide communications networks, communications systems, architectures, protocols, and standard Army tactical communications equipment and procedures common to the echelon supported. The system comprises a primary HMMWV shelter (PHS) (9600 lbs., which includes the prime mover), a spare equipment and maintenance shelter (SEM) (9500 lbs., which includes the prime mover), a mobile antenna platform (MAP) (3,750 lbs.), and a mobile X-band satellite communications (SATCOM) trailer (10,700 lbs. A 5 ton truck is provided to pull the X-band trailer. The system also contains non-line item number components:

- 10 kw tunnel-mounted generator.
- Environmental control unit.
- Red processing equipment multiplexer, fully carded (DNE 2048AT-16), FIREBERD 6000M test set, TROJAN digital voice instrument (TSP-9100A), TEMPEST facsimile (KIV-7) COMSEC device.
- Analyst workstation group (P (AWG) with a UNIX workstation, a UNIX laptop, printer (DNE 9030T), and a color Postscript printer.
- Black Baseband processing equipment.

**CAPABILITIES—** The TROJAN SPIRIT II System (V)4 integrates data transfer, multiplex, encryption, and radio frequency (RF) transmission equipment. The system provides Defense satellite Communications System (DSCS) X-band in conjunction with the C- and KU-band commercial satellite capabilities. A moblile radio telephone (MRT)—digital cellular radio/international maritime satellite–mobile (INMARSAT-M)—is provided to assist in coordinating link establishmen and system line ups.

**POWER SOURCE—**The system requires 115 -VAC, 60 Hz power provided by system on-board tunnel generator, tactical power generators, commercial power, or other unit power generation equipment.

**OPERATOR/MAINTAINER—**Not MOS specific; specialized training required; field service representative (FSR).

**REFERENCES—**TM 32-5895-400-12&P.

**STATUS—**

# TROJAN SPECIAL PURPOSE INTEGRATED REMOTE INTELLIGENCE TERMINAL LIGHTWEIGHT INTELLIGENCE TELECOMMUNICATIONS EQUIPMENT (V)1



**SYSTEM SUMMARY**

| | |
|---|---|
| • Length—88 inches. | • Maximum EIRP (mid Band)—55.0 dBW or 65 dBW. |
| • Width—108 inches. | • Intelsat certification—Type G. |
| • Height—103.5 inches. | • Ku-Band Transmission frequency range—14.0 to 14.5 GHz. |
| • Cube—319.9 feet. | • Ku-Band receive frequency range—10.95 to 12.75 GHz. |
| • Weight—2156.8 pounds. | • System G/T (mid Band)—25.0 dB/K. |
| • C-Band transmission frequency range—5.850 to 6.425 GHz. | • Maximum EIRP (mid Band)—62.0 dBW or 71 dBW. |
| • C- Band receive frequency range—3.625 to 4.200 GHz. | • Intelsat certification—Type E1. |
| • System G/T (mid Band)—19.0 dB/K. | |

**Figure K-4. TROJAN Special Purpose Integrated Remote Intelligence Terminal Lightweight Intelligence Telecommunications Equipment (V) 1, AN/TSQ-226 (V)1**

**NOMENCLATURE—**AN/TSQ-226 (V)1.
**PROJECT NAME—**TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Intelligence Telecommunications Equipment (LITE) (V)1, TS LITE (V)1.
**FUNCTION—**TS LITE (V)1 provides secure voice and data intelligence dissemination capability for the brigade or battalion tactical operations center (TOC) with connectivity to the division or corps G-2, theater intelligence brigade (TIB), other TROJAN users, and National Agencies.

**DESCRIPTION—** The TS LITE (V)1 is a satellite communications system that serves as a lightweight, early-entry, fly-away communications means for the receipt, analysis and dissemination of near real time (NRT), time-sensitive critical voice and intelligence data. The TS LITE (V)1 is transported in 21 transit cases weighing 2000 pounds, complemented with a quick-erect segmented C-/Ku-band 2.4-meter SATCOM antenna mounted on a positioner assembly. The positioner assembly functions as an auto-tracking assembly when interfaced with the antenna control receiving unit (ACRU). Set-up and activation time, from time of arrival at the deployment site, is under 30 minutes. Employing commercial-off-the-shelf (COTS) SATCOM and networking equipment, this worldwide deployable system takes advantage of leased commercial C- and Ku-band transponder space and the TROJAN communications network infrastructure. TS LITE (V)1 has the following additional features:

- Classified local and wide area network (LAN/WAN) access—TDN 3 (JWICS); TDN 2 (NSANet); 10/100 BaseT Ethernet LAN, voice over internet protocol (VoIP) phone.
- Transit case configuration for rapid deployment.
- 64 kilobytes per second (Kbps) to 1,544 Kbps.
- 30-minute setup/teardown.
- Laptop computer for monitoring and control (M&C).
- KG-175D TACLANE Micro (secure COMSEC unit).
- Supportable worldwide via TROJAN logistics system.

**CAPABILITIES—** The TS LITE (V)1 operates over leased commercial satellite circuits, and is readily deployed at any level of operations. TROJAN LITE (V)1 operates at the TS/SCI security level. TS LITE (V)1 is fielded to the US Army Special Operations Forces (SOF) MI community and the United States Marine Corps.

**POWER SOURCE—**Commercial or generator power (user supplied or optional generator set) at 115 VAC, single phase, 50/60 Hz, at approximately 2.5kW.

**OPERATOR/MAINTAINER—**Not MOS specific; specialized training required; field service representative (FSR).

**REFERENCES—**TM 32-5895-400-12&P.

**STATUS—**

# TROJAN SPECIAL PURPOSE INTEGRATED REMOTE INTELLIGENCE TERMINAL LIGHTWEIGHT INTELLIGENCE TELECOMMUNICATIONS EQUIPMENT (V)2 AND (V)3



**SYSTEM SUMMARY**

| | |
|---|---|
| • Length—675.5 inches. | • Maximum EIRP (mid Band)—55.0 dBW or 65 dBW. |
| • Width—354 inches. | • Intelsat Certification—Type approved. |
| • Height—401.5 inches. | • Ku-Band Transmission frequency range—14.0 to 14.5 GHz. |
| • Cube—3,512.5 inches. | • Ku-Band Receive frequency range—10.95 to 12.75 GHz. |
| • Weight—28,248 pounds. | • System G/T (mid Band)—25.0 dB/K. |
| • C-Band Transmission frequency range—5.850 to 6.425 GHz. | • Maximum EIRP (mid Band)—62.0 dBW or 67 dBW. |
| • C-Band Receive frequency range—3.625 to 4.200 GHz. | • Intelsat Certification—Type approved. |
| • System G/T (mid Band)—19.0 dB/K. | |

**Figure K-5. TROJAN Special Purpose Integrated Remote Intelligence Terminal Lightweight Intelligence Telecommunications Equipment (V)2 and (V)3**

**NOMENCLATURE—**AN/TSQ-226 (V)2 and AN/TSQ-226 (V)3.
**PROJECT NAME—**TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Intelligence Telecommunications Equipment (LITE); TS LITE (V)2 and TS LITE (V)3.
**FUNCTION—**The TS LITE is a C- and Ku-band satellite system that provides Secret and TS/SCI network access for intelligence processing systems.
**DESCRIPTION—**TROJAN SPIRIT LITE is a functional equivalent to the TROJAN SPIRIT II and was originally developed to support the Stryker brigade combat team (SBCT). The TS LITE (V)3 is comprised of two sub-systems; the Mission Subsystem and the Communications Subsystem. The

Mission Subsystem, shown on the right in the above drawing, is mounted on an M1152 expanded capacity vehicle (ECV) and transports a Type III lightweight multipurpose shelter (LMS), an on-board generator set, and an environmental control unit (ECU). The LMS houses mission equipment consisting of a workstation, a laptop, a scanner, printers, and phones. The mission subsystem vehicle tows the M1102 lightweight tactical trailer (LTT), and a SATCOM band change equipment and spares trailer. The communications subsystem is mounted on the M1152 ECV and transports one pallet-type shelter with an on-board generator set, ECU, a 2.4-meter antenna mounted on top of the pallet. The pallet houses the SATCOM subsystem and network equipment. The communications subsystem vehicle tows the M1102 LTT cargo trailer with modular command post system (MCPS). The stand-alone version of the communications shelter is also known as the TS LITE (V)2. The TS LITE (V)2 comprises a communications subsystem and an M1152 ECV used as a "chase vehicle". The chase vehicle tows the second M1102 LTT SATCOM band change equipment and spares trailer. TROJAN LITE (V)3 contains secure voice, data, and video and secondary imagery dissemination capabilities. The system will receive, display, and transmit digital imagery, weather and terrain products, templates, graphics, and text between CONUS/OCONUS bases and deployed forces. Connectivity is provided through the Fort Belvoir and Fort Bragg TROJAN Network Control Centers (TNCCs). The terminal can transmit and receive data rates up to 2.048 Mbps and provides ETHERNET connectivity for various Joint intelligence processing systems. Validated networking requirements for this system include NIPRNET, SIPRNET, JWICS, and NSANet as well as LAN connectivity. The NSANet connectivity, including NSTS, supports TS/SCI users with direct access to the Global SIGINT Enterprise to facilitate collaboration, targeting support, analysis, and other data exchanges as needed.

**CAPABILITIES—**TROJAN LITE has the following capabilities:

- Classified local and wide area network (LAN/WAN) access—TDN 3 (JWICS); TDN 2 (NSANet); 10/100 BaseT Ethernet LAN, voice over IP (VoIP) phone.
- Deployable world-wide using TROJAN communications network.
- 64 kilobytes per second (Kbps) to 2,0484 Kbps.
- UAS video forwarding.
- KG-175D TACLANE Micro (secure COMSEC unit).
- Supportable worldwide via TROJAN logistics system.

**POWER SOURCE—** Operates from commercial or generator power (user supplied or optional generator set); 10 kW tunnel-mount generator and ECU.

**OPERATOR/MAINTAINER—**Three CMF 35F (Intelligence Analyst)/CMF 35T (Military Intelligence Systems Maintainer & Integrator).

**STATUS—**Program of record; the TS LITE (V)2 is fielded to the MI company within the SBCT.

# LOW COST S-BAND RECEIVER

**SYSTEM SUMMARY**

| | |
|---|---|
| • S-band SATCOM receiver supporting TENCAP system. | • System weight—15 lbs. |
| • Receive capability— | • Transport weight (soft case)—3 lbs. |
| • SID. | • Frequency (transmit/receive)—UHF. |
| • National intelligence products. | • Modulation—BPSK, QPSK. |
| • Messages and file transfer. | • Data rate—0.552 to 256 Kbps. |
| • High data rate (receive). | • User interface—RS 530, RS 232. |
| • Lightweight, reduced size. | • Cryptographic interface—KIV-7. |
| • 15-minute setup time. | • Power—115 VAC, 50/60 Hz. |

**Figure K-6. Low Cost S-Band Receiver**

**NOMENCLATURE—**M-22 Communications System.
**PROJECT NAME—**Portable S-Band Receiver (LSR).
**FUNCTION—**The LSR is designed to support the Army's tactical mission by receiving intelligence data obtained from national assets. The LSR supports deployed, tactical units with the receipt of nationally derived data through immediate access sources and satellite relay capabilities. It can acquire secondary imagery products and nationally collected information, and provide an alternate routing of messages and files.
**DESCRIPTION—**The system consists of a receiver subsystem, antenna subsystem, and a crypto subsystem. LSR size and weight enhances deployment with the mobile ground maneuver forces currently supported by Army TENCAP equipment. A soft transit case is included for transporting the receiver, providing packaging within the 84-pound commercial airline baggage limits. The M-22 S-band data services receiver is a small, flexible receiver for reception of M-22 data. Receiver control is also available by means of a PC-compatible serial port. Direct connection to the KIV-7 COMSEC device is supported. Complete reception systems can be provided by adding the Quorum Router, a user-supplied PC and appropriate reception software. The M-22 receiver incorporates an analog PM demodulator followed by a DSP subcarrier demodulator which provides exceptional stability and performance. User-selectable operational modes, which include subcarrier frequencies, data rates, modulation type, differential coding, convolutional coding and descrambling, provide a flexible solution to M-22 data reception in a PC- and workstation-friendly drive bay format. These

files can be transmitted from in-theater via a TES-Forward or from a fixed CONUS site. While the terminal's primary function is reception of imagery, it is used also to transfer other data such as message traffic. The M-22 tactical network (MTN) transponders are secondary payloads on classified DOD host vehicles that are in highly elliptical orbits. M-22 S-band communications satellites provide the capability to download imagery, as well as minimum-essential wideband support in the event of wideband link outages. The M-22 data rate is limited, but its capability fulfills most present and future vehicle reception requirements. The MTN provides a bridge between DOD common user networks and tactical networks with broadcast dissemination of a variety of collateral intelligence products at data delivery rates ranging from 8 to 256 Kbps. MTN uses a small, rapidly deployable S-band receive terminal; or alternatively, operates with existing LSRs and SOF IRIS or similar terminals, with MTN software augmentation. Flexible LAN and serial interfaces accommodate a variety of existing tactical intelligence processors, and its modular and scalable design facilitates adding capacity and functionality. The following are features of the system:

- Rapidly employable on C-130, C-17, and C-5 aircraft, maritime transport, rail, and as baggage on commercial air transport.
- 24-hour mission availability.
- Operated in a tactical- or fixed-site environment.
- Supports degraded mode, jump, and split-based operations.

**CAPABILITIES—** The LSR Receiver is capable of receiving signals at data rates up to 1,024 Kbps from the Defense Meteorological Support Program and low elliptical orbit (LEO) satellites, and up to 128 Kbps from high elliptical orbit HEO and geosynchronous earth orbit (GEO) relay satellites. The LSR is self-contained and requires no tools for assembly or operation. The M-22 receiver provides state-of-the-art performance and can be quickly configured in the field using the front panel switches. The M-22 receiver can be used with existing S-band reception systems or can be mated with the Quorum Flat Panel antenna systems to provide a small and lightweight tactical receive system. In an early entry environment, the only communications available to Army TENCAP may be organic RF systems.

**POWER SOURCE—**Requires 115-VAC, 50/60 Hz power provided by supporting unit tactical generators, commercial power, or other power-generation equipment.

**OPERATOR/MAINTAINER—**Not MOS specific; specialized training required, field service representatives.

**STATUS—**

# COMMUNICATIONS CONTROL SET

**SYSTEM SUMMARY**

| | |
|---|---|
| • Multi-coupler TD-1289. | • Datalink processor. |
| • UHF antenna AS-2810. | • TSEC/KY-68 (DSVT) (2 carry-in). |
| • Red patch panel. | • Telephone TA-838A/TT. |
| • Black patch panel. | • Headset H-161. |
| • Ruggedized computer PDP 11/94. | • Handset H250/U. |
| • Communications protocol processor. | • Intercom control C-6533. |
| • Computer operator terminal. | • Microphone M80/U. |
| • 2 x 280 MB HDDs. | • Foot switch. |
| • Journal and audit printers. | • HYP-71 power supply. |
| • Unbalanced to balanced converter. | • Data adapter (2 carry-in). |

**Figure K-7. Communications Control Set, AN/TYQ-128(V)2/3**

**NOMENCLATURE**—AN/TYQ-128(V)2/3 (formerly AN/TYQ-63A and AN/TYQ-40A).
**PROJECT NAME**—Communications Control Set (CCS).
**FUNCTION**—The CCS provides a communications front end to interface the ASAS enclaves, both all source and single source, with a variety of communications systems. The ASAS-CCS was designed to bridge the gap between dissimilar networks and protocols, thus providing the mechanism for transferring time-sensitive tactical information between these networks. The information sources accessed depend on unit mission and intelligence requirements.
**DESCRIPTION**—The CCS is a tactically deployable, sheltered or unsheltered, ruggedized automated information system. It consists of computer hardware, software, and associated secure communications equipment that support the execution of intelligence, surveillance, and reconnaissance (ISR) tasks in its primary function as a central communications node for ASAS. The two primary communications methods employed within the ASAS-CCS are—

- Ethernet communications for LAN operations using TCP/IP with FDMP. TCP/IP/FDMP protocol operates either with or without encryption.
- Serial communications for point-to-point connectivity using DDCMP. This communications protocol may operate in either synchronous or asynchronous transmission mode. DDCMP operates with FDMP.

The communications system for the ASAS consists of a series of CCS. There are two variants—shelterized and dismounted. The AN/TYQ-128(V)2 is the shelterized variant, and the AN/TYQ-128(V)3 is the dismounted variant. The CCS provides a communications front end interfacing the ASAS

enclaves (both all source and single source) with various communications systems, principally via LAN connection to MSE's high-capacity line of sight (HCLOS), JNN direct wireline connection to the AN/TYC-39 message switch, and other interfacing systems. The CCS receives and relays information from adjacent, superior, and subordinate units to and from the intelligence processing enclaves. At Division level it also connects multiple sensors via LAN directly to the ASAS. The ASAS-CCS provides the multi-level security (MLS) required for the US Intelligence Communications Architecture. The development, fielding, and ongoing US Army Communications Electronics Life Cycle Management Command SEC IFS maintenance efforts supports the near-term communications needs of units, exploits merging technology, and complies with the standards of the ABCS. The ASAS-CCS provides DSSCS/GENSER automatic message processing and routing. Message formats supported by the ASAS-CCS include DOI-103, DOI-103M, ACP-126, ACP-127, JANAP-128, DD-173 message formats and Defense Message System. Additional capabilities include access to the DMS connectivity (SMART 2.6.9a/CDAC 1.7.2b), connectivity to the AFATDS via SMART, direct serial connectivity to JTT, Incorporates JTT Control Client and provides Message Safe-Store, Archive, and Retrieval. The CCS supports collateral- and SCI-level communications processing and relay; it interfaces with ACUS and special purpose intelligence communications systems. These information systems provide the G-2/S-2 and the ACE with access into joint intelligence systems and gateways into allied systems in multinational operations. The CCS can be deployed either as part of a larger CP, or separately as a DISE, to sustain a variety of training and real-world missions. When deployed apart from its higher headquarters, the DISE and the CCS should collocate with an available signal unit and communications node for communications support, logistics, and mutual security. The sheltered version of CCS is accommodated on the M1097, Heavy HMMWV. The following are features of the CCS:

- Deployable on C-130, C-17, or C-5 aircraft.
- 24-hour mission availability.
- Operated in a tactical- or fixed-site environment.

**CAPABILITIES—**The CCS provides secure connectivity between command and control elements at all echelons, as well as conduits from users to various information sources. The CCS enables the ASAS system to have a rapid and secure means to receive combat information, issue collection requirements, submit requests for information and disseminate intelligence. The CCS handles SCI message traffic to and from the ASAS Block II ASAS Fusion System and ASAS Single Source Workstations, and collateral message traffic for the ASAS-Light supporting the G-2 in the TOC. The CCS supports communications to and from remote sensors and allows data and voice communications with higher, lower, and adjacent units. The CCS can automatically send, receive, and distribute a variety of message types and formats between higher, lower, and adjacent units over innumerable pathways. The CCS also acts as an internal "post office" routing messages and data between various internal ASAS enclaves, DCGS-A, TENCAP systems, and other automated information systems. The CCS is the linchpin that holds the ASAS system together.

**POWER SOURCE—**Requires 115-VAC, 60-Hz power is provided to system 10 kW tactical generators, commercial power, or other unit power generation equipment.

**OPERATOR/MAINTAINER—**Operator: Not MOS specific; specialized training required. Direct support maintenance is provided by system MOS 35T personnel; general support maintenance is provided by depot maintenance personnel.

**REFERENCES—**

**STATUS—**

# COUNTER RADIO CONTROLLED IMPROVISED EXPLOSIVE DEVICE ELECTRONIC WARFARE (CREW) SYSTEMS

## DUKE V2, AN/VLQ-12(V)1

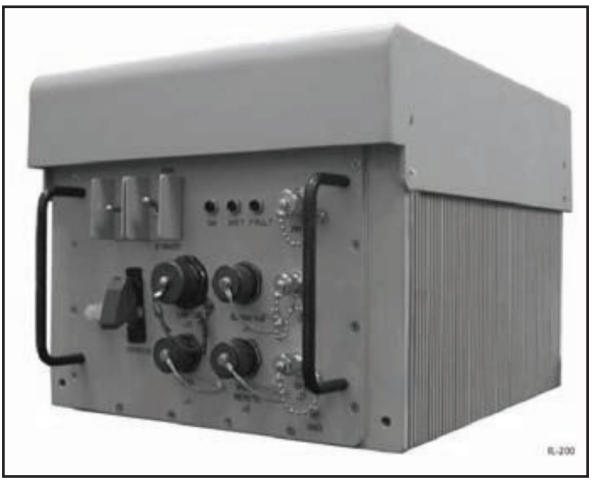


Figure K-8. AN/VLQ-12(V)1, Duke V2

**NOMENCLATURE—**AN/VLQ-12(V)1, Duke V2.
**PROJECT NAME—**Duke.
**FUNCTION—**Active and Reactive jammer (vehicle mounted).
**DESCRIPTION—**The Duke is an active and reactive jammer. It is effective against high- and low-power threats, and provides threat event logging. The Duke is theater-provided equipment.
**SYSTEM COMPONENTS—**System components are displayed and listed below in figure K-9.
**STATUS—**QRC.

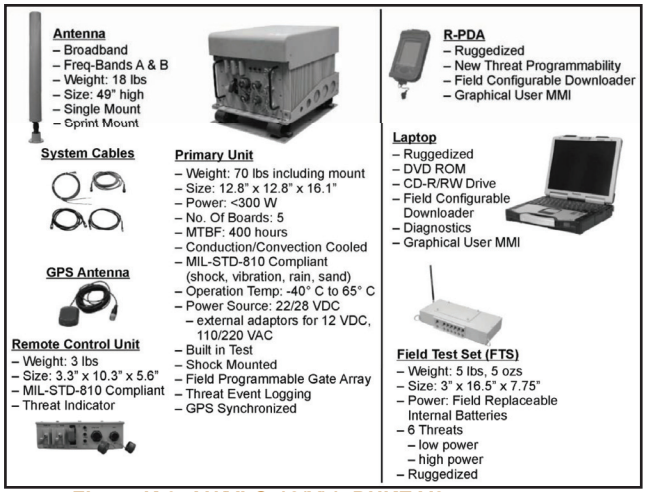



**Figure K-9. AN/VLQ-12(V)1, DUKE V2 components**

## DUKE V3, AN/VLQ-12(V)3

**Figure K-10. AN/VLQ-12(V)3, DUKE V3**

**NOMENCLATURE—**AN/VLQ-12(V)3, Duke 3.
**PROJECT NAME—**Duke.
**FUNCTION—**Active and reactive jammer (vehicle mounted).
**DESCRIPTION—**The Duke V3 is an upgraded version of the Duke V2 active and reactive jammer. The Duke V3 provides increased capability through the addition of a secondary unit and FRF-119C antenna. It is effective against high- and low-power threats. Duke V3 also provides threat event logging and is theater-provided equipment.
**SYSTEM COMPONENTS—**System components are displayed and listed below in figure K-11.
**STATUS—**QRC.

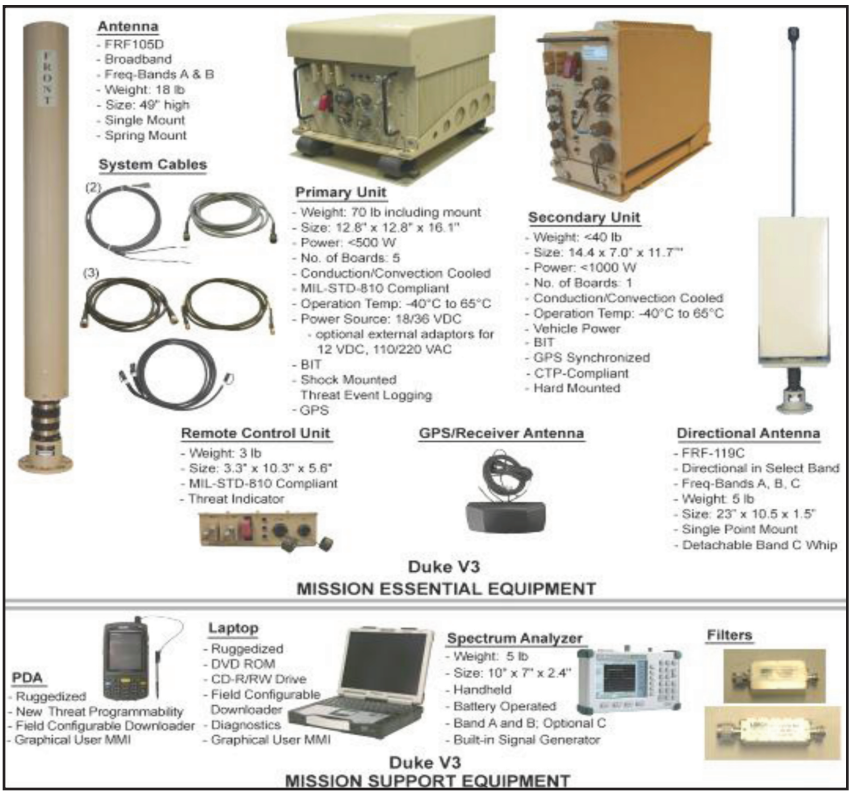



Figure K-11. AN/VLQ-12(V)3, DUKE V3, components

## CREW Vehicle Receiver/Jammer (CVRJ) (AN/VLQ-13(V)1)

Figure K-12. AN/VLQ-13(V)1, CREW Vehicle Receiver/Jammer

**NOMENCLATURE**—AN/VLQ-13(V)1.
**PROJECT NAME**—CREW Vehicle Receiver/Jammer (CVRJ).
**FUNCTION**—Active and reactive jammer (vehicle mounted and fixed site).
**DESCRIPTION**—The CVRJ is a U.S. Army Warlock system. The system operates on 24v DC and has a remote control unit (RCU) to operate the system. The CVRJ is effective against high- and low-power threats. It is theater-provided equipment.
**STATUS**—QRC.



## Mobile Multi Band Jammer, AN/VLQ-14(V)1

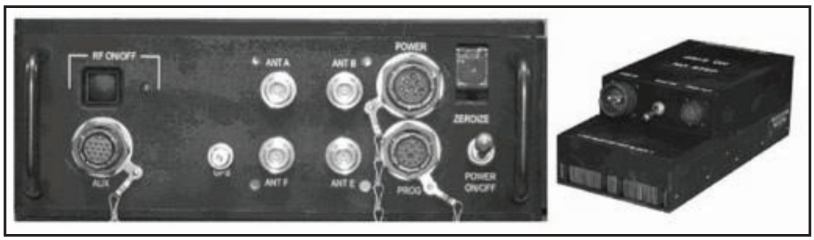



Figure K-13. Mobile Multi Band Jammer, AN/VLQ-14(V)1

**NOMENCLATURE**—AN/VLQ-14(V)1.
**PROJECT NAME**—Mobile multi band jammer (MMBJ-1B).
**FUNCTION**—Active jammer (vehicle mounted).
**DESCRIPTION**—The MMBJ-1B is a U.S. Army system that operates on 24v DC and has an RCU to operate the system. The system is effective against low-power threats. It is theater-provided equipment.
**STATUS**—QRC.

## DISMOUNTED CREW SYSTEMS

### Guardian Quick Reaction Dismount


Figure K-14. GUARDIAN QUICK REACTION DISMOUNT

**NOMENCLATURE—**None.
**PROJECT NAME—**Guardian Quick Reaction Dismount (QRD).
**FUNCTION—**Active jammer.
**DESCRIPTION—**The QRD system is designed for deployment in a tactical man-pack configuration. It is comprised of three man-portable units:

- Guardian B1 (Low-band).
- Guardian B (Mid-band).
- Guardian C (High-band).

Each unit weighs approximately 24 lbs. and can be used alone. When used as a suite of systems, protection is increased. Each system uses its own antenna. The Guardian QRD is theater-provided equipment.
**STATUS—**QRC.

## CREW 3.1

**Counter Radio Controlled IED Dismount System, AN/PLQ-9(V)1**


**Figure K-15. Counter Radio Controlled IED Dismount System, CREW 3.1, AN/PLQ-9(V)1**

**NOMENCLATURE—**AN/PLQ-9(V)1, CREW 3.1.
**PROJECT NAME—**Joint CREW; THOR III (Developed by US Navy; PMS-408).
**FUNCTION—**Active and reactive jammer.
**DESCRIPTION—**CREW 3.1 is a man-portable, active and reactive system designed to prevent radio controlled detonation of IEDs. The system consists of three man-packs, each weighing approximately 25lbs. It is theater-provided equipment.
**STATUS—**QRC.

## USMC and Coalition Forces CREW Systems

### Chameleon (USMC)

Figure K-16. Chameleon

**NOMENCLATURE—**None.
**PROJECT NAME—**Chameleon (USMC).
**FUNCTION—**Active, vehicle mounted jammer.
**DESCRIPTION—**The Chameleon is a U.S. Marine Corps 4-channel active jammer system which jams high- and low-power threats. The system uses a ruggedized personal digital assistant for programming and operator interface. It is theater-provided equipment.
**STATUS—**QRC.



### SYMPHONY (Coalition Forces)


Figure K-17. SYMPHONY

**NOMENCLATURE—**None.
**PROJECT NAME—**SYMPHONY.
**FUNCTION—**Active, vehicle-mounted jammer.
**DESCRIPTION—**The primary user for this system is Coalition Forces. The system is effective against low- and some high-power threats. It is theater-provided equipment.
**STATUS—**QRC.

# MACHINE FOREIGN LANGUAGE TRANSLATION SYSTEM

Machine foreign language translation (MFLT) is defined as the use of computers and computer software to conduct language translation. MFLT is an emerging capability that is currently being used in Iraq and Afghanistan by Army units in support of command and control, movement and maneuver, intelligence, protection, and sustainment. The family of MFLT capabilities is referred to as the MFLT systems (MFLTS). Examples of MFLTS are displayed in figure K-18.

**Figure K-18. Examples of Machine Foreign Language Translation Systems**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Machine Foreign Language Translation Systems (MFLTS).
**FUNCTION—**MFLTS is a family of software products developed to meet foreign language translation requirements when human linguists are unavailable. An MFLTS, when employed appropriately, can mitigate some linguistic shortfalls in the Joint Force. It can also, in a limited capacity, expand the number of languages supported within the DoD.
**CAPABILITIES—**Conceptually, MFLTS is the idea that languages can be translated using a machine instead of, or in addition to, a human linguist. An MFLTS component can complement human linguists and enable non-linguists. While MFLTS is primarily focused on low-level linguistic tasks, it is capable of supporting rapidly deploying forces, special operations forces (SOF), and first responders when linguistic support is unavailable. Additionally, MFLTS can provide deployed forces the ability to conduct rudimentary cross-lingual communications in both cooperative and non-cooperative environments. A machine foreign language device is a piece of hardware with a language translation

software program that allows the user to translate one language into another. MFLTS devices use the following methods:

- Speech-to-speech (S2S).
- Speech-to-text (S2T).
- Text-to-text (T2T).
- Text-to-speech (T2S).

MFLTS devices operate in the following modes:

- A one-way device contains prerecorded 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. One-way devices are not used often, but there may be lingering equipment that performs in this manner.
- T2S is a one-way "plus" device. A one-way plus device is an MFLT system that utilizes commonly used prerecorded phrases but combines them with additional phrases as added by the user. These can be loaded with a series of relevant questions and/or commands or instructions based on an operational situation.
- S2S and S2T are two-way devices. A two-way device is a machine foreign language translation system that translates one language into another natural language, and then in turn, translates the response. This is the device that most users think of when they think of MFLT as it replicates a two-way spoken conversation at the basic level. Coalition Chatline Plus (CCL+) is another example of two-way method of communicating using instant messaging service.

There are several enduring MFLTS capabilities under the umbrella of Deployable Harmony Collection Tools:

- Deployable Harmony DOCEX Suite (DHDS).
- Project HARMONY—a tool for managing document collection and translation resources.
- "Dirty-to-Clean" (D2C) tool that produces clean representations of documents from captured electronic media, enabling their import into and dissemination across multiple secure national networks from captured hard drives, thumb drives, CDs, DVDs.
- Theater Exploitation Database (TED)—TED is an interface between the internet and the DHDS allowing for worldwide access to theater-specific DOMEX.

Also covered by the enduring capabilities are Media Monitoring, which creates a continuous searchable archive of international television broadcasts; and Coalition Chatline Plus, which is a multilingual instant messaging and document translation system.

**POWER SOURCE—**Dependent on the particular MFLTS device.

**OPERATOR/MAINTAINER—**Not MOS specific; embedded training is part of the capability for future software although current QRCs require initial training for user, FSR.

**STATUS—**QRC. This capability is considered an enduring capability, likely to be employed, enhanced, and upgraded rather than replaced.

# TROJAN SWARM

## TROJAN SWARM System and Architecture

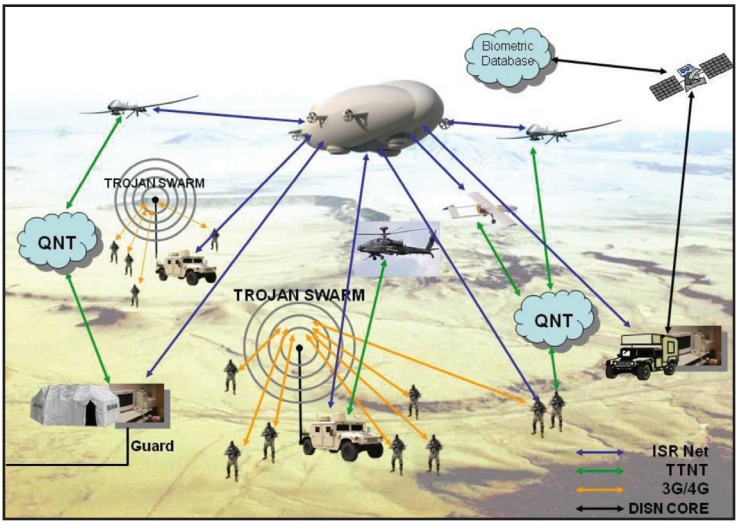



Figure K-19. TROJAN SWARM Architecture

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**TROJAN SWARM.
**FUNCTION—**TROJAN SWARM will provide the "last tactical mile" solution between a dismounted Soldier or team and the nearest TROJAN communications node using a third generation (3G)- or fourth generation (4G)-enabled intelligence collection device to SIGINT, HUMINT, MASINT, IMINT, or other intelligence, surveillance, and reconnaissance (ISR) applications.
**DESCRIPTION—**TROJAN SWARM is a subsystem of relevant ISR to the edge (RITE). It is an internet protocol (IP)-based beyond-line-of-sight (BLOS) cellular canopy or mobile broadband network.
**CAPABILITIES—**TROJAN SWARM is ISRNet interoperable and bridges the terrestrial layer with the aerial layer. TROJAN SWARM is interoperable with the space layer using its organic TROJAN dissemination systems (TS LITE (V)1, (V)2, and (V)3 systems). TROJAN SWARM was founded on the biometrics requirement driven by deployed forces to the Rapid Equipment Force (REF) for a solution to reduce the latency of biometrics feedback during extended operations. TROJAN SWARM's developmental path is toward SIGINT SCI collection, and find, fix, finish, exploitation, analysis, and dissemination (F3EAD) missions. The TROJAN SWARM architecture (figure K-19) consists of fixed and mobile nodes. Each node provides Universal Mobile Telecommunications System (UMTS), wide-band code division multiple access (WCDMA) cellular technology. Each node is a network. Each mobile TROJAN SWARM node (TSN) may be interconnected with a fixed-site TSN when within line-of-sight (LOS) of each other or within range of accompanying QNT radios utilizing aerial layer LOS ranges capable of forming a single mesh network.
**POWER SOURCE—**Dependent on deployment.
**OPERATOR/MAINTAINER—**To be determined.
**STATUS—**HQ DA, G-2-funded research and development. INSCOM TROJAN (I2WD) is the materiel developer.

## Fixed-Site TROJAN SWARM Node


**Figure K-20. Fixed-site TROJAN SWARM Node**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Fixed-site TROJAN SWARM Node (TSN).
**FUNCTION—** The fixed-site TSN is the primary 3G or 4G node connecting the intelligence collection devices to the TROJAN SWARM network. It provide "mud to space" connectivity between 3G and 4G devices and destination database.
**DESCRIPTION—**The fixed-site TSN may consist of multiple UMTS pico-cell transceivers. Each fixed-site TSN is outfitted with an amplifier, and dual 1U Servers in a ruggedized 9U case. The antenna should be raised and affixed to a mast, tower, or static high-altitude platform (HAP). The operational range of the fixed-site TSN is largely dependent on LOS and the power capacity embedded within the specific 3G- or 4G-enabled intelligence collection device. The higher the antenna is erected, the greater the area of coverage.
**CAPABILITIES—**Fixed-site TSNs may be integrated at a forward operating base (FOB), for example, and configured for local database access, as well as multiple classification networks via TROJAN Points of Presence (PoP) and Turnstile. Fixed-site TSNs are designed primarily to service TSNs for a variety of applications at extended ranges, as well as local intelligence collection devices.
**POWER SOURCE—**Dependent on deployment.
**OPERATOR/MAINTAINER—**To be determined.
**STATUS—**Development in conjunction with TROJAN SWARM.

## Mobile TROJAN SWARM Node

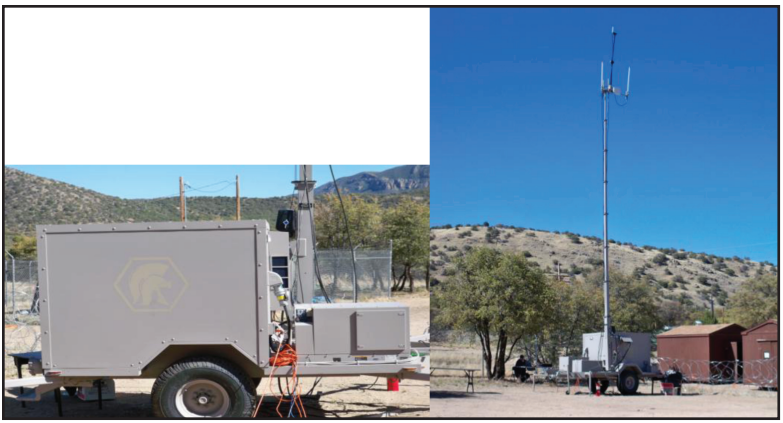


Figure K-21. Mobile TROJAN SWARM Node

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Mobile TROJAN SWARM Node (TSN).
**FUNCTION—**The TSN is the primary 3G or 4G node connecting the intelligence collection devices to the TROJAN SWARM network.
**DESCRIPTION—** The mobile TSN generally consists of a dual UMTS pico-cell, an amplifier, and dual 1U servers in a ruggedized case for mobile applications. TSNs form a tactical 3G or 4G cloud around a vehicle platform.
**CAPABILITY—**Mobile TSNs are capable of supporting intelligence collection devices autonomously, while extending the TROJAN SWARM network via a variety of IP connections to a fixed TSN or another mobile TSN. TSNs have integrated amplified air cards for LOS connectivity to fixed-site TSNs. They may also utilize systems such as QNT or EPLRS for alternative and long range IP connectivity. TSNs may be configured remotely, or operated locally using monitor, keyboard, mouse, and the Praefectus software interface.
**POWER SOURCE—**Dependent on deployment.
**OPERATOR/MAINTAINER—**To be determined.
**STATUS—**Development in conjunction with TROJAN SWARM.

# RELEVANT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE TO THE TACTICAL EDGE

## Immediate Response Intelligence Syste

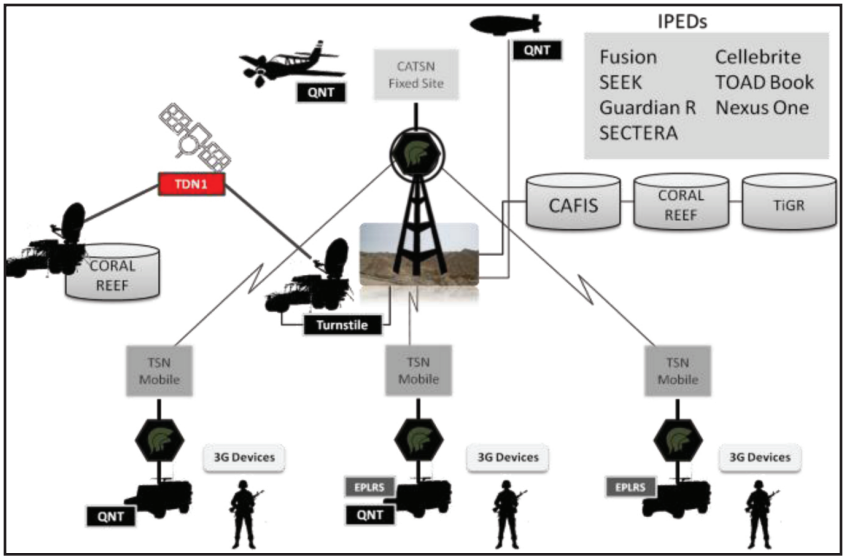



**Figure K-22. Immediate Response Intelligence System**

**NOMENCLATURE—**Not applicable.
**PROJECT NAME—**Immediate Response Intelligence System (IRIS).
**FUNCTION—**Provide Army Soldiers at the edge with timely and relevant information via a seamless integration of IRIS-certified devices to TROJAN data network (TDN) 0, 1, 2, and 3 via TROJAN SWARM and TROJAN Points of Presence.
**DESCRIPTION—**The IRIS personal exploitation devices (IPEDS) are wireless, handheld devices. Transmission of data will occur using the TROJAN SWARM architecture for the initial operational capability (IOC) and will demonstrate interoperability between nodes in the terrestrial, aerial and space layers. Figure K-23 depicts the overall test environment conducted at the U.S. Army Intelligence Center of Excellence. Figure K-24 depicts the collection and transmission site activities and equipment at Site Uniform. Figure K-25 depicts the reception activities and equipment at Site Papa.
**CAPABILITIES–**IRIS will transmit biometrics and cellular forensics data to Automated Fingerprint Identification System (AFIS) and cellular forensics databases, and provide immediate responses to operators.
**OPERATOR/MAINTAINER—**Under development.
**STATUS—**IOC and technical demonstration.

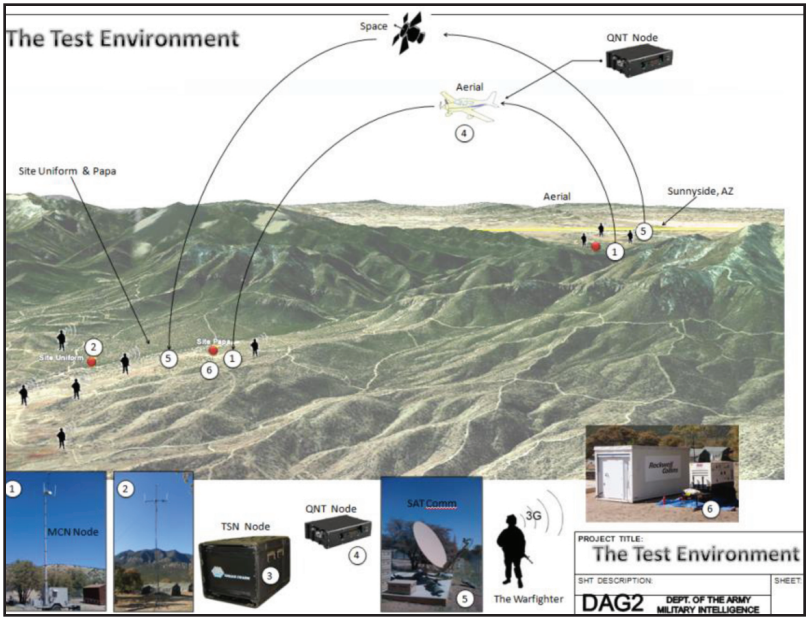



Figure K-23. Overall IRIS Test Environment


Figure K-24. Test collection and transmission site activities and equipment at Site Uniform

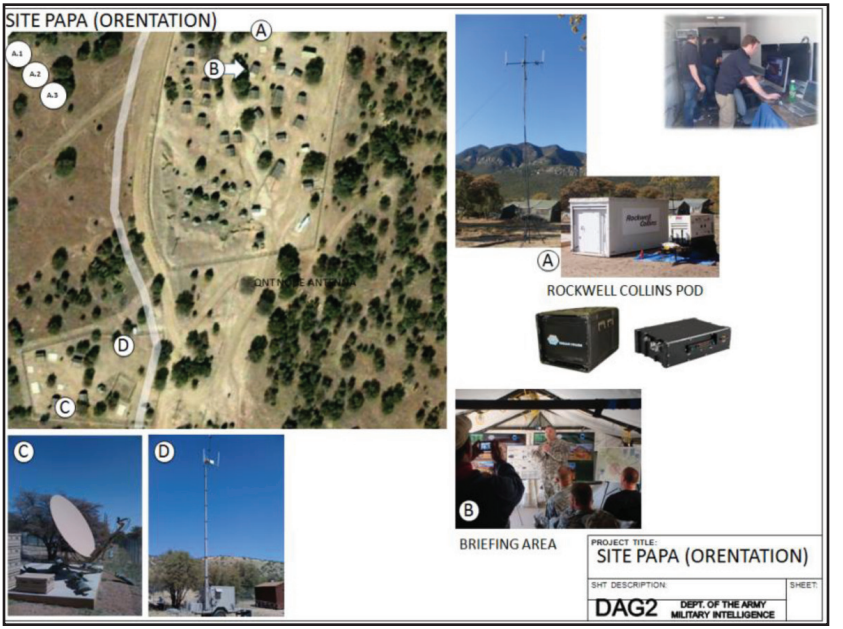



**Figure K-25. Test reception activities and equipment at Site Papa**





FOR OFFICIAL USE ONLY

# Appendix L

# Tactical Signals Intelligence Operations

## INTRODUCTION

**L-1.** This appendix discusses the signals intelligence (SIGINT) process model, factors to consider when conducting SIGINT cell operations, and the duties of SIGINT cell personnel.

## TACTICAL SIGNALS INTELLIGENCE FOCUS

**L-2.** Army tactical SIGINT focuses on providing three primary types of intelligence to commanders and operators during combat operations:

- Support to protecting the force.
- Support to targeting.
- Support to situation development.

**L-3.** Tactical SIGINT significantly contributes to the overarching SIGINT exploitation enterprise. Tactical SIGINT directly contributes to the SIGINT picture, resulting in more effective national and theater-level SIGINT reporting. Information is made available to decisionmakers at all levels. Collaboration is understandably important to the entire process model, yet should always remain a top-down architecture in which theater and national entities apply maximum efforts to support tactical elements with commodity services.

## SIGNALS INTELLIGENCE PROCESS MODEL

**L-4.** The Army tactical SIGINT operations process model is constructed of five core components, each of which is defined by specific characteristics. The core components and characteristics do not vary by echelon. Effective implementation of these components is critical to mission success anywhere. The tactical SIGINT process model is not effective unless all core components and characteristics are clearly understood by leaders and analysts alike. The core components of the operations process model are—

- Collection/intercept operations.
- SIGINT payload prosecution.
- SIGINT reporting.
- Collection management.
- Process effectiveness.

### Collection/Intercept Operations

**L-5.** Characteristics of this component are the foundation of the unit's mission. These are—

- **Mission definition.** This characteristic specifies the precise mission on which a SIGINT cell focuses.
- **Sensor distribution**. This characteristic illustrates how organic sensors will be employed or arrayed.
- **Analytic distribution.** This characteristic defines how organic analysts are employed to meet mission goals, taking several variables into account. Variables include friendly force prosecution, connectivity bandwidth, skill level of analysts, and effective capacity to prosecute.
- **Linguist distribution.** This characteristic defines how organic linguists are arrayed or deployed

to meet mission goals.

- **Leadership distribution (unit commander/operations officer [S-3]).** This characteristic defines how a unit's leadership is arrayed within the area of operations (AO) and how the most time-sensitive intelligence will reach them to support operational decisionmaking.
- **Supported distribution.** This characteristic describes access elements of the broader recipient base. This characteristic determines the vector and payload for delivering intelligence to the end points, providing force protection, threat warning, and targeting intelligence.
- **Support distribution (such as CACI, LOG).** This characteristic describes the tactical support array, including bottlenecks and points of failure for personnel/equipment replacement schema.

## Signals Intelligence Payload Prosecution

**L-6.** Characteristics of SIGINT payload prosecution include—

- Flash analysis (prioritized rapid exploitation).
- Detailed analysis (corroborated).
- Correlated analysis (flash/corroborated).
- Correlated analysis (detailed/correlated).
- Survey analysis (detailed/correlated).
- Target prosecution (rapid/comprehensive/correlated).
- Smart exploitation.



## Signals Intelligence Reporting

**L-7.** Characteristics of this component define outbound intelligence flow and response to supported elements. These characteristics include—

- Actionable reporting (immediate, actionable).
- Detailed/summary reporting (support).
- Comprehensive reporting (diagrams, multidiscipline correlated).
- Situational awareness reporting.
- Targeting-specific reporting.
- Response to requests for information (RFIs).

## Collection Management

**L-8.** Characteristics of this component help to accurately target the enemy, using all available sensors and resources. These characteristics include—

- Tasking and detasking characteristics.
- Configuration management process, end points, and threads characteristics.
- Sensor coordination characteristics.
- Effectiveness and assessment characteristics.

## Process Effectiveness

**L-9.** Process effectiveness is an abstract component that encompasses the entire tactical SIGINT prosecution model. This component is initiated by identifying SIGINT cell effectiveness. Usually this is accomplished through an ongoing series of metrics and statistics (such as numbers of reports, threat tippers, tasking evaluation, requirements met and missed, and sensor effectiveness). This component should be managed by the SIGINT cell officer in charge (OIC) or noncommissioned officer in charge (NCOIC). Details are reported to the unit commander for incorporation into future resource allocation coordination.

## PREMISSION

**L-10.** Before any deployment, SIGINT elements should prepare for their future environment by contacting the Army Technical Control and Analysis Element (ATCAE) at Fort Meade, Maryland, the G-3 Army Cryptologic Office (ACO) of the U.S. Army Intelligence and Security Command (INSCOM), and the Meade Operations Center (MOC). These organizations can aid in the acquisition of premission information as well as put cell analysts in contact with SIGINT analysts who are currently prosecuting targets in the area of interest.

**L-11.** Table L-1 lists several questions that should be asked and critical tasks a team should be trained on before deploying. The ATCAE, ACO, MOC leaders and analysts can help with acquiring this information.

**Table L-1. Questions that should be asked, and critical tasks a team should be trained on before deploying**

| |
|---|
| Who is currently reporting on activity in the area of interest? What types of reporting are they producing? (The analyst should contact the analysts currently working in the area of interest and acquire recent summary reporting, at a minimum, to familiarize the team with the targets and target behavior in the operational environment). |
| Have any recent detailed reports been produced that may help define proposed sensor employment locations (or areas to avoid)? |
| Where are the current collectors located and how effective are they? |
| Does the team have the appropriate intercept equipment to provide the three basic types of reporting? |
| Are there enough personnel to meet the demands of sensor placement within the area of operations? |
| Who is the tasking authority and how are they contacted? |
| What is the base battle rhythm? (It will undoubtedly change, but rehearsing the battle rhythm in garrison can give Soldiers a sense of familiarity that will pay dividends during operations when deployed.) |
| Does the team know the architecture of the targets and what high-value entities are associated with each hierarchy? |
| Is coordination for communications bandwidth needed? |
| What configuration and control information is needed? |
| What signals intelligence accreditation (Annex P) requirements must personnel meet? |



### Primary Critical Team Tasks

**L-12.** Critical tasks are both individual and collective.

#### Individual Tasks

**L-13.** Individual tasks include knowing how to read a map and knowing the AO. Rapidly determining distances between points, estimating derived locations, and correlating locations from differing grid systems can be tricky. Accuracy and speed are the keys to effectively depicting enemy activity within the AO.

**L-14.** Successful Soldiers know the geography of the AO. All team members need to know the urban layout and geography associated with their future target environment. This includes knowledge of the location of major bridges and waterways (what are the names, official and local?); knowledge of

the location of government buildings and transportation centers, such as police stations, prisons, rail stations, and bus stations; and knowledge of the location of key infrastructure nodes, such as electricity generation or distribution plants and oil or gas pipelines.

### Collective Tasks

**L-15.** Collective tasks include—

- **Conveying information to users.** Successful Soldiers know how to send sanitized key components of tactical intercept over collateral channels. A team must be able to quickly process tactical intercepts and relay that information to decisionmakers, focusing on avoiding misinformation and recipient misunderstanding. SIGINT team members must know how to convey information to recipients at the level they require.
- **Managing the collection and processing of information.** Successful Soldiers know how to manage the collection and processing architecture. If a specific type of protocol is being targeted, every member of the team should know how that protocol works and where the architecture is effective or lacking, and what resources are available.
- **Managing reporting.** Successful soldiers know how to manage SIGINT reporting, the various reporting formats, and which formats are appropriate for what types of payload.
- **Managing follow-on reporting.** Successful Soldiers also know how to manage follow-on reporting and battle damage assessments (BDA). They are prepared to correct mistakes as soon as they are recognized. If a target is misidentified or incorrect information is disseminated, they issue a cancellation or correction as soon as possible. After that, they fix the process model to reduce the potential for errors.



## Mission Preparation

**L-16.** Once the operation order (OPORD) has been received and the bounds of the operational support area are known, the team must plan for the types of signals to prosecute and the placement of assets so that the team can provide effective SIGINT support. Some important characteristics that will aid decisionmaking concerning the asset utilization process are listed below.

## Supporting an Area of Operations with Signals Intelligence

**L-17.** Determine the number and types of patrols and the area where they will be conducted each operational day, including such activities as multinational training, mine sweeping, combat patrols, security reconnoitering, intelligence gathering, and targeting missions. The terrain, times of day, frequency, and types of patrols should be considered heavily when drawing up the SIGINT support plan. As a standard SIGINT rule of thumb, always assign experienced analysts and linguists to the most critical time periods of activity.

## Identify and Map the Signals Intelligence Environment

**L-18.** After identifying and mapping the SIGINT environment, determine the availability of signals to prosecute by type that match the unit's collection and prosecution capability. Terrain plays a critical role in orienting sensor arrays. In some cases, elevated positions can provide access to communicant origination points, reducing the need for multiple sensors. The collection array should not be overly duplicative in nature since sensor-processing capability is a valuable commodity and it should not be wasted on duplicate intercepts. Once in position, each asset should perform a signals survey to verify that the payload is consistent with the expected intercept return.

# SIGNALS INTELLIGENCE CELL ORGANIZATION

**L-19.** SIGINT cells typically produce better intelligence and generally are more effective when the analytic and linguistic components are co-located. It is unnecessary, and often ineffective, to spread out the linguistic and analytic work force. This has the effect of decoupling the expertise and knowledge base from the dissemination and decisionmaking focal points for the sake of manning equipment. The most effective analytic, linguistic, and sensor distribution characteristics form a star topology where the sensors are lightly manned funneling intelligence back to a centralized node that has robust communications to all operator nodes. This facilitates rapid decisionmaking by coupling SIGINT expertise with operator leadership and operational knowledge of the AO. The ability to rapidly respond to RFIs from operators is a critical component to successful SIGINT support. If most time-sensitive mission decisions occur at specific tactical operations centers, the SIGINT cell and its dissemination architecture must be oriented to provide interactive, robust service to them.

**L-20.** As a lesser priority, the dissemination framework must also support graphic products and nontraditional SIGINT products that are authorized for wide dissemination.



**L-21.** Support distribution characteristics should be considered when designing the SIGINT cell's architecture. Sensor equipment seemingly fails at the most inappropriate times, so consider providing as much redundant logistic capacity as possible to remote sensor locations. This is also true with analytic expertise. If a sensor is temporarily sent to a remote location in support of a specific mission, be sure to provide effective analytic and linguistic support or be capable of remotely supporting that sensor.

## Types of Reports

**L-22.** Identify the report types that the team will deliver and the frequency of that delivery based on the unit's battle rhythm and leadership distribution characteristics. For example, if the team is co-located with the unit's leadership, there will probably be a requirement to provide input to daily all-source intelligence products. While this big picture information is important, most of the effort should be focused on supporting real-time operations, such as threat warning and situational awareness, and providing actionable targeting information. Having the appropriate communications infrastructure to support intelligence distribution is critical. The SIGINT cell can collect and process all of the information in the world, but if that information cannot be disseminated to the appropriate recipient in a timely fashion it is effectively worthless.

## Threat Tippers

**L-23.** Threat tippers are the most important vectors for dissemination. These are typically disseminated directly from the SIGINT cell to operators through various secure communications modes. These vectors consist of urgent threat warning, situational awareness, and target update messages. SIGINT cells must have this capability to effectively support their units. Effective cells ensure a framework is in place to implement this vector and rehearse it often. Junior analysts are often afraid or uncomfortable disseminating this information if they are not confident of their ability to distribute the correct information. Therefore, rehearsal and trust are critical to successful dissemination of time-sensitive threat tippers.

## Tactical Reports

**L-24.** Disseminating tactical reports (TACREPs) is important to formalizing the intelligence distribution process. When the framework is set up, there should be a reliable transmission medium

and a method of serialization that promotes a common way of referencing previously disseminated information. This supports the interactive answering of requests for further information, as well as providing an accurate method of correcting tactical reporting mistakes. Since TACREP reporting comprises the bulk of reporting and timeliness is important, the successful analyst ensures there is sufficient network architecture to reach all the supported end points. It is often better to immediately report the 80 percent solution and then send out updated TACREPs to clarify the reporting thread as more information is received. This saves time in answering redundant RFIs, in addition to providing effective and timely support.

### Signals Intelligence Cross-Talk

**L-25.** Technical exchanges between SIGINT-producing organizations is also important. Dissemination and processing architecture must take this into account as well, though the highest priority is to provide time-sensitive collateral reporting and tipping to the supported unit.



## SIGNALS INTELLIGENCE CELL SET-UP AND OPERATION

**L-26.** A number of positions and key processes should be considered for SIGINT cells. They are not all-encompassing and will vary based on number of assigned personnel and their expertise level. In some cases many individuals may perform similar tasks, such as collection management or constructing targeting packages.

**L-27.** Each shift should begin with a short briefing to provide the shift personnel with operational details of the day, including—

- What missions are occurring, and where and how the cell is supporting the effort, such as handbill distribution, cordon and search, and active targeting.
- Collection or processing problems involving such things as equipment or networks.
- Enemy activity overview and threat watches.
- RFI overview and reporting issues, including corrections to make and reports to be issued.

**L-28.** Time-sensitive prosecution drives the process model; all intercepts are collected and examined in priority order. When targets are tasked, they should be tasked according to priority. If a target's role changes, a change to the collection and processing priority will likely be in order. Some targets can be used as a protection or threat warning indicator, even though they will never go through the targeting process. Juggling too many high priorities can cause problems; it is best to keep them to a manageable number with as few tiers as possible.

**L-29.** Although some targets are useful as activity indicators, the desired end state for most targets is fixed or finished. This could range from a lethal strike to detainment, to disruption of enemy activity, through denial of key terrain.

### General Operations Guidelines

**L-30.** Day-to-day operations should consist of a plan of support, including a synchronized focus of enemy activity around friendly operations for the day. If counterintelligence or human intelligence teams will be operating in a specific area or there is a planned cordon and search occurring at a specific location, the tipper analyst should know where this area is and be prepared to tip actionable intelligence to supported operators in those areas.

**L-31.** In many cases friendly operations occur simultaneously throughout the supported AO and

will require the OIC or NCOIC to prioritize the support of these efforts. Effective prior planning by the OIC or NCOIC can alleviate some of this synchronization by coordinating the employment of nonorganic sensor coverage to facilitate comprehensive coverage of the AO.

**L-32.** Mastery of five following skills will greatly enhance the SIGINT cell's ability to operate in any environment maximizing SIGINT's effects on the AO:

- BDA analysis.
- Sanitization at the collateral level.
- Summary reporting.
- Target package production and SIGINT support to targeting.
- Development and mastery of techniques and procedures by the cell prior to deployment, then adjusted to mission needs once operational.

**L-33.** There are many possible ways to provide superior support using tactical SIGINT. The most effective methods are often well rehearsed, simple, and include a variety of collaborative inputs from combatant command, joint task force and national resources. As new technologies are employed by the enemy, Army SIGINT must be agile and adaptive enough to exploit and report this information to the individuals that need it as quickly as possible.



## Signals Intelligence Cell Duty Positions and Functions

**L-34.** There are a variety of positions and functions associated with the SIGINT cell.

### Officer in Charge (Mission Vision)

**L-35.** The SIGINT OIC has overall responsibility for the collection and reporting mission and for defining the battle rhythm. OICs should spend a large percentage of their time ensuring the team is aware of friendly operations for the day and evaluating targets to submit for prosecution. A great deal of effort is required to synchronize friendly operations with the appropriate level of support.

**L-36.** Primary OIC functions include the following:

- Makes daily evaluations of the team's effectiveness in terms of collection efficiency, reporting efficiency, and consumer satisfaction. A careful balance of real-time reporting and tipping with detailed and summary reporting is the key to ensuring valuable intelligence is disseminated as quickly as possible.
- Ensures that critical information is not held internally because the SIGINT cell lacks the entire picture.
- Serves as the collaborative interface with the collection and processing threads in the unit, such as counterintelligence, human intelligence, and imagery intelligence. This is necessary to ensure a uniform focus is applied to the unit's priority intelligence requirements.
- Ensures all production requirements are met.
- Collaborates with adjacent and higher headquarters collection and processing organizations to achieve maximum focus of available assets on the unit's targets of interest.
- Takes the lead in managing contractors and any other civilians within the SIGINT cell and ensures the collection managers are collaborating with adjacent and higher intelligence collection organizations.
- Determines the threshold and priority for reporting by evaluating the amount and type of traffic compared with the number of reporters available.
- Becomes familiar with outside intelligence organizations and clearly understand all aspects of collection, processing, and exploitation.
- Possesses sufficient knowledge of processing and collection subsystems to know what organizations to contact at specific points when common problems occur with their associated processing or collection systems.

**Noncommissioned Officer in Charge (Mission Integrity)**

**L-37.** The NCOIC has overall responsibility for the validity and quality of every report.

**L-38.** Primary NCOIC functions include the following:

- Ensures that consistent terminology, abbreviations, and acronyms are applied to all tippers and reports. Additionally, the NCOIC ensures reporting occurs in accordance with the appropriate priority and threshold set by the OIC.
- Produces or reviews the daily summary report before it is disseminated, thus ensuring the appropriate level and type of information is contained in the document. If reporting timeliness is reduced, the NCOIC should identify the problem and recommend or implement courses of action to remedy the issue.
- Works the shift opposite the OIC and is responsible for managing the targeting process in general, recommending targets to the OIC, and ensuring targeting and force protection tipper information is disseminated in a timely fashion.
- Assumes responsibility for the support characteristics of the mission, ensuring replacement parts are available or on order, equipment components are operating nominally, and the overall baseline architecture is functioning properly.
- Possesses sufficient knowledge of processing and collection subsystems to know what organizations to contact at specific points when common problems occur with their associated processing or collection systems.

**Collection Manager (Mission Stability)**

**L-39.** One person per shift is responsible for updating daily changes to the priorities of existing targets—adding, modifying, or removing targets. The collection manager works with analysts on shift to determine what targets to remove and add for collection. Anyone on the team should be able to recommend targets.

**L-40.** Primary collection manager functions include—

- Coordinating with nonorganic collection organizations to ensure all available resources are applied to high-payoff targets. At a minimum, this coordination should take place daily and all challenges and issues should be brought to the attention of the OIC or NCOIC.
- Informing the OIC or NCOIC of collection issues so they can suggest new targets for prosecution during S-3 targeting meetings and advise the leadership where additional collection focus is needed.

**Tipper Analyst (Mission Focus)**

**L-41.** Tipping threat information is critical to providing time-sensitive intelligence to the supported command. One position or person per shift should be responsible for looking for threat warning, protection, situational awareness and targeting information.

**L-42.** Primary tipper analyst functions include the following:

- Rapidly evaluates intelligence value.
- Issues threat tippers over any and all modes of communication that the cell uses.
- Informs the OIC or NCOIC of issues that require leadership decisions to respond to potential threat streams.
- Facilitates responses to RFIs.

**Reporter-Analysts (Mission Execution)**

**L-43.** The remaining available analytic personnel, (that is, SIGINT analysts [MOS 35N] personnel without the target language skills) are categorized as reporters or analysts.

**L-44.** Primary reporter-analyst functions include—

- Taking direction from the tipper analyst regarding what to report and what further analysis to

perform. In many cases a reporter or analyst will work on specified targets of interest, only to be interrupted several times to issue reports as directed by the tipper analyst.
- Assuming responsibility for the bulk of the analytic work involved in producing TACREPs, traditional SIGINT reports, target packages, and nontraditional reports.
- Working closely with the tipper analyst in order to ensure all critical information is being released as soon as it is available while following in-depth analysis streams. The two threads of execution are separate and must be accomplished asynchronously and as quickly as possible in most cases.
- Taking guidance from the OIC or NCOIC and coordinating with the collection manager, reporters prioritize new threat streams for prosecution.
- Issuing threat tippers and respond to RFIs as necessary as operations demand.

**Senior Linguist (Mission Assurance)**

**L-45.** The senior military linguist on site is responsible for the management of all available linguist resources across shifts, including military and civilian linguists working the mission. Ideally this person is trained in the target language, but this is not mandatory.

**L-46.** Primary senior linguist functions include—
- Task-organizing the indigenous linguistic assets to maximize mission efficiency. The senior military linguist coordinates daily with the OIC or NCOIC to ensure priority missions are covered.
- Developing and tailoring language processing techniques and procedures to meet mission requirements, closely coordinating with the tipper analysts and collection managers to ensure intercepts are processed at current priority.
- Providing periodic quality control of linguistic products. If the senior military linguist is dependent on civilian language support, the senior military linguist must develop a trusted working relationship with the most experienced linguist on site to coordinate quality control efforts.
- Determining the division of effort between, and amount of support to be provided, by limited linguistic resources. The senior military linguist must know the channels for requesting outside linguistic assistance as required by the mission and how to leverage linguistic support from a tactical support activity for the AO.

**Cryptologic Linguists (Mission Execution)**

**L-47.** All remaining military and civilian linguists with ability in the target language work as transcribers for local collection on priority targets.

**L-48.** Primary cryptologic linguistic functions include the following:
- Produces timely gists of intercepted communications in the established formats according to local standing operating procedures.
- Takes direction from the tipper analyst and collection manager to ensure priority traffic is processed first.
- Quickly alerts the analytic team to modify the targeting or collection process. Therefore, the cryptologic linguist must be alert for changes in target activity and personalities.
- Nominates targets for change in priority or removal from target lists, based on indicators within target intercept.

# Appendix M

# Telecommunications and Signal Fundamentals

**M-1.** This appendix contains information on telecommunications fundamentals, including basic signal theory, personal communications, networks, wireless technologies, and satellites. It is intended to give the user of this manual a basic overview of the material presented. It is not intended to serve as a replacement for further research into these subjects.

## TELECOMMUNICATIONS

**M-2.** *Telecommunication* is the transmission of messages over significant distances for the purpose of communication. In earlier times, telecommunications involved the use of visual signals, such as smoke, semaphore telegraphs, signal flags, and optical heliographs, or audio messages via coded drumbeats, lung-blown horns, or loud whistles.

**M-3.** In the modern age of electricity and electronics, telecommunications has typically involved the use of electric means. These means include the telegraph, telephone, and teletype and the use of microwave communications, fiber optics and their associated electronics, and the Internet.

**M-4.** A basic telecommunications system consists of three primary units that are always present in some form:

- A transmitter that takes information and converts it to a signal.
- A transmission medium, also called the physical channel that carries the signal (for example, the free space channel).
- A receiver that takes the signal from the channel and converts it back into usable information.

### Communications Methods

**M-5.** There are three methods by which communications systems relay information:

- **Simplex—**communication travels only one way. On television, this method of communication is called broadcasting. An important distinction of broadcasting is that it is a one-to-many communications method. Some forms of simplex may be strictly one-to-one communications method, but they do not use resources efficiently.
- **Half duplex—**relays communication in one direction at a time. A two-way radio system is like a walkie-talkie. There is only one channel of communication between each user and each one must take a turn and speak while the others listen.
- **Full duplex—**is the most popular way to relay communications. Information is transmitted both ways simultaneously. This method is the same one used when talking on the telephone.

### Signal Definitions

**M-6.** The following are some of the common terms used to describe signals:

- **Wave.** A recurring pattern that transfers energy between two distant points.
- **Frequency.** The number of times a full wave occurs per second.
- **Amplitude.** This characteristic is represented by the deflection from the lowest point of the wave to the highest point of the wave.
- **Wavelength.** The physical length of one full-length wave (Symbol – λ).

## Signal Types

**M-7.** Communications signals can be either analog or digital. These are analog or digital communications systems. An analog signal varies continuously with respect to the information. In a digital signal, information is encoded as a set of discrete values (for example, a set of ones and zeros).

### Analog Signals

**M-8.** An *analog signal* comprises different voltage levels that vary smoothly from one level to the next. Figure M-1 shows one cycle in an analog signal ranging from 0 volts, rising to positive 10 volts over time, then receding back to 0 volts, continuing on to negative 10 volts over time, then receding back to 0 volts for the start of the next cycle.

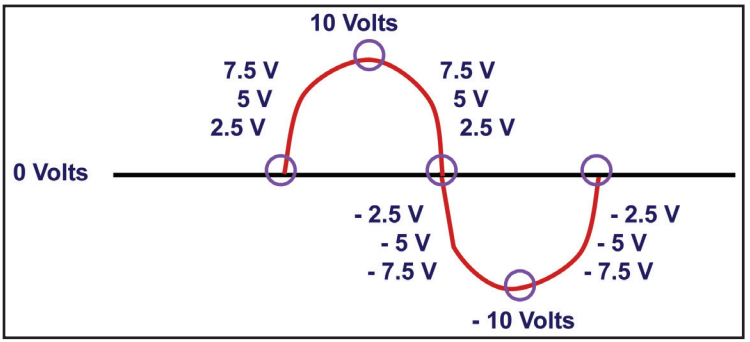



Figure M-1. One cycle of an analog signal

**M-9.** Putting several analog cycles back-to-back, measured over a period of one second, renders the bandwidth of an analog signal. If 20 cycles occur over a one-second time period, the bandwidth of the signal is 20 hertz (Hz). If 2,000 cycles occur over a one-second time period, the bandwidth of the signal is 2,000 Hz. Hz is another way to say cycles per second. (See figure M-2.)

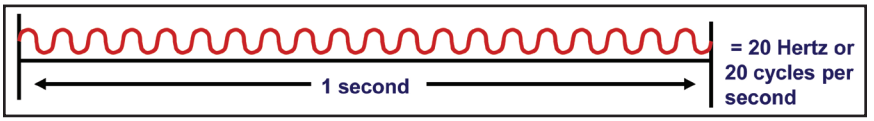



Figure M-2. Bandwidth of an analog signal

### Digital Signals

**M-10.** *Digital signals* are transmitted as binary bits that have two possible values: one or zero. In figure M-3, positive 5 volts represents a binary value of zero, while negative 5 volts represents a binary value of one. Notice that there is no smooth transition from one voltage level to the next. Digital signals are discrete and independent of each other.

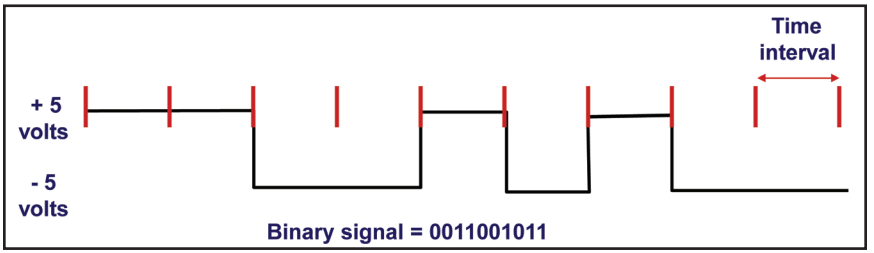



Figure M-3. Digital signal


FOR OFFICIAL USE ONLY

## Telecommunications Measurement Abbreviations

**M-11.** The following describes the measurement abbreviations used when describing telecommunications. Table M-1 shows the metric symbols used to express values in telecommunications:

- **Expressing large numbers.** Large values are expressed using the metric symbols k, M, G, or T.
- **Expressing small numbers.** The symbols used to express small numbers are d, m, µ, n, and p. In telecommunications, these symbols are often used to express voltage levels. They are also used in timing, which is expressed in fractions of a second.
  - 10/1,000 of a second = 10 milliseconds (ms).
  - 125/1,000,000 of a second = 125 microseconds (µs).

**Table M-1. Metric symbols**

| Expressing large numbers | Expressing small numbers |
|---|---|
| k = kilo = 1,000 (one thousand). | d = deci = 1/10 (one tenth). |
| M = mega = 1,000,000 (one million). | m = milli = 1/1,000 (one thousandth). |
| G = giga = 1,000,000,000 (one billion). | µ = micro = 1/1,000,000 (one millionth). |
| T = tera = 1,000,000,000,000 (one trillion). | n = nano = 1/1,000,000,000 (one billionth). |
| | p = pico = 1/1,000,000,000,000 (one trillionth). |

### Measuring Bandwidth in Analog

**M-12.** When measuring bandwidth in analog, the symbols in table M-1 are used with Hz. For example:

- 10,000 Hz = 10 kHz.
- 2,400,000 Hz = 2.4 MHz.

### Measuring Bandwidth in Digital

**M-13.** When expressing bandwidth in digital, the symbols in table M-1 are used with bits per second (bps) or bytes per second (Bps):

- 2,500,000,000 bps = 2.5 Gbps.
- 100,000,000 bps = 100 Mbps.
- 56,000 bps = 56 Kbps.

---

***Note.*** The letter k is capitalized in 56 Kbps. With most values, the letter k is lowercase. It is common practice, however, to capitalize the letter k when referencing digital values. This comes from the bytes used in storage values (like those used for hard drives). A kilobyte of storage is not 1,000 bytes; it is 1,024 bytes. The capital letter k was originally implemented to show the difference. From there, it has spread to all digital values.

---

## Communication Devices

**M-14.** The basic communications devices are—

- Radio.
- Telephone.
- Codec.
- Modem.
- Channel service unit/data service unit (CSU/DSU).

### Radio

**M-15.** A *radio* consists of a transmitter that takes information and converts it to a signal and a transmission medium, also called the physical channel that carries the signal. An example of this is

the free space channel and a receiver that takes the signal from the channel and converts it back into usable information. (See figure M-4.)

**M-16.** For example, a radio broadcasting station's large power amplifier is the transmitter and the broadcasting antenna is the interface between the power amplifier and the 'free space channel." The free space channel is the transmission medium; and the receiver's antenna is the interface between the free space channel and the receiver. Next, the radio receiver is the destination of the radio signal. It is converted from electricity to sound.

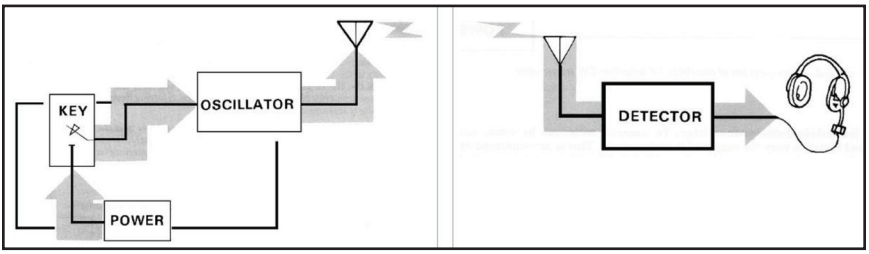



**Figure M-4. Radio components**

### Telephone

**M-17.** The two main components of the telephone are the transmitter and the receiver. Each component contains a transducer for converting energy from one form to another. The microphone converts an acoustical energy (speech) to electrical energy, while the speaker converts electrical energy from the public switched telephone network (PSTN) back to acoustical energy. (See figure M-5.)

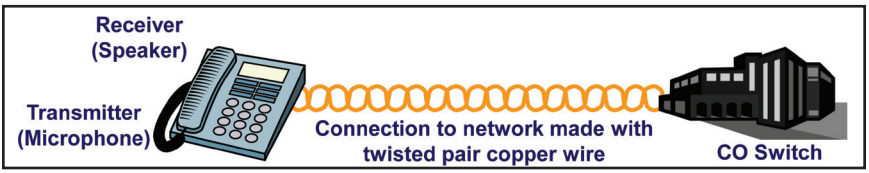



**Figure M-5. Telephone components**

### Codec

**M-18.** A *codec* converts analog signals into digital signals for transmission over a digital network. On the receiving end, another codec receives the information and converts the signal back to analog. (See figure M-6.)

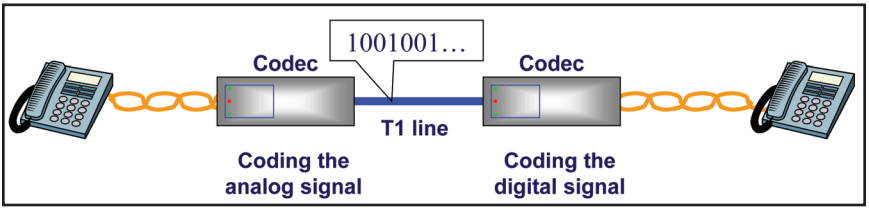



**Figure M-6. Codec components**


FOR OFFICIAL USE ONLY

### Modem

**M-19.** A *modem* converts a digital (unipolar) signal to analog for transmission over an analog network. The carrier signal is removed and the data is converted to its original digital form when the modulated analog signal arrives at its destination. (See figure M-7.)

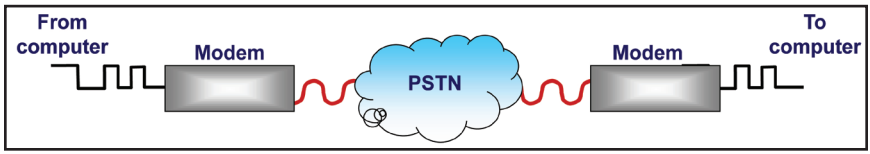



**Figure M-7. Modem components**

### Channel Service Unit/Data Service Unit

**M-20.** A *CSU/DSU* transports a digital signal over a digital line. A DSU takes the digital unipolar signal, which means a signal with two states for a binary value of one and zero, and converts them to a bipolar signal that is more suitable for transmission over long distances. A CSU performs certain coding, line conditioning, and equalization functions, and responds to loop-back commands sent over the circuit from the service provided for testing. (See figure M-8.)

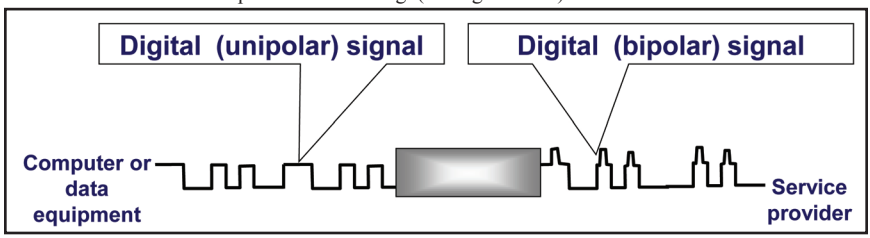



**Figure M-8. CSU/DSU components**

# SIGNAL FUNDAMENTALS

**M-21.** A signal is information transmitted by means of a modulated current or an electromagnetic wave and received by telephone, telegraph, radio, television, or radar.

## ELECTROMAGNETIC SPECTRUM

**M-22.** An electromagnetic wave is an analog waveform produced by inducing a current in a pair of conductors. These waveforms can range in frequency from 30 Hz to beyond 300 GHz. This frequency range, largely made up of radio waves and microwaves, is called the electromagnetic spectrum. (See figure M-9.)

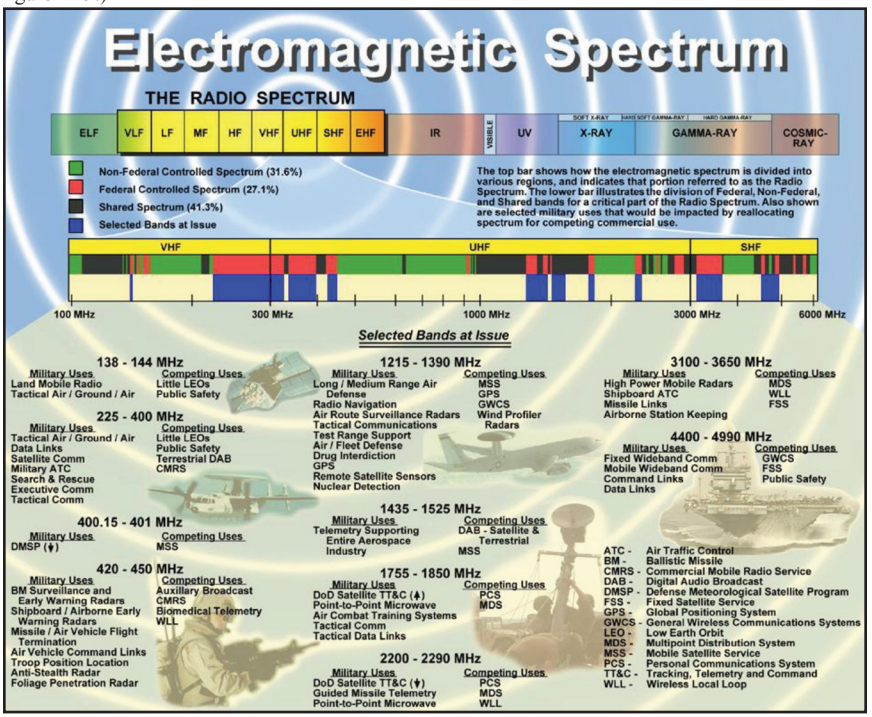



**Figure M-9. Electromagnetic and radio spectrums**

### Frequency Bands

**M-23.** The electromagnetic spectrum is divided into frequency bands (as shown in figure M-10). The frequency range of each band is 10 times the frequency range of the band before it.

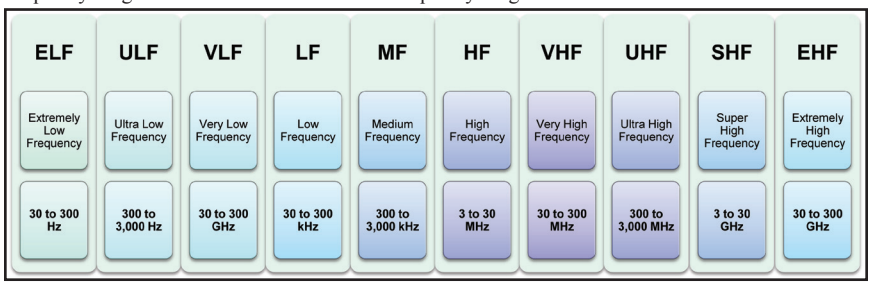



**Figure M-10. Frequency bands**

### Frequency Ranges

**M-24.** Current communications systems use frequencies in one of the following bands: televisions and cellular phones operate in the very high frequency (VHF) and ultra high frequency (UHF) bands, while satellites operate a little higher (super high frequency [SHF] band). In contrast, the frequency range of the human voice is much lower (very low frequency [VLF] band). Frequency ranges are—

- **Audible range**—30 Hz to 20 kHz (VLF, ultra low frequency [ULF], extremely low frequency [ELF]).
- **Voice band**—300 Hz to 3,400 Hz (VLF, ULF).
- **AM broadcast**—540 to 1,710 kHz (medium frequency [MF]).
- **Cordless phone**—43 to 50 MHz (VHF).
- **Broadcast TV (ch 2-13)**—54 to 216 MHz (VHF).
- **FM broadcast**—88 to 108 MHz (VHF).
- **Broadcast TV (ch 14-69)**—470 to 800 MHz (UHF).
- **Cellular phone**—824 to 924 MHz (UHF).
- **Personal communication system (PCS)**—1,850 to 2,000 MHz (UHF).
- **Satellite links (C and Ku Bands)**—4 to 18 GHz.

### Higher Frequencies

**M-25.** The electromagnetic spectrum extends beyond the EHF band. Figure M-11 shows some of the energy forms that propagate within these higher frequencies, including light, x-rays, and gamma rays. Fiber optic cables transport light in the infrared range.

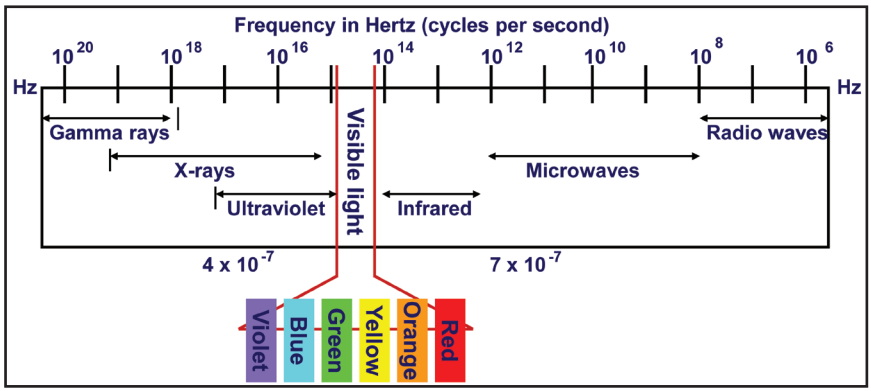



**Figure M-11. Electromagnetic spectrum above extremely high frequency band**

### Wave Measurement

**M-26.** Waves at higher frequencies are usually measured in terms of their wavelength. Wavelength is the length of a waveform from one point on the wave to the same point on the next wave. It is measured in meters, but at higher frequencies, the wavelengths are so small that nanometers (billionths of a meter) are used.

## Modulation and Demodulation

**M-27.** Key definitions and concepts of modulation include (see figure M-14)—

- **Carrier wave.** A radio frequency that will be mixed with the information wave.
- **Information or intelligence wave.** The wave that contains the information or intelligence to be transmitted.
- Carrier wave + information or intelligence wave = modulated wave.

### Modulation

**M-28.** *Modulation* is the process of varying the amplitude or frequency characteristics of a carrier wave in accordance with the amplitude or frequency changes in the intelligence wave to convey information through free space.

**M-29.** In an analog communications system, the analog modulator equipment mixes with a carrier signal. This produces a modulated analog signal at the output. In a digital communications system, a pulse modulator produces a digitally modulated signal. (See figure M-12.)

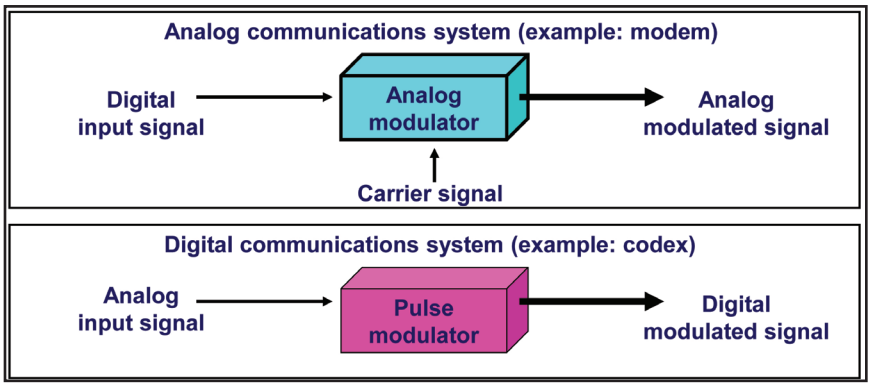



Figure M-12. Modulation example


FOR OFFICIAL USE ONLY

### Demodulation

**M-30.** In demodulation, the modulation process is reversed. In an analog communications system, the carrier signal is removed from the modulated signal in the analog modulator equipment. This produces a close replica of the original input signal. Noise prevents the signal from being an exact copy of the original input. In a digital communications system, the pulse modulator creates an exact copy of the original digital signal. Binary code can theoretically be transported exactly as it is sent, so it is decoded exactly as it is encoded. (See figure M-13.)

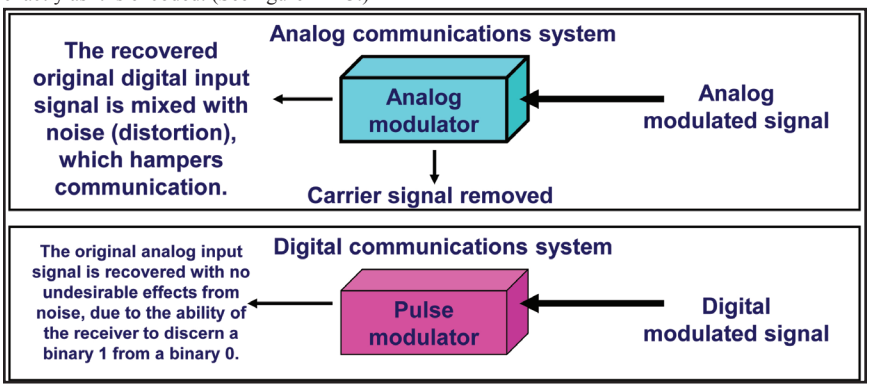



**Figure M-13. Demodulation example**

### Amplitude Modulation

**M-31.** *Amplitude modulation (AM)* is the variation of the radio frequency (RF) power output of a transmitter at an audio rate. In other words, the RF energy increases and decreases according to the audio frequencies (AFs) superimposed on the carrier signal. When AF signals are superimposed on the RF carrier signal, additional RF signals are generated. These additional frequencies are equal to the sum and the difference of the AFs and the radio frequency used. For example, assume a 500 kHz carrier is modulated by a 1 kHz audio tone. Two new frequencies are developed, one at 501 kHz (the sum of 500 kHz and 1 kHz) and the other at 499 kHz (the difference between 500 kHz and 1 kHz). If a complex audio signal is used instead of a single tone, two new frequencies will be set up for each of the AFs involved. The new frequencies resulting from superimposing an AF signal on an RF signal are called sidebands. (See figure M-14.)

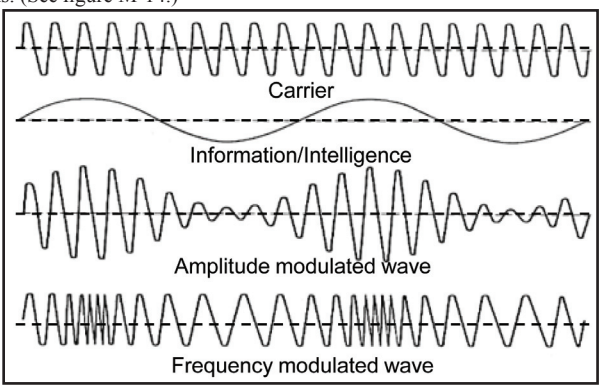



**Figure M-14. Wave shapers**

**M-32.** As described previously, when the RF carrier is modulated by complex tones, such as speech, each separate frequency component of the modulating signal produces its own upper and lower sideband frequencies. (See figure M-15.) These additional frequencies occupy sidebands. The sideband that contains the sum of the RF and AF signals is the upper sideband (USB). The sideband that contains the difference between the RF and AF signals is the lower sideband (LSB).

**M-33.** The space occupied by a carrier and its associated sidebands in the RF spectrum is called a channel. In AM, the width of the channel (bandwidth) is equal to twice the highest modulating frequency. For example, if a 5000 kHz (5 MHz) carrier is modulated by a band of frequencies ranging from 200 to 5000 cycles (0.2 to 5 kHz), the USB extends from 5000.2 to 5005 kHz. The LSB extends from 4999.8 to 4995 kHz. Thus, the bandwidth is the difference between 5005 and 4995 kHz, a total of 10 kHz.

### Amplitude-Modulated System

**M-34.** AM generally is used by radiotelephone and radio teletypewriter transmitters operating in the medium and high frequency bands. The intelligence of an amplitude modulated signal exists solely in the sidebands.

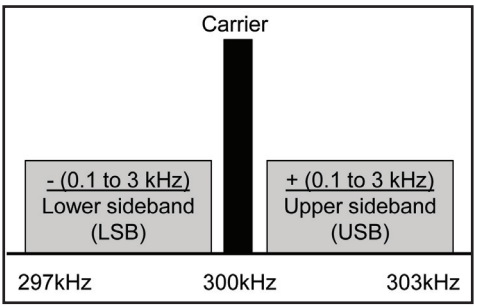



**Figure M-15. Amplitude modulation system**

**M-35.** Each sideband alone contains all the intelligence needed for communication. Since this is true, it may be correctly inferred that one sideband and the carrier signal can be eliminated. This is the principle on which single sideband (SSB) communications is based. Although both sidebands are generated within the modulation circuitry of the SSB radio set, the carrier and one sideband are removed before any signal is transmitted. (See figure M-16.)

**M-36.** The sideband that is higher in frequency than the carrier is USB. The sideband that is lower in frequency than the carrier is LSB. Either sideband can be used for communications as long as both the transmitter and the receiver are adjusted to the same sideband. Most Army SSB equipment operates in the USB mode.

**M-37.** The transmission of only one sideband leaves open that portion of the RF spectrum normally occupied by the other sideband of an AM signal. This allows more emitters to be used within a given frequency range.

**M-38.** SSB transmission is used in applications where it is desired to—

- Obtain greater reliability.
- Limit size and weight of equipment.
- Increase effective output without increasing antenna voltage.
- Operate a large number of radio sets without heterodyne interference (whistles and squeals) from RF carriers.
- Operate over long ranges without loss of intelligibility due to selective fading.

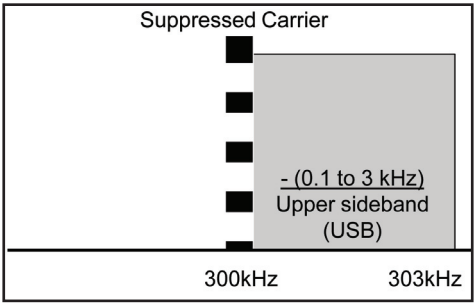



**Figure M-16. Single-sideband system**

### Frequency Modulation

**M-39.** *Frequency modulation (FM)* is the process of varying the frequency (rather than the amplitude) of the carrier signal in accordance with the variations of the modulating signals. The amplitude or power of the FM carrier does not vary during modulation. The frequency of the carrier signal when it is not modulated is called the center or rest frequency. When a modulating signal is applied to the carrier, the carrier signal will move up and down in frequency, away from the center or rest frequency.

**M-40.** The amplitude of the modulating signal determines how far away from the center frequency the carrier will move. This movement of the carrier is called deviation; how far the carrier moves is called the amount of deviation. During reception of the FM signal, the amount of deviation determines the loudness or volume of the signal.

**M-41.** The FM signal leaving the transmitting antenna is constant in amplitude, but varies in frequency according to the audio signal. As the signal travels to the receiving antenna, it picks up natural and manmade electrical noises that cause amplitude variations in the signal. All of these undesirable amplitude variations are amplified as the signal passes through successive stages of the receiver until the signal reaches a part of the receiver called the limiter. The limiter is unique to FM receivers, as is the discriminator.

**M-42.** The limiter eliminates the amplitude variations in the signal, and then passes it on to the discriminator, which is sensitive to variations in the frequency of the RF wave. The resultant constant amplitude, frequency modulated signal is then processed by the discriminator circuit, which changes the frequency variations into corresponding voltage amplitude variations. These voltage variations reproduce the original modulating signal in a headset or loudspeaker.

## Multiplexing

**M-43.** *Multiplexing* combines communications channels over one physical transmission link, allowing a higher data rate (throughput). The types of multiplexing include—

- Frequency division multiplexing (FDM).
- Time division multiplexing (TDM).
- Wave division multiplexing (WDM).
- Code division multiplexing (CDM).

**M-44.** Figure M-17 shows four channels connected to the multiplexer at one end of the transmission link. The job of the multiplexer is to combine the signals of the four individual communication channels into one signal transmission link.

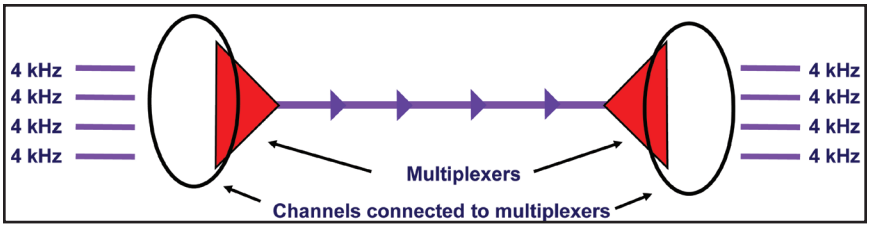



Figure M-17. Multiplexing

### Frequency Division Multiplexing

**M-45.** FDM was the first type of multiplexing developed. FDM divides channels by using a different frequency range for each channel. If each channel were 3,100 Hz, the transmission equipment and medium being used would have to support a bandwidth of 12,400 Hz. The multiplexing equipment incorporates a guard band between channels to keep them from interfering with each other. (See figure M-18.)

**M-46.** Cable television systems use FDM, with each channel using 6 MHz of bandwidth. Cable systems usually support from 750 MHz to 1 GHz of overall bandwidth. This allows them to support a large number of video channels.

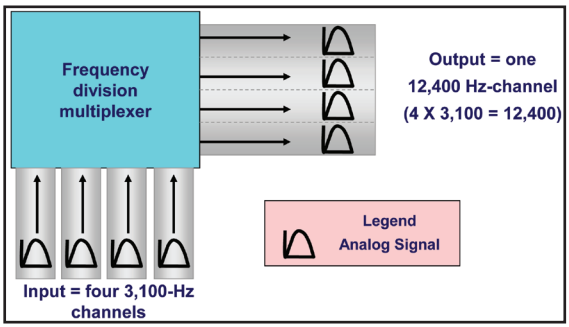



Figure M-18. Frequency division multiplexing

### Time Division Multiplexing

**M-47.** The problem with FDM is that it uses analog signals. During the transmission of voice or data signal noise is picked up. TDM eliminates this problem by converting the analog signal to digital. The multiplexer divides the channels into time slots, which are transmitted one at a time over the network. (See Figure M-19.)

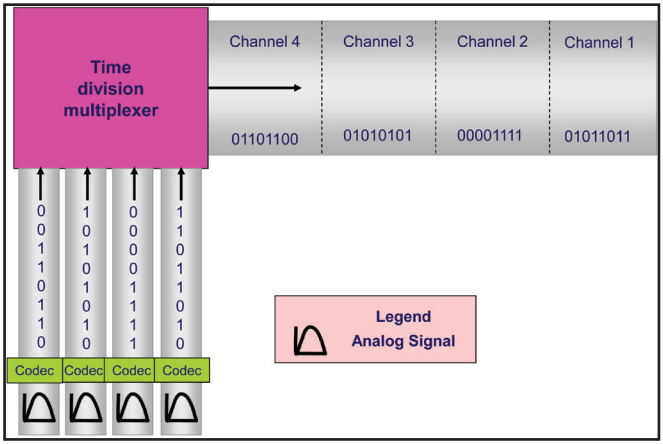



**Figure M-19. Time division multiplexing**

***Time Division Multiplexing Bandwidth Allocation***

**M-48.** In FDM, the total bandwidth is divided equally among the transmitted channels. TDM allocates the full bandwidth of the line to each channel individually, but each channel is transmitted separately. (See figure M-20.)

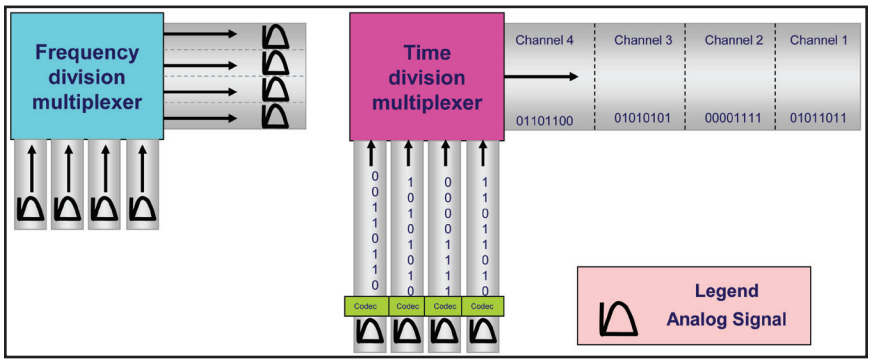



**Figure M-20. FDM and TDM comparison**

**M-49.** T1 uses TDM by employing a channel bank, which is a multiplexer combined with codecs, to interweave the channels into 24 time slots. (See figure M-21.) Each slot contains 8 bits, and the 24 time slots are transmitted 8,000 times per second. T1 also uses one framing bit for every 24 time slots to maintain timing between channel banks and other network equipment. This yields a total transmission speed of 24 channels × 8 bits × 8,000 times per second + 8,000 framing bps = 1,544,000 bps (1.544 Mbps).

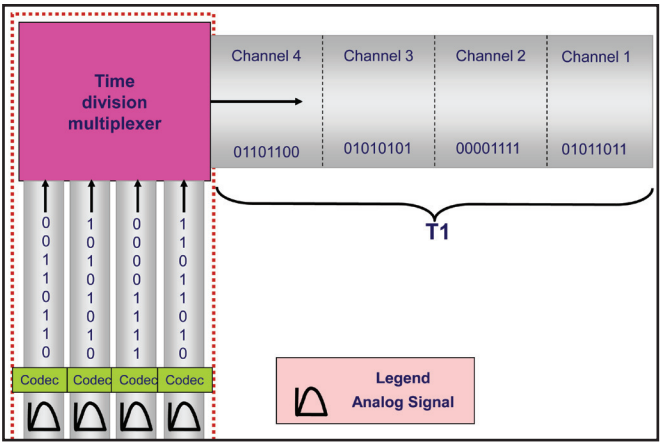



**Figure M-21. T1 example of TDM**

*Statistical Time Division Multiplexing*

**M-50.** Statistical time division multiplexing (STDM) dynamically allocates a share of the available transmission bandwidth to channels. In STDM, a line is not assigned to one specific time slot. When the communication must be transmitted, the next available time slot is used. STDM generally allows more information to be transmitted over the same type of facility than TDM allows. (See figure M-22.)

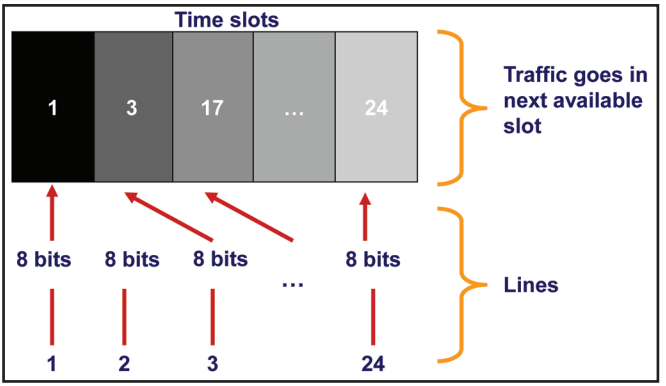



**Figure M-22. Statistical time division multiplexing**

**M-51.** STDM allows overbooking. By having more lines than available channels connected to the system, more users can be accommodated. There are usually fewer active lines than channels. Statistical multiplexers have buffers to hold data so that even if there are more active lines than channels, no data is lost.

**Wave Division Multiplexing**

**M-52.** WDM is used for optical transmission. (See figure M-23.) During transmission, a wave division multiplexer receives four separate optical inputs driven by lasers operating in four different wavelengths. The wavelengths are combined over one fiber optic transmission path and sent to the destination.


FOR OFFICIAL USE ONLY

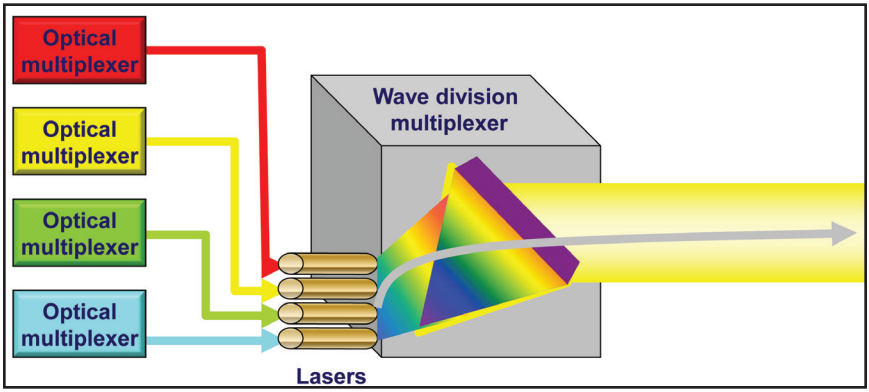



Figure M-23. WDM transmission

**M-53.** At the receiving end, the signal is filtered into four separate paths. (See figure M-24.) The filtering process divides the signal strength for each output and filters the signal into the different wavelengths. The next step is to amplify the incoming signals so that they can be accurately presented to the optical multiplexers connected to each output channel.

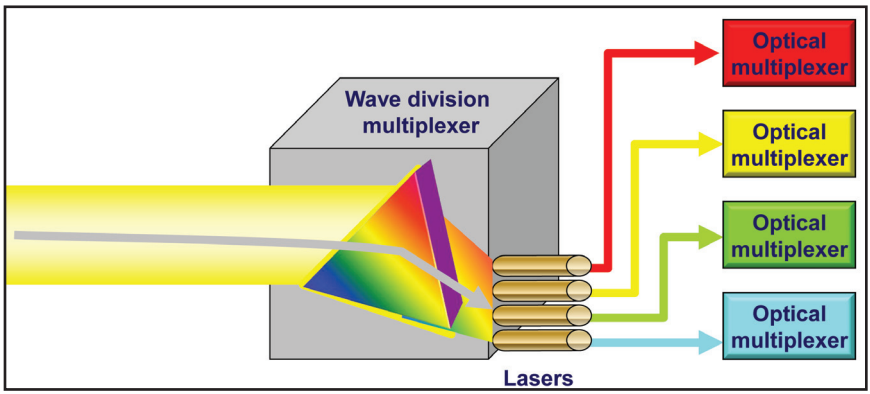



Figure M-24. WDM reception

### Code Division Multiplexing

**M-54.** An additional method is CDM. (See figure M-25.) Instead of each channel occupying a given wavelength, frequency, or time slot, each channel transmits its bits as a coded channel-specific sequence of pulses. This coded transmission typically is accomplished by transmitting a unique, time-dependent series of short pulses. These short pulses are placed within chip times within the larger bit time. All channels, each with a different code, can be transmitted on the same fiber and asynchronously demultiplexed. One effect of coding is that the frequency bandwidth of each channel is broadband, or "spread." If ultra-short, optical pulses can be successfully generated and modulated, then a significant fraction of the fiber bandwidth can be used. Unfortunately, it is difficult for the entire system to operate at these speeds without enormous cost and complexity.

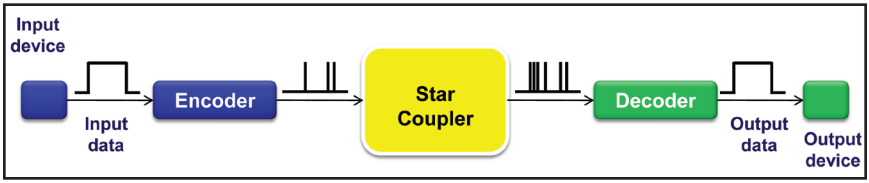



Figure M-25. Code division multiplexing

## Radio Wave Propagation

**M-55.** The following are definitions related to radio wave propagation (see figure M-26):

- **Reflection.** The turning back of a radio wave from an object, the ionosphere, or the surface of the Earth.
- **Refraction.** The bending or change in direction of a radio wave passing through mediums of different density.
- **Diffraction.** The ability of a radio wave to bend around an object.
- **Scatter.** The deflection of a radio wave in several different directions.
- **Absorption.** The removal of energy from a radio wave as it passes through the atmosphere or over the surface of the Earth.

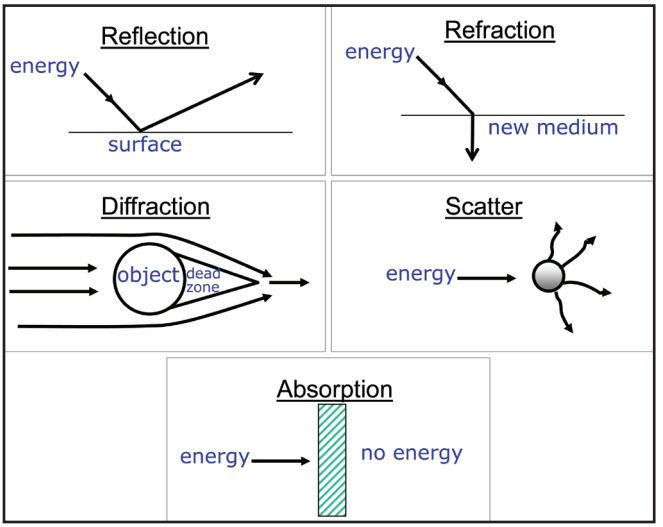



Figure M-26. Radio wave propagation

### Radio Wave Propagation Paths

**M-56.** Propagation paths are the ways a wave travels. Ground waves travel directly from the transmitter to the receiver. Sky waves travel up to the ionosphere and are refracted (bent downward) back to the Earth. Short distance, and all UHF and upper VHF transmissions, are accomplished by ground waves. Long distance transmission is accomplished principally by sky waves. Single-channel radio sets can use either ground wave or sky wave propagation for communications.

#### *Ground Wave Propagation*

**M-57.** Radio communications, which use ground wave propagation, do not use or depend on waves

that are refracted from the ionosphere (sky waves). Ground wave propagation is affected by the electrical characteristics of the Earth and by the amount of diffraction (bending) of the waves along the curvature of the Earth. The strength of the ground wave at the receiver depends on the power output and frequency of the transmitter, the shape and conductivity of Earth along the transmission path, and the local weather conditions. The following components of a ground wave include—

- **Direct wave.** The part of the radio wave that travels directly from the transmitting antenna to the receiving antenna. This part of the wave is limited to the line-of-sight (LOS) distance between the transmitting and receiving antennas, plus the small distance added by atmospheric refraction and diffraction of the wave around the curvature of the Earth. This distance can be extended by increasing the height of either the transmitting or the receiving antenna, or both.
- **Ground deflected wave.** The portion of the radio wave that reaches the receiving antenna after being reflected from the surface of the Earth. Cancellation of the radio signal can occur when the ground reflected component and the direct wave component arrive at the receiving antenna at the same time and are 180 degrees out of phase with each other.
- **Surface wave.** The part of the ground wave that is affected by the conductivity and dielectric constant of the Earth. The surface wave follows the curvature of the Earth.
- **Tropospheric scatter wave.** A modified direct wave path that is reflected or scattered by the troposphere back to Earth on a predictable path. (See figure M-27.)

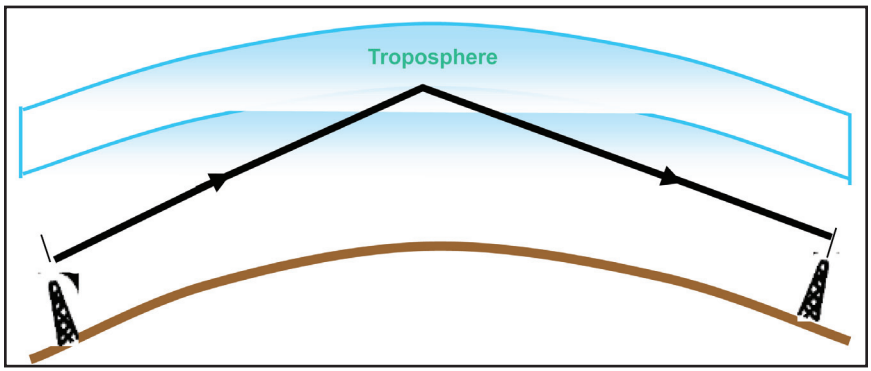



**Figure M-27. Tropospheric scatter wave**

***Sky Waves Propagation***

**M-58.** Sky waves are radio waves that are reflected back to Earth by the ionosphere (see figure M-28):

- **Skip distance.** The ground distance from the transmitter to the area where the sky wave first returns to the Earth.
- **Skip zone.** The area between the location where the last ground wave terminates (cannot be received) to the area where the sky wave first returns to Earth.

---

***Note.*** No communications are possible with the transmitting station if the receiver is in the skip zone.

---

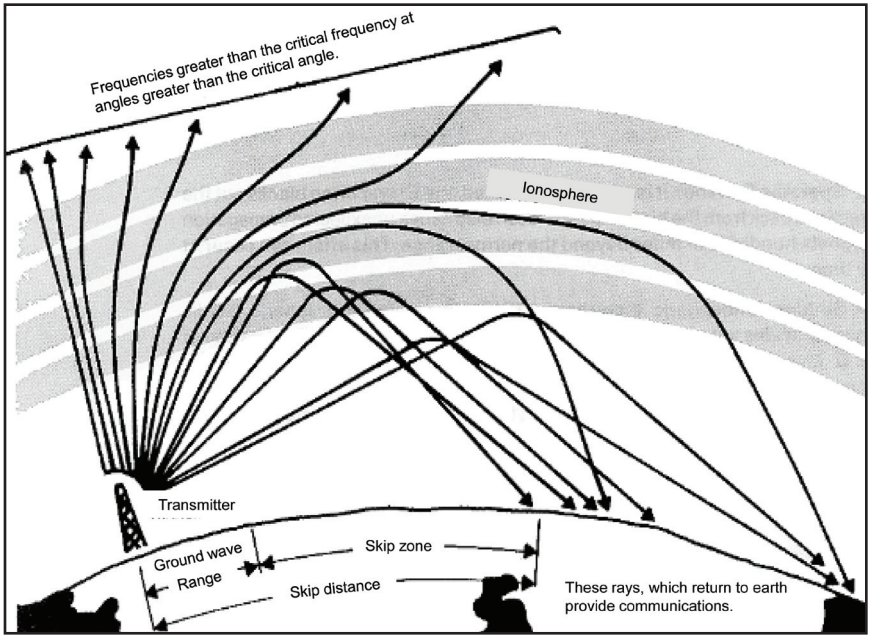



**Figure M-28. Reflection of sky waves**

### Radio Wave Propagation Weather and Terrain Factors

**M-59.** The following factors affect telecommunications:

- **Heavy rainfall**—causes excessive absorption and may reduce the transmission or receiving range of VHF and above radio equipment.
- **Lack of humidity**—induces static.
- **Extreme cold**—causes radio signals to fade and sometimes be blacked out totally.
- Jungle or vegetation—causes increased absorption, which shortens the range of transmitters.
- **Mountains**—are effective obstacles to LOS radio signals because of increased absorption. Mountains can increase LOS transmissions when communicating between high areas to lower lands.
- **Urban or built-up areas**—cause increased absorption and reflection, which shortens the range of transmitters. There will be increased interference from other transmitters within the area.

## Antennas

**M-60.** The functions of antennas can be simplified to transmission and reception of electromagnetic energy:

- **Transmit antennas**—transform the output RF energy produced by a radio transmitter into an electromagnetic field that is radiated through space.
- **Receive antennas**—act as a collector that draws electromagnetic energy into RF energy.

### Antenna Directivity

**M-61.** An antenna's ability to radiate or receive electromagnetic energy is based on directivity—the property of an antenna of being more sensitive in one direction than in another:

- **Omnidirectional**—radiates or receives electromagnetic energy equally in all directions. In an omnidirectional system, the antenna does not have to be aimed in the direction of the receiver.

The signal is projected in a 360-degree radius from the antenna; thus, more power is required for an omnidirectional system than for a directional system.

- **Bidirectional**—radiates or receives electromagnetic energy mainly in two directions.
- **Directional**—radiates or receives electromagnetic energy primarily in one direction.

### Dominant Polarization by Frequency Bands

**M-62.** Polarization gives transmission signals a direction by concentrating the beam of energy. Two forms of polarization are vertical and horizontal.

**M-63.** Extremely low frequency (ELF), very low frequency (VLF), low frequency (LF), and medium frequency (MF) work best using vertical polarization. However, in LF and lower, antenna length makes vertical polarization impractical. Lower frequencies are used with antennas that are designed to produce strong ground waves that can travel long distances. Examples include large vertical towers used by commercial AM broadcast stations.

**M-64.** High frequency (HF) uses both vertical and horizontal polarization. Vertical polarization is preferred for short range omnidirectional ground wave transmissions. Horizontal polarization is used for sky wave communications. The receiving antenna can be either vertically or horizontally polarized.

### Grounding Effects

**M-65.** The presence of ground near an antenna alters the free space radiation patterns of the antenna. Some antennas require good ground to operate correctly. For these antennas, two types of grounds can be used—natural Earth ground or counterpoise:

- **Natural Earth ground**—connects the antenna to the Earth using a highly conductive metal such as a grounding rod, buried wire, screen, or an underground water pipe.
- **Counterpoise**—is used when natural Earth ground connection cannot be used. A counterpoise is a device composed of wire or mass of metal that must be kept above the Earth's surface and insulated from it. A tactical counterpoise is the use of a vehicle—tracked, wheeled, or airframe as a counterpoise.

### Antennas and Wavelength

**M-66.** Antenna size is often referred to relative to wavelength. For example, a 1/2 wave dipole is approximately half a wavelength long. Wavelength is the distance a radio wave travels during one cycle. The formula for wavelength is: **wavelength = speed of light ÷ frequency**.

**M-67.** Wavelength, frequency, and the speed of light are related. The length of a radio wave for a given frequency when multiplied by that operating frequency equals the speed of light.

## Antenna Types

**M-68.** Figure M-29 depicts common antenna types and their directivity, polarization, advantages, and disadvantages.

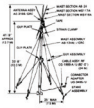
| Antenna Type | Directivity | Polarization | Advantages | Disadvantages |
|---|---|---|---|---|
|  Whip | Omnidirectional | Primarily vertical | -Highly mobile<br>-Do not need to know receivers location<br>-Extremely compact | -Susceptible to jamming<br>-Insufficient use of transmitter power<br>-No control over emanations |
|  Ground Plane | Omnidirectional | Primarily horizontal (vertical can be used) | -Better range than whip<br>-No requirement to know other station's location<br>-More efficient use of transmitter power | -Can not transmit on the move<br>-Setup time is 15-30 minutes<br>-No control over emanations |
|  Dipole | Bidirectional | Primarily vertical | -Extended transmission range<br>-Very good for sky wave propagation<br>-More efficient use of transmitter power | -Setup time is 30 minutes<br>-Can not transmit on the move<br>-Antenna length must be changed when freq is changed<br>-Must know direction of other station |
|  Near Vertical Incident Sky wave | Omnidirectional | Primarily vertical | -Very good for short distance sky wave propagation<br>-Falls in the sky wave transmission skip zone | -Setup time consuming<br>-Can not transmit on the move<br>-Can only be used in a set frequency range |
|  Log Periodic Array (LPA) | Unidirectional | Horizontal or vertical | -Concentrates majority of power in one direction<br>-Very good at receiving from one direction<br>-Good jamming antenna | -Setup time is 15 minutes<br>-Not mobile<br>-Must know location of other stations |
|  Reflector "Parabolic Dish" | Unidirectional | Horizontal or vertical | -Concentrates majority of power in one direction<br>-Very good at receiving from one direction | -Setup time is 15-45 minutes<br>-Not mobile<br>-Must know location of other stations |
| (H-Adcock)  Adcock | Omnidirectional | Primarily vertical | -Very good receiving antenna<br>-Can be used for direction finding<br>-Relatively simple reliable | -Setup time is 15 minutes<br>-Can not be used for transmitting |

**Figure M-29. Antenna types**

## Antenna Deployment Factors

**M-69.** The following are factors for Soldiers to consider when using antennas during deployment:

- **Terrain.** Not all antennas can be used in all terrain, sometimes field expedient antennas must be used because of terrain restrictions. Use surrounding terrain features to mask unintentional radiations towards the enemy. Make use of cover and concealment practices to protect antennas

from visual observation.

- **Range.** When determining the antenna type, Soldiers consider how much range is required. Increased range means increased susceptibility to intercept and jamming from threat units, as well as increased operating range.
- **Directivity.** When possible, it is best to consider a unidirectional antenna to reduce the susceptibility to interception, direction finding, and jamming. It is not always possible. In mobile or fluid situations, where the location of other stations in the net are unknown, omnidirectional antennas are best.
- **Time.** In all cases where time is available, Soldiers set up the antenna that gives the best range with the narrowest directivity. Soldiers who will be on a site for a reasonable period of time use a better antenna; when they do not have time, Soldiers use a more mobile antenna.



# WIRELESS COMMUNICATIONS

**M-70.** In wireless communications, free space is used to carry the modulated signal between the transmitter and the receiver. Factors that impair wireless transmission include—

- **Free space loss.** An omnidirectional signal that loses its power over distance.
- **Multipath fading.** A signal that is propagated through the air sometimes reflects off buildings or other objects before it arrives at the receiver. Meanwhile, the unreflected signal is being collected by the receiver. This phenomenon, known as multipath fading or Rayleigh fading, causes a phase difference between the two signals that must be compensated before clear communication can take place.
- **Co-channel interference.** Two wireless communication links, in fairly close proximity to each other, share the same frequency for transmission or reception. The two signals interfere with one another and prevent clear conversation from occurring.
- **Transmission impairments.**

## Wireless Telephony

**M-71.** The first mobile phone service began with the introduction of mobile telephony service (MTS) in 1946. This early system required an operator to connect calls to and from a mobile phone. In 1966, the improved mobile telephone service (IMTS) was introduced. With IMTS, users could randomly access any available channel by automatically searching all available channels and selecting a specific one for use. IMTS also offered automatic dialing, which eliminated the need for operator assistance. The early MTS service was a push-to-talk operation. IMTS replaced that system with full-duplex service, thus allowing users to talk and listen simultaneously.

**M-72.** Early MTS/IMTS systems used a single, central base station that transmitted at a relatively high power (250 watts). High power was required to allow the single base station the ability to reach all portions of its coverage area. Early mobile units were bulky and transmitted at relatively high power (35 watts). The mobile units required high power to allow units at the edges of the coverage area to reach the central antenna. The radio transmission techniques used by these early systems mirrored those used by traditional mobile radio systems. These early systems used FM and had limited capacity. Typically, only six to eight channels per band were available in each coverage area. This meant that only a limited number of individuals could use the system at any given time. To solve the capacity problem, a team of researchers developed a cellular approach to mobile telephony. Under the cellular radiotelephony concept, a service area would be subdivided into many smaller areas called cells (hence the name, "cellular telephony"). Instead of using the traditional single large antenna to cover the entire service area, the cellular approach uses many smaller antennas, each covering only a small segment (cell) of the entire service area. (See figure M-30.)

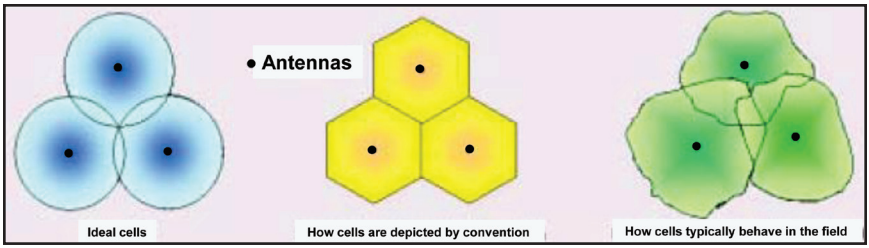



Figure M-30. Cells

### Frequency Reuse

**M-73.** Due to the small size of the cells and the subsequent reduction in the need for high transmission power, the RFs available in the service area can be shared among the cells and reused, thus increasing capacity. This is the main reason for using the cellular approach—increased capacity through frequency reuse.

### Cell Types

**M-74.** In a mobile phone system, a cell can be either an omni cell or a sectored cell. An omni cell uses omnidirectional antennas that radiate power equally in all directions. With omnidirectional antennas, gain greater than unity is achieved by forming a collinear vertical array, which reduces the elevation beam width but leaves the azimuth (horizon) pattern unaffected. Omni cells typically have as few as three antennas—one to transmit and two to receive. The two receive antennas are typically used to provide space diversity reception. (See figure M-31.)

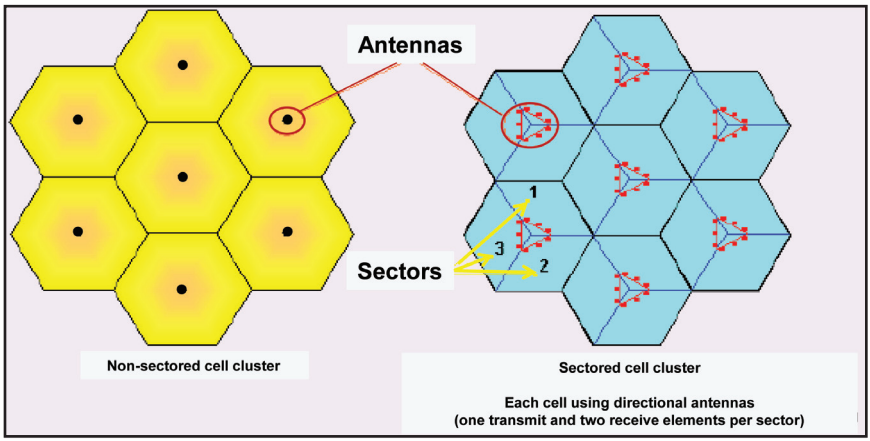



Figure M-31. Omni and sectored cells

## Wireless Telephony Technology

**M-75.** Over the years, three generations—first generation (1G), second generation (2G), and third generation (3G)—of wireless telephony have been implemented. Examples of these generations are provided in the following discussion.

### First Generation

**M-76.** 1G wireless telephony includes the following systems:

- Advanced Mobile Phone System (AMPS). A 1G system developed in the 1970s and first used


FOR OFFICIAL USE ONLY

commercially in the United States in 1983. It operates in the 800 MHz band and is currently the world"s largest cellular standard.
- Total Access Communications System (TACS). A 1G system that is similar to AMPS. Known as JTAC in Japan, TACS was first used in the United Kingdom in 1985. It operates in the 900 MHz frequency range throughout North America.

### Second Generation

**M-77.** The main differentiator to previous mobile telephones, retroactively dubbed 1G, is that 1G networks process analog data but 2G networks are digital. 2G technologies can be divided into time division multiple access (TDMA)-based and code division multiple access (CDMA)-based standards depending on the type of multiplexing used. The main 2G standards are global system for mobile communications (GSM), TDMA and CDMAone:

- **GSM—**(TDMA-based) originally from Europe but used worldwide.
- **IDEN—**(TDMA-based) a proprietary network used by Nextel in the United States and Telus Mobility in Canada.
- **IS-136—**(TDMA-based; commonly referred to as TDMA in the United States) used in the Americas.
- **IS-95—**(CDMAone used by Sprint/Verizon is CDMA-based, commonly referred as simply CDMA in the United States) is used in the Americas and parts of Asia.
- **PDC—**(TDMA-based) used exclusively in Japan.

**M-78.** 2.5G extensions, which enable high-speed data transfer over upgraded existing 2G networks, are general packet radio services (GPRS) and enhanced data rate for GSM (EDGE):

- **GPRS—**(nonvoice protocol) allows for wireless Internet/intranet and multimedia services and connects users directly to Internet service providers.
- **EDGE—**builds on GPRS and allows GSM operators to use existing GSM radio bands to offer wireless multimedia Internet protocol (IP)-based services and applications at theoretical maximum speeds of 384 kbps with a bit-rate of 48 kbps per timeslot and up to 69.2 kbps per time slot in good radio conditions.

### Third Generation

**M-79.** 3G is commonly used in the context of cell phones. The services associated with 3G provide the ability to transfer both voice data (a telephone call) and nonvoice data (such as downloading information, exchanging e-mail, and instant messaging. The main 3G standards are—

- **Universal telecommunication system (UMTS)—**a specific implementation of W-CDMA within the 2.1GHz band, which is the frequency that is made available for 3G in Europe and other parts of the world. It is an implementation of 3G and it supports speeds between 384 kbps and 2 Mbps. When this protocol is used in a wide area network (WAN), the top speed is 384 kbps. When it is used in a local area network (LAN), the top speed is 2 Mbps. Also adopted by the International Telecommunications Union (ITU). W-CDMA is based on the Direct Spread CDMA technique.
- **CDMA2000—**an outgrowth of the earlier 2G CDMA standard IS-95. CDMA2000's primary proponents are outside the GSM zone in the Americas, Japan, and Korea. CDMA2000 offers data rates of 144 kbps to over 3 Mbps.

## Global System for Mobile Communications

**M-80.** Key GSM network terms are (see figure M-32)—

- **Mobile station (MS)—**physical equipment used by a subscriber, most often a normal hand-held cellular telephone.
- **Base transceiver station (BTS)—**comprises the radio transmission and reception devices, and also manages the signal processing related to the air interface.
- **Base station controller (BSC)—**manages the radio interface, mainly through the allocation,

release and handover of radio channels.

- **Mobile switching center (MSC)—**an integrated services digital network ISDN-switch, coordinating and setting up calls to and from MSs. An interworking function (IWF) may be required to adapt GSM specific rates to that used in a particular PSTN.
- **Visitor location register (VLR)—**contains all the subscriber data, both permanent and temporary, which are necessary to control a MS in the MSCs coverage area. The VLR is commonly realized as an integral part of the MSC, rather than a separate entity.
- **Authentication center (AuC)—**database that contains the subscriber authentication keys and the algorithm required to calculate the authentication parameters to be transferred to the HLR.
- **Home location register (HLR)—**database that is used to store permanent and semipermanent subscriber data; as such, the HLR will always know in which location area the MS is (assuming the MS is in a coverage area), and this data is used to locate an MS in the event of a MS terminating call set-up.
- **Equipment identity register (EIR)—**database that contains information on the MS and its capabilities. The IMEI (International Mobile Subscriber Identity) is used to interrogate the EIR.
- **Gateway mobile switching center (GMSC)—**the point to which a MS terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the mobile station roaming number (MSRN) from the HLR based on the mobile station ISDN number (MSISDN), the "directory number" of a MS, and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to a MSC.
- **Short message services gateways (SMS-G)—**term used to collectively describe the two SMS-G described in the GSM recommendations. The Short Message Service Gateway Mobile Switching Center (SMS-GMSC) is for mobile terminating short messages, and short message service inter-working mobile switching center (SMS-IWMSC) for mobile originating short messages. The SMS-GMSC role is similar to that of the GMSC, whereas the SMS-IWMSC provides a fixed access point to the short message service center.

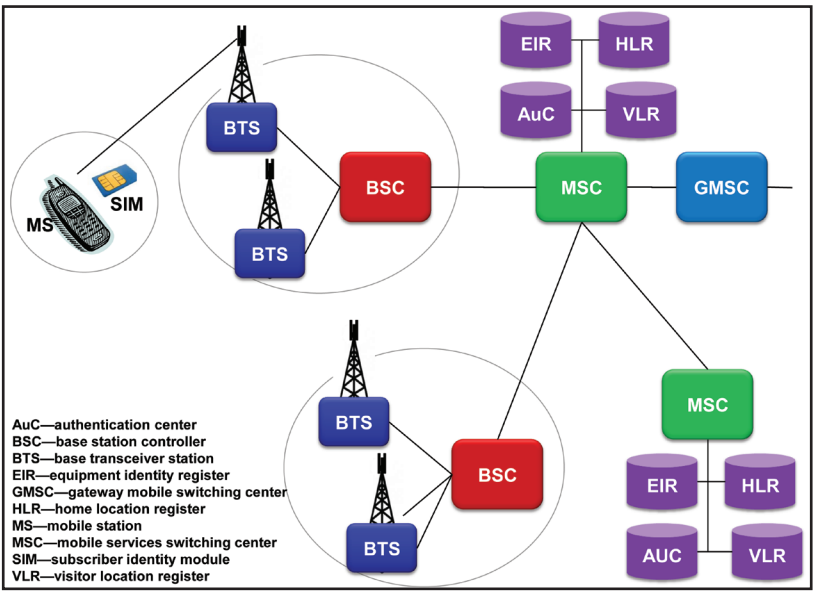



Figure M-32. GSM network


FOR OFFICIAL USE ONLY

### Global System for Mobile Communications Frequency Allocation and Use

**M-81.** GSM can use slow frequency hopping where the mobile station and the base station transmit each TDMA frame on a different carrier frequency. (See table M-2.) The frequency-hopping algorithm is broadcast on the broadcast control channel. Since multipath fading is dependent on carrier frequency, slow frequency hopping helps to alleviate the problem. Frequency hopping is an option for each individual cell and a base station is not required to support this feature. The structure of the most common timeslot burst. A total of 156.25 bits is transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps. There are three other types of burst structure for frame and carrier synchronization and frequency correction. The 26bit training sequence is used for equalization, as described below. The 8.25-bit guard time allows for some propagation time delay in the arrival of bursts. Each group of eight time slots is called a TDMA frame, which is transmitted every 4.615 ms.

**Table M-2. GSM comparison**

| GSM-900 | GSM-1800 |
|---|---|
| • Uplink: 890,2 MHz – 915 MHz (25 MHz). | • Uplink: 1725,2 - 1780,4 MHz. |
| • Downlink: 935,2 MHz – 960 MHz (25 MHz). | • Downlink: 1820,2 - 1875,4 MHz. |
| • Uplink-Downlink distance: 45 MHz. | • Uplink-downlink distance: 95 MHz. |
| ***Frequency division multiple access*** | • 384 pairs of channels. |
| • Channels are 200 kHz wide. | • **Full rate-channel (speech)** 13 kbps. |
| • 124 pairs of channels. | • **Half rate-channel (speech)** 6,5 kbps. |
| ***Time division multiple access*** | • **GSM-data-channel** 9,6 kbps. |
| • 8 connections each channel. | |
| • Theoretical 124*8 = 992 channels to use. | |

**M-82.** TDMA frames are further grouped into multiframes to carry control signals. There are two types of multiframe, containing 26 or 51 TDMA frames. The 26frame multiframe contains 24 traffic channels (TCH) and two slow associated control channels (SACCH) that supervise each call in progress. The SACCH in frame 12 contains eight channels, one for each of the eight connections carried by the TCHs. The SACCH in frame 25 is not currently used, but will carry eight additional SACCH channels when halfrate traffic is implemented. A fast associated control channel (FACCH) works by stealing slots from a traffic channel to transmit power control and handover signaling messages. The channel stealing is done by setting one of the control bits in the time slot burst.

### Global System for Mobile Communications Control Channels

**M-83.** In addition to the associated control channels, there are several other control channels which (except for the standalone dedicated control channel) are implemented in time slot zero of specified TDMA frames in a 51frame multiframe, implemented on a nonhopping carrier frequency in each cell.

**M-84.** The control channels include—

- **Broadcast control channel (BCCH)—**continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency hopping sequences.
- **Standalone dedicated control channel (SDCCH)—**used for registration, authentication, call setup, and location updating. Implemented on a time slot, together with its SACCH, selected by the system operator.
- **Common control channel (CCCH)—**comprises three control channels used during call origination and call paging.

- **Random access channel (RACH)—**A slotted Aloha channel to request access to the network.
- **Paging channel (PCH)—**used to alert the mobile station of incoming call.
- **Access grant channel (AGCH)—**used to allocate an SDCCH to a mobile for signaling, following a request on the RACH.
- **Speech coding—**since GSM is a digital system, speech signals, inherently analog, have to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high-speed trunks and optical fiber lines, is pulse-coded modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal contains much redundancy, although it is simple to implement. The GSM group studied several voice-coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a regular pulse excited-linear predictive coder (RPELPC) with a long term predictor loop. Basically, information from previous samples, which does not change very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 ms samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps.
- **Multipath equalization—**at the 900 MHz range, radio waves bounce off everything—buildings, hills, cars, airplanes and the like, thus many reflected signals, each with a different phase, can reach an antenna. Equalization is used to extract the desired signal from the unwanted reflections. Equalization works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal.
- **Power control—**There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize cochannel interference and to conserve power, both the mobiles and the BTSs operate at the lowest power level that will maintain an acceptable signal quality.
- **Handover or hand-off—**there are four different types of handovers in the GSM system that involve transferring a call between—
  - Channels (time slots) in the same cell.
  - Cells (base-transceiver stations) under the control of the same BSC.
  - Cells under the control of different BSCs, but belonging to the same MSC.
  - Cells under the control of different MSCs.
  - The first two types of handover, called internal handovers, involve only one BSC. To save signaling bandwidth, they are managed by the BSC without involving the MSC, except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved.
- Location updating and call routing—the MSC provides the interface between the GSM mobile network and the public fixed network. From the fixed network's point of view, the MSC is just another switching node. However, switching is a little more complicated in a mobile network since the MSC has to know where the mobile is currently roaming—in GSM it could even be roaming in another country. The way GSM accomplishes location updating and call routing to the mobile is by using two location registers: the HLR and the VLR. Location updating is initiated by the mobile when, by monitoring the Broadcast Control Channel, it notices that the location-area broadcast is not the same as the one previously stored in the mobile's memory. An update request and the IMSI or previous TMSI is sent to the new VLR via the new MSC. An MSRN is allocated and sent to the mobile's HLR (which always keeps the most current location) by the new VLR. The MSRN is a regular telephone number that routes the call to the new VLR and is subsequently translated to the TMSI of the mobile. The HLR sends back the necessary callcontrol parameters, and sends a cancel message to the old VLR, so that the previous MSRN can be reallocated. Finally, a new TMSI is allocated and sent to the mobile to identify it in future paging or call-initiation requests.

## Global System for Mobile Communications Authentication

**M-85.** Key terms for GSM authentication include—

- **A3**—the authentication algorithm used in the GSM system. Currently the COMP128 algorithm is used as the A3/A8 implementation in most GSM networks.
- **A5**—the encryption algorithm used in the GSM system. There are various implementations named A5/1, A5/2. The A5/1 is known as the strong over-the-air voice-privacy algorithm. A5/x (A5/2 ...) are weaker implementations targeted at foreign markets outside of Europe. There is also an A5/0 algorithm, which encloses no encryption at all.
- **A8**—the key generation algorithm used in the GSM system. Currently COMP128 algorithm is used as the A3/A8 implementation in most GSM networks.

**M-86.** Authentication involves two functional entities, the SIM card in the mobile system and the authentication center. Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the authentication center (AC).

**M-87.** During authentication, the AC generates a random number that it sends to the mobile. Both the mobile and the AC then use the random number, in conjunction with the subscriber's secret key and a ciphering algorithm, called A3, to generate a number that is sent back to the AC. If the number sent by the mobile is the same as the one calculated by the AC, the subscriber is authenticated.

**M-88.** The above-calculated number is also used, together with a TDMA frame number and another ciphering algorithm, called A5, to encipher the data sent over the radio link, preventing others from listening in. Enciphering is possible but not needed since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.

**M-89.** Another level of security is performed on the mobile equipment, as opposed to the mobile subscriber. As mentioned earlier, each GSM terminal is identified by a unique international mobile equipment identity (IMEI) number. A list of IMEIs in the network is stored in the equipment identity register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

- **Whitelisted**—the terminal is allowed to connect to the network.
- **Graylisted**—under observation from the network, possible problems.
- **Blacklisted**—the terminal has either been reported as stolen, or it is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

**M-90.** In a typical phone call using a GSM cell phone—

- The mobile station (MS) signs into the network.
- The MSC requests five triplets from the HLR.
- The HLR creates five triples utilizing the A8 algorithm.
- These five triples each contain—
  - A 128-bit random challenge (RAND).
  - A 32-bit matching signed response (SRES).
  - A 64-bit ciphering key used as a session key (Kc).
- The HLR sends the MSC the five triplets.
- The MSC sends the random challenge from the first triplet to the BTS.
- The BTS sends the random challenge from the first triplet to the MS.
- The MS receives the random challenge from the BTS and encrypts it with the individual subscriber authentication key (Ki) assigned to the MS utilizing the A3 algorithm.
- The MS sends the SRES to the BTS.
- The BTS sends the SRES to the MSC.
- The MSC verifies the SRES.
- The MS generates a Kc using the A8 algorithm, the (Ki) assigned to the MS, and the RAND

received from the BTS.

- The MS sends the Kc to the BTS.
- The MSC sends the (Kc) to the BTS.
- The BTS receives the Kc from the MSC.
- The BTS receives the Kc from the MS.
- The BTS verifies the session keys from the MS and the MSC.
- The A5 algorithm is initialized with the Kc and the number of the frame to be encrypted.
- Over-the-air communication channel between the MS and BTS can now be encrypted using the A5 algorithm.

### Short Message Service

**M-91.** Messages are sent via a store-and-forward mechanism to a short message service center (SMSC) that attempts to send the message to the recipient and possibly retry if the user is not currently reachable. Both mobile terminated (MT), for messages sent to a mobile handset, and mobile originating (MO), for those that are sent from the mobile handset, operations are supported. Message delivery is best effort, so there is no guarantee that a message will actually be delivered to its recipient. Delay or the complete loss of a message is not uncommon, particularly when sending between networks. Users may choose to request delivery reports, which can provide positive confirmation that the message has reached the intended recipient. Notifications for failed deliveries are unreliable at best.

**M-92.** Transmission of the short messages between SMSC and phone is via SS7 within the standard GSM framework. Messages are sent with the additional operation forward short message, whose payload length is limited by the constraints of the signaling protocol to precisely 140 bytes. In practice, this translates to either 160 7-bit characters, 140 8-bit characters, or 70 2-byte characters in languages such as Arabic, Chinese, Korean, Japanese, or Slavonic languages (such as Russian) when encoded using 2-byte UTF-16 character encoding. This does not include routing data and other metadata, which is additional to the payload size.

**M-93.** Larger content (known as long SMS or concatenated SMS) can be sent segmented over multiple messages, in which case each message will start with a user data header (UDH) containing segmentation information. Since UDH is inside the payload, the number of characters per segment is lower: 153 for 7-bit encoding, 134 for 8-bit encoding, and 67 for 16-bit encoding. The receiving phone is then responsible for reassembling the message and presenting it to the user as one long message. While the standard theoretically permits up to 255 segments, three to four segment messages are the practical maximum, and long messages are billed as equivalent to multiple SMS messages.

**M-94.** Short messages can also be used to send binary content, such as ringtones or logos as well as over the air (OTA) programming or configuration data. Such uses are a vendor-specific extension of the GSM specification and there are multiple competing standards, although Nokia's smart messaging is by far the most common.

**M-95.** Some service providers offer the ability to send messages to land line telephones, regardless of their capability of receiving text messages, by automatically phoning the recipient and reading the message aloud using a speech synthesizer along with the number of the sender.

## Wireless Computer Protocols, Terms and Overview

**M-96.** A wireless LAN (WLAN) is the linking of two or more computers without using wires. It is the same as LAN, but has a wireless interface. WLAN uses spread-spectrum technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and remain connected to the network.

**M-97.** All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface cards (NICs). Stations fall into one of two categories—wireless clients and access points:

- **Wireless clients—**can be mobile devices (such as laptops, personal digital assistants, and IP phones) or fixed devices (such as desktops and workstations equipped with a wireless NIC).
- **Access points—**are base stations for the wireless network. They transmit and receive radio frequencies wireless-enabled devices to communicate.

**M-98.** The basic service set (BSS) is a set of all stations that can communicate with each other. There are two types of BSSs—independent BSS and infrastructure BSS. Every BSS has an identity called the BSSID. The BSSID is the media access control (MAC) address of the access point servicing the BSS:

- **Independent BSSs—**are an ad-hoc network that contains no access points. Since they do not use access points, they cannot connect to any other basic service set.
- **Infrastructure BSSs—**can communicate with other stations that are not in the same basic service set through access points servicing the other stations.

**M-99.** An extended service set (ESS) is a set of connected BSSs. Access points in an extended service set are connected by a distribution system. Each ESS has an identification called the SSID, which is a 32-byte (maximum) character string. An example is linksys (the default SSID for Linksys routers).

**M-100.** A distribution system connects access points in an extended service set. A distribution system is usually a wired LAN but can be a wireless LAN.

### Types of Wireless Local Area Networks

**M-101.** There are a variety of wireless LANs.

#### *Peer-to-Peer or Ad-Hoc*

**M-102.** Peer-to-peer or ad-hoc wireless LANs allow wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. Two computers typically use this to connect to each other to form a network.

**M-103.** A strength meter for the signal coming from all the other ad-hoc devices will not read the strength accurately, and can be misleading because it is registering the strength of the strongest signal, such as the closest computer.

#### *Access Point or Infrastructure Wireless Local Area Networks*

**M-104.** Infrastructure WLAN is the most common type of WLAN. To connect to the network a wireless-enabled client connects to an access point. An access point is often a hub or router that has an antenna built in to transmit and receive the RF and bridges a wireless network to a wired Ethernet network. The network administer can configure the access point through a Web interface or telnet. When it is difficult to get all the access points wired up, it is also possible to put up access points as repeaters.

Home networks typically have one access point that is directly connected to the Internet to provide the network with Internet access. Larger networks that provide wireless access to entire buildings usually have multiple access points placed at strategic locations.

#### *Wireless Protocol IEEE 802.11 (Wi-Fi)*

**M-105.** In 1990, the Institute of Electrical and Electronic Engineers (IEEE) formed a group to develop a standard for wireless equipment. On 26 June 1997, a standard was developed called 802.11. The standard specified that the upper layers of the open system interconnection (OSI) model cannot be modified, and WLANs must be implemented on the physical and data link layers. This provided the ability to run any operating system or LAN application on a WLAN without any modification. They

accomplished this by doing upper layer features on the data link layer.

# COMPUTER NETWORKING

**M-106.** Networks may be characterized as LAN, metropolitan area network (MAN), or WAN.

**M-107.** A *LAN* is small network, limited to a single collection of machines and one or more cables and other peripheral equipment. A LAN is the basic building block for constructing larger networks.

**M-108.** *MANs* interconnect LAN's within a specific geographic region, such as a city or county. A *WAN* spans distances between cities and links two or more separate locations. It is not uncommon to find networks involving all three of these network types: LANs for local access, MANs for regional or citywide access, and WANs for access to remote sites elsewhere in the country.



## Network Types

**M-109.** Networks also fall into two major types: peer-to-peer and client/server (sometimes called server based). Client/server networks are the most typical in most organizations.

### Peer-To-Peer Network

**M-110.** In a peer-to-peer network—

- Computers take both client and server roles.
- There is no centralized control over shared resources, such as files and printers.
- Users control access to the resources on their own computers.
- There is no centralized control, meaning there is no network-wide security.
- This is only used for small networks. There should not be more than 10 computers on the network.

### Client/Server Network

**M-111.** A client/server network—

- Provides centralized verification of user accounts and passwords.
- Provides centralized control over network resources, such as files and printers.
- Uses servers to provide access to resources.
- Has better security compared to peer-to-peer networks.
- Allows a single password for network login to be used to deliver access to all resources.

## Server Types

**M-112.** There are four types of servers:

- **Dedicated server—**acts only as a server and is not intended for regular use as a client machine.
- **Application server—**provides access to applications on the network.
- **File server—**provides access to files across the network and is one of the most common types of servers.
- **Print server—**provides selected clients access to printers via the network.

## Network Topologies

**M-113.** A network's topology refers to the physical layout of its computers, cables, and other resources. It also refers to how those components communicate with each other. A network's topology has a significant effect on its performance as well as its growth potential. All network design is based on three basic topologies—bus, star, and ring:

- **Bus:**
  - The simplest and most common method of connecting computers.
  - The entire network can be halted by a single cable break.
  - All components are connected via a backbone or single cable segment.
  - 10Base2 Ethernet is the most common cable type used in a bus topology.
- **Star:**
  - Computers are connected by cable segments to a central hub.
  - A signal is transmitted to the hub and then to all other computers connected to the hub.
  - The hub is a single point of failure. 10BaseT Ethernet is the most common cable type used in a star topology.
- **Ring:**
  - Created when a computer is connected directly to the next computer in line, forming a circle.
  - A computer receives a signal and either acts on it or regenerates it and passes it along.
  - Signals travel in only one direction.
  - Token ring or token passing is the most common type.



**M-114.** There are variations to the three basic topologies. Two basic hybrid types are mesh and star bus:

- **Mesh:**
  - The most fault-tolerant topology.
  - Each device in the network is connected to every other device.
  - The most expensive due to all the connections.
  - A cable or device failure has no effect on the network.
- **Star bus:**
  - This is a combination of the star and bus topologies.
  - Hubs are connected in a bus backbone with computers connected to the hubs in a star.
  - If a hub fails, the computers attached will not talk, but other hub-computer connections will remain intact.

## Network Protocols

**M-115.** Protocols are the rules, conventions, and procedures that networks use for communicating from one computer to another. Protocols serve their function based on the OSI model. When a set of protocols work together cooperatively, it is called a protocol suite:

- **NetBios Enhanced User Interface (NetBEUI).** A small nonroutable protocol developed by IBM and Microsoft that is installed on all Microsoft Operating Systems.
- **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).** A Novell protocol used for packet routing and forwarding.
- **Transmission Control Protocol/Internet Protocol (TCP/IP).** The Internet protocol, TCP/IP is a suite of protocols. TCP/IP uses small, very specialized protocols (examples include file transfer protocol [FTP], simple mail transfer protocol [SMTP], and Telnet). The Internet would not exist without TCP/IP.

**M-116.** There are two forms of data delivery over a network:

- **Connectionless.** A computer places data on the network and assumes it will get through. This can be very fast because it requires little overhead and does not waste time establishing connections. Error checking is done at the receive end. Packets in connectionless environments are often referred to as datagrams.
- **Connection-oriented.** A connection is established between the two computers before any packets are transmitted. It is more reliable than connectionless, but slower. As each packet reaches the destination, its receipt is acknowledged. If errors occur during transmission, the packet is re-sent.

## Access Methods

**M-117.** When multiple computers are attached to a network, the way they share the cable must be defined. When computers have data to send, they transmit data across the network. If two computers send data at the same time, there is a data collision, destroying both messages. A number of rules have been defined to prevent collisions.

**M-118.** Channel access is handled at the data link layer of the OSI model. There are five major types of channel access:

- **Deterministic:**
  - Also referred to as "round-robin" scheduling.
  - Assumes multiple nodes in a TDMA environment.
  - Prevents collision by assigning each node a specified time slot to broadcast node state information over a shared channel. This precludes nodes "stepping" on each other.
  - Allows for asynchronous data transmission.
- **Contention (CSMA/CD):**
  - Used by Ethernet networks (the most popular).
  - Prevents collisions by listening to the channel to see if another computer is sending data.
  - Gives all computers on the network an equal chance at controlling the channel.
  - Increases the chances of collisions when more computers are on the network. This can dramatically slow network transmissions.
- **Contention (CMSA/CA):**
  - Computer sends an intent-to-transmit data. All other computers receive this signal and wait until data has been sent before they send data.
  - The system is more reliable than CSMA/CD but slower.
  - The system is not used as much as CSMA/CD. Apple's Local Talk is the only major network to use it.
- **Token-passing.** A token packet is passed from one computer to the next. Only the computer with the token can send data. A computer can keep the token only a specific amount of time (token-hold time). If a computer on the network has data to send, it must wait until it gets the token. This complicated process requires more expensive equipment than contention-based systems.
- **Demand priority:**
  - Used solely by 100 Mbps Ethernet systems. Uses star-bus topology.
  - Uses intelligent hubs to control access to the network.
  - Transmits a demand signal from the computer to the hub if a computer has data to send. The hub then allows that computer to send data.
  - Sends data from computer to hub and from hub directly to receiving computer.
- **Polling.** A central controller (primary device) asks each computer (secondary device) on the network if it has data to send. Computers with data are allowed to send its data up to a certain point and then another computer is allowed to send data. This allows each computer equal access, but if the primary device fails, the network fails.

## Network Architectures

**M-119.** A network's architecture generally refers to its overall structure, including topology, physical media, and channel access method. The most common network architecture is Ethernet, but there are others, such as fiber distributed data interface (FDDI) and Apple Talk. Ethernet transmits at either 10 Mbps or 100 Mbps. Five common architectures are listed below:

- **10base5 Ethernet:**
  - Also called Thicket due to the size of the cable (RG8—Yellow).
  - Was the original Ethernet but is being replaced by 10Base2 ThinNet.
  - Generally used as a backbone for networks today.

- Uses a maximum cable length segment of 500 meters, hence the name.
- Uses coaxial cable.

- **10base2 Ethernet:**
  - Called ThinNet (RG58—Gray).
  - Uses a thinner cable, which is easier to work with than 10base5.
  - Is replacing 10base5 because it is easier to install and cheaper. Maximum cable length per segment is 185 meters. Uses coaxial cable.
- **10base T Ethernet:**
  - Is the most popular Ethernet architecture due to its low cost.
  - Is normally wired in a star topology.
  - Eases troubleshooting because each computer is an end node on a cable segment.
  - Uses UTP cable.
  - Can run on category 3, 4, or 5 cable with maximum length of 100 meters.
- **10base F Ethernet:**
  - Has the fastest transmission speed of any Ethernet.
  - Is normally wired in a star or star-bus configuration.
  - Uses fiber-optic cable.
  - Has high cost and installation is difficult.
  - Uses a maximum cable length segment of 2000 meters.
  - Runs at 100 Mbps Ethernet.
  - Includes 100VG-AnyLAN and 100BaseT.
  - Is well suited for applications such as video and computer aided design (CAD).
  - Is called fast Ethernet.
  - Will normally use either category 5 UTP or fiber-optic cable.
- **Token ring:**
  - Developed by IBM in the mid-1980s.
  - Passes a token along the ring until it is needed by a computer to pass data.
  - Prevents collisions, unlike Ethernet.
  - Provides all computers on the network equal access to the token.
  - Uses FDDI.
  - Used primarily as a backbone for larger networks.
  - Transmits at 100 Mbps.
  - Uses two counterrotating rings instead of one ring.
  - Uses token passing.

## Network Connectivity

**M-120.** Certain devices are used to connect networks or give networks connectivity to the outside world—the Internet. There are several ways to stretch or expand network capabilities:
- Physically expanding to support additional computers.
- Segmenting to filter network traffic.
- Extending to connect separate LANs.
- Connecting two separate computing environments.

**M-121.** Other means of increasing network connectivity include the following:
- **Repeaters:**
  - A signal degenerates as it travels down a cable.
  - A repeater regenerates the signal and extends the length of the network.
  - Repeaters retransmit the data at the same speed as the network, although there is a slight delay as the repeater regenerates the signal.
- **Bridges:**
  - The primary function is to filter traffic between network segments.

- The bridge looks at the address of a packet. If the packet's destination is another network, the bridge retransmits the packet to that network. If the destination is on the same network segment, the packet is discarded. A bridge greatly reduces network traffic.

- **Routers:**
  - Routers can connect networks of different physical media and network architectures.
  - Routers can choose the best path for a packet through an internet work.
  - Routers reduce network traffic by not forwarding broadcasts or corrupt packets.
- **Gateways:**
  - Gateways can connect completely different systems.
  - Gateways translate data between different protocols.
  - Gateways are dedicated to one task.
  - Gateways are the most expensive of the devices discussed.
  - Gateways are used to distribute data from one input to several outputs.
  - Gateways only see "1 and 0" instead of intelligible traffic.
  - Gateways often connect uplink with several outputs.
  - Gateways often cause increased net congestion.

## Open System Interconnection Reference Model

**M-122.** The OSI reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. (See figure M-33.) The International Organization for Standardization (ISO) developed the model in 1984. It is now considered the primary architectural model for intercomputer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers.

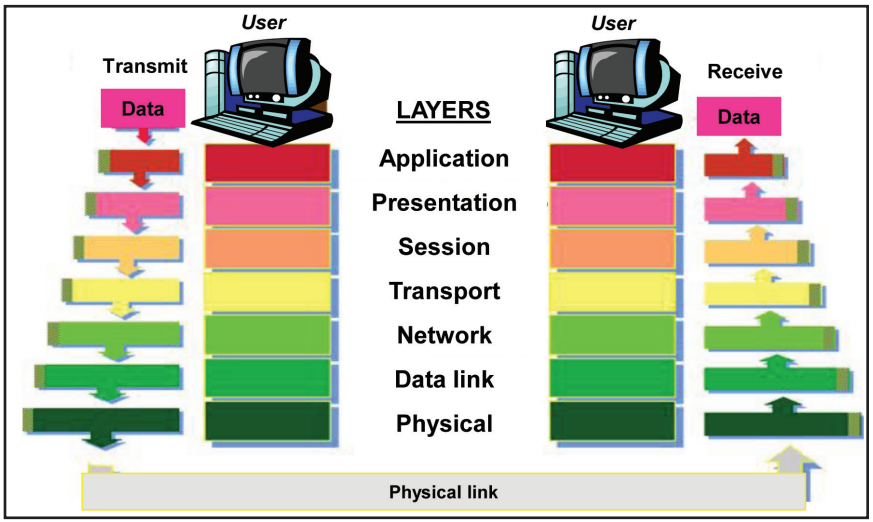



Figure M-33. The open system interconnection


FOR OFFICIAL USE ONLY

**M-123.** A handy way to remember the seven layers is the sentence "All people seem to need data processing." The beginning letter of each word corresponds to a layer:

- **All.** Application layer.
- **People.** Presentation layer.
- **Seem.** Session layer.
- **To.** Transport layer.
- **Need.** Network layer.
- **Data.** Data link layer.
- **Processing.** Physical layer.



## Characteristics of the Open System Interconnection Layers

**M-124.** The seven layers of the OSI reference model can be divided into two categories—upper layers and lower layers.

- **Upper layers—**deal with application issues and are generally implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term "upper layer" is sometimes used to refer to any layer above another layer in the OSI model.
- **Lower layers—**handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (for example, network cabling) and is responsible for actually placing information on the medium.

### Layer Seven—Application

**M-125.** The application layer is closest to the end user. Users can access information on the network through an application. This layer is the main interface for users to interact with the application and therefore the network. Examples of application layer protocols include Telnet, FTP, SMTP, and hypertext transfer protocol (HTTP).

### Layer Six—Presentation

**M-126.** The presentation layer transforms data to provide a standard interface for the application layer. MIME encoding, data compression, data encryption, and similar manipulation of the presentation occur at this layer to present the data as a service or protocol developer sees fit. Examples include converting an EBCDIC-coded text file to an ASCII-coded file or serializing objects and other data structures into and out of XML.

### Layer Five—Session

**M-127.** The session layer controls the dialogues (sessions) between computers. It establishes, manages, and terminates the connections between the local and remote application. It provides for either duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for "graceful close" of sessions, which is a property of TCP, and for session checkpointing and recovery, which is not usually used in the Internet protocol suite.

### Layer Four—Transport

**M-128.** The transport layer provides transparent transfer of data between end users, thus relieving the upper layers from any concern while providing reliable and cost-effective data transfer. The transport layer controls the reliability of a given link through flow control, segmentation or desegmentation, and error control. Some protocols are state and connection oriented. This means that the transport layer can keep track of the packets and retransmit those that fail. The best-known example of a layer four protocol is the TCP. It is the layer that converts messages into TCP, user datagram protocol (UDP),

stream control transmission protocol (SCTP), and similar packets.

**Layer Three—Network**

**M-129.** The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the transport layer. The network layer performs network routing functions, might perform segmentation or desegmentation, and reports delivery errors. Routers operate at this layer—sending data throughout the extended network and making the Internet possible (there also exists layer three or IP switches). This is a logical addressing scheme—values are chosen by the network engineer. The addressing scheme is hierarchical. The best-known example of a layer three protocol is the IP.

**Layer Two—Data Link**

**M-130.** The data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. The addressing scheme is physical, which means that the addresses (MAC address) are hard-coded into the network cards at the time of manufacture. The addressing scheme is flat. The best-known example of this is Ethernet. Other examples of data link protocols are HDLC and ADCCP (for point-to-point or packet-switched networks) and Aloha (for LANs).

**M-131.** On IEEE 802 LANs and some non-IEEE 802 networks, such as FDDI, this layer may be split into a MAC layer and the IEEE 802.2 logical link control (LLC) layer. This is the layer where the bridges and switches operate. Connectivity is provided only among locally attached network nodes. However, there is a reasonable argument to be made that these really belong at "layer two and one half" rather than strictly at layer two.

**Layer One—Physical**

**M-132.** The physical layer defines all the electrical and physical specifications for devices. This includes the layout of pins, voltages, and cable specifications. Hubs, repeaters, network adapters, and host bus adapters (HBAs) used in storage area networks are physical-layer devices. The major functions and services performed by the physical layer are—

- Establishing and terminating a connection to a communications medium.
- Participating in the process whereby the communication resources are effectively shared among multiple users, for example, contention resolution and flow control.
- Modulating or performing the conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling—copper and fiber optic—or over a radio link.

**M-133.** Parallel SCSI buses operate in this layer. Various physical-layer Ethernet standards are also in this layer. Ethernet incorporates both this layer and the data-link layer. The same applies to other LANs, such as token ring, FDDI, and IEEE 802.11.

## Protocols

**M-134.** The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. A protocol implements the functions of one or more of the OSI layers.
A wide variety of communication protocols exist. Some of these protocols include—

- **LAN protocols—**operate at the physical and data link layers of the OSI model and define communications over the various LAN media.
- **WAN protocols—**operate at the lowest three layers of the OSI model and define communications over the various wide-area media.

- **Network protocols**—various upper-layer protocols that exist in a given protocol suite.
- **Routing protocols**—network-layer protocols that are responsible for exchanging information between routers so that the routers can select the proper path for network traffic.

**M-135.** Many protocols rely on others for operation. For example, many routing protocols use network protocols to exchange information between routers. This concept of building upon the layers already in existence is the foundation of the OSI model.



## International Organization for Standardization Hierarchy of Networks

**M-136.** Large networks are typically organized as hierarchies. A hierarchical organization provides such advantages as ease of management, flexibility, and a reduction in unnecessary traffic. Thus, ISO has adopted a number of terminology conventions for addressing network entities. Key terms and their definitions include—

- **End system (ES).** A network device that does not perform routing or other traffic forwarding functions. Typical ESs include devices such as terminals, personal computers, and printers.
- **Intermediate system (IS).** A network device that performs routing or other traffic-forwarding functions. Typical ISs include devices such as routers, switches, and bridges. Two types of IS networks exist:
  - ***Intradomain IS***—communicates within a single autonomous system.
  - ***Interdomain IS***—communicates within and between autonomous systems.
- **Area.** A logical group of network segments and their attached devices. Areas are subdivisions of ASs.
- **Autonomous system (AS).** A collection of networks under a common administration that share a common-routing strategy. ASs are subdivided into areas and an AS is sometimes called a domain.

## Connection-Oriented and Connectionless Network Services

**M-137.** In general, transport protocols can be characterized as being either connection-oriented or connectionless.

### Connection-Oriented Network Services

**M-138.** Connection-oriented network services must first establish a connection with the desired service before passing any data. In general, connection-oriented network services provide some level of delivery guarantee. Connection-oriented network services involve three phases:

- **Connection establishment.** End nodes may reserve resources for the connection. They may negotiate and establish certain criteria for the transfer, such as a window size used in TCP connections. This resource reservation is exploited in some denial of service attacks. An attacking system will send many requests for establishing a connection but will not complete the connection. The attacked computer is left with resources allocated for many never-completed connections. When an end node tries to complete an actual connection, there are not enough resources for the valid connection.
- **Data transfer.** Actual data is transmitted over the connection. During data transfer, most connection-oriented network services monitor for lost packets and handle resending them. The protocol is generally responsible for putting the packets in the right sequence before passing the data up the protocol stack.
- **Connection termination.** Upon completion of data transfer, the end nodes terminate the connection and release resources reserved for the connection.

### Connectionless Network Services

**M-139.** Connectionless network services can send data without any need to establish a connection

first. Connectionless network services do not provide some level of delivery guarantee.

## Data Link Layer Addresses

**M-140.** A data link layer address uniquely identifies each physical network connection of a network device. Data link addresses are sometimes referred to as physical or hardware addresses. Data link addresses usually exist within a flat address space and have a preestablished and typically fixed relationship to a specific device.



**M-141.** End systems generally have only one physical network connection and thus have only one data link address. Routers and other Internetworking devices typically have multiple physical network connections and therefore have multiple data link addresses.

### Media Access Control Addresses

**M-142.** MAC addresses consist of a subset of data link layer addresses. MAC addresses identify network entities in LANs that implement the IEEE MAC addresses of the data link layer. As with most data link addresses, MAC addresses are unique for each LAN interface.

**M-143.** MAC addresses are 48 bits in length and expressed as 12 hexadecimal digits. The first six hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and thus comprise the organizationally unique identifier (OUI). The last six hexadecimal digits comprise the interface serial number, or another value administered by the specific vendor. MAC addresses sometimes are called burned-in addresses (BIAs) because they are burned into read-only memory (ROM) and are copied into random access memory (RAM) when the interface card initializes.

### Mapping Addresses

**M-144.** Because a network uses network addresses to route traffic around the network, there is a need to map network addresses to MAC addresses. When the network layer has determined the destination station's network address, it must forward the information over a physical network using a MAC address. Different protocol suites use different methods to perform this mapping, but the most popular is address resolution protocol (ARP). Different protocol suites use different methods for determining the MAC address of a device. The following three methods are used most often. ARP maps network addresses to MAC addresses. The hello protocol enables network devices to learn the MAC addresses of other network devices. MAC addresses either are embedded in the network layer address or are generated by an algorithm.

#### *Address Resolution Protocol*

**M-145.** ARP is the method used in the TCP/IP suite. When a network device needs to send data to another device on the same network, it knows the source and destination network addresses for the data transfer. It must somehow map the destination address to a MAC address before forwarding the data. First, the sending station will check its ARP table to see if it has already discovered this destination station's MAC address. If it has not, it will send a broadcast on the network with the destination station's IP address contained in the broadcast. Every station on the network receives the broadcast and compares the embedded IP address to its own. Only the station with the matching IP address replies to the sending station with a packet containing the MAC address for the station. The first station then adds this information to its ARP table for future reference and proceeds to transfer the data.

**M-146.** When the destination device lies on a remote network, one beyond a router, the process is the same except that the sending station sends the ARP request for the MAC address of its default gateway. It then forwards the information to that device. The default gateway then forwards the information over necessary networks to deliver the packet to the network on which the destination device resides. The

router on the destination device's network then uses ARP to obtain the MAC of the actual destination device and delivers the packet.

### *Hello Protocol*

**M-147.** The hello protocol is a network layer protocol that enables network devices to identify one another and indicate that they are still functional. For example, when a new end system powers up, it broadcasts hello messages onto the network. Devices on the network return hello replies, and hello messages are also sent at specific intervals to indicate that they are still functional. Network devices can learn the MAC addresses of other devices by examining hello protocol packets.



### *Predictable Media Access Control Addresses*

**M-148.** Three protocols use predictable MAC addresses. In these protocol suites, MAC addresses are predictable because the network layer either embeds the MAC address in the network layer address or uses an algorithm to determine the MAC address. The three protocols are Xerox network systems (XNS), Novell internetwork packet exchange (IPX), and DECNet.

## Network Layer Addresses

**M-149.** A network layer address identifies an entity at the network layer of the OSI layers. Network addresses usually exist within a hierarchical address space and are sometimes called virtual or logical addresses.

**M-150.** The relationship between a network address and a device is logical and unfixed. It typically is based either on physical network characteristics (the device is on a particular network segment) or on groupings that have no physical basis (the device is part of an AppleTalk zone). End systems require one network layer address for each network layer protocol that they support. (This assumes that the device has only one physical network connection.) Routers and other internetworking devices require one network layer address per physical network connection for each network layer protocol supported.

**M-151.** For example, a router with three interfaces each running AppleTalk, TCP/IP, and OSI must have three network layer addresses for each interface. The router therefore has nine network layer addresses.

## Hierarchical Versus Flat Address Space

**M-152.** Internetwork address space typically takes one of two forms:

- **Hierarchical address space—**organized into numerous subgroups, each successively narrowing an address until it points to a single device (in a manner similar to street addresses).
- **Flat address space—**organized into a single group (in a manner similar to U.S. social security numbers).

**M-153.** Hierarchical addressing offers certain advantages over flat-addressing schemes. Address sorting and recall is simplified using comparison operations. For example, "Ireland" in a street address eliminates any other country as a possible location.

## Address Assignments

**M-154.** Addresses are assigned to devices as one of two types:

- **Static addresses—**assigned by a network administrator according to a preconceived network addressing plan. A static address does not change until the network administrator manually changes it.
- **Dynamic addresses—**obtained by devices when they attach to a network by means of some protocol-specific process. A device using a dynamic address often has a different address each time that it connects to the network.

**M-155.** Some networks use a server to assign addresses. Server-assigned addresses are recycled for

reuse as devices disconnect. A device is therefore likely to have a different address each time that it connects to the network.

### Addresses Versus Names

**M-156.** Internetwork devices usually have both a name and an address associated with them. Internetwork names typically are location-independent and remain associated with a device wherever that device moves (for example, from one building to another). In contrast, Internetwork addresses usually are location-dependent and change when a device is moved (although MAC addresses are an exception to this rule). As with network addresses being mapped to MAC addresses, names are usually mapped to network addresses through some protocol. The Internet uses Domain Name System (DNS) to map the name of a device to its IP address.



## Flow control Basics

**M-157.** Flow control is a function that prevents network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. For example, a high-speed computer may generate traffic faster than the network can transfer it, or faster than the destination device can receive and process it. The three commonly used methods for handling network congestion are buffering, transmitting source-quench messages, and windowing.

### Buffering

**M-158.** Buffering is used by network devices to temporarily store bursts of excess data in memory until they can be processed. Occasional data bursts are easily handled by buffering. Excess data bursts can exhaust memory, however, forcing the device to discard any additional data grams that arrive.

### Source-Quench Messages

**M-159.** Source-quench messages are used by receiving devices to help prevent their buffers from overflowing. The receiving device sends source-quench messages to request that the source reduce its current rate of data transmission, as follows:

- The receiving device begins discarding received data due to overflowing buffers.
- The receiving device begins sending source-quench messages to the transmitting device at the rate of one message for each packet dropped.
- The source device receives the source-quench messages and lowers the data rate until it stops receiving the messages.
- The source device gradually increases the data rate as long as no further source-quench requests are received.

### Windowing

**M-160.** Windowing is a flow-control scheme in which the source device requires an acknowledgment from the destination after a certain number of packets have been transmitted. With a window size of three, the source requires an acknowledgment after sending three packets, as follows:

- The source device sends three packets to the destination device.
- After receiving the three packets, the destination device sends an acknowledgment to the source.
- The source receives the acknowledgment and sends three more packets. If the destination does not receive one or more of the packets for some reason, such as overflowing buffers, it does not receive enough packets to send an acknowledgment.
- The source then retransmits the packets at a reduced transmission rate.

# SATELLITE COMMUNICATIONS

**M-161.** There is nothing mystical about satellites. Aside from its associated high-tech design, scientific documentation, and costly launch vehicle, a communications satellite is basically a relay

station placed on a very high hill. Satellites provide a tremendous network extension advantage for the Army. Widely separated satellite terminal users within the same very large area of the Earth covered by a single satellite's footprint can communicate directly with each other. A single satellite can link sites that are far beyond the range of a single terrestrial line-of-sight radio link. Satellites allow the global relay of important information in a variety of ways, either to a single user or in a simultaneous broadcast to many users.

**M-162.** Satellite systems often provide the best, most accurate weather data available. Placing a long distance telephone call often involves a satellite transmission. Maps are routinely updated using data acquired by satellites. The Army uses satellite communications (SATCOM) primarily for voice and data, but the use of SATCOM has quickly developed into other application areas to satisfy broadly ranging needs. Imagery, video teleconferencing, and global broadcast are examples of those needs.

**M-163.** Terrestrial communications systems, even those involving fiber-optic cables, cannot duplicate all of the functions of satellites. Mobility and flexibility on the battlefield, and broadcast capability to deployed units throughout a combatant command's area of responsibility are unique satellite capabilities. The integration of satellite and terrestrial networks permits maximum communications flexibility for the Soldier.



## The Environment of Space

**M-164.** Orbital space is a vast area. It ranges from 60 miles above the surface of the Earth to arbitrary points as far out as 60,000 miles, where gravity is reduced to 0.05 percent of what it is experienced on the Earth. It is difficult to envision the totality of this region, encompassing about 900 trillion cubic miles.

### Earth's Atmosphere

**M-165.** The Earth's atmosphere comprises a mixture of gasses held close to the earth by gravity. The atmosphere supports life, protects the planet from damaging radiation, and recycles water. It is made up of nitrogen (78.08 percent), oxygen (20.9 percent), argon (0.93 percent), and trace gases, including carbon dioxide, helium, and hydrogen.

**M-166.** Air density, gravity, and propulsion vehicle capabilities help determine the altitude at which a satellite can be placed into orbit. Although decreasing with altitude, atmospheric friction (directly related to air density) creates drag on any flying object. Significant atmospheric drag can affect objects as far out as 1,200 miles from the Earth's surface. Due to the effects of drag and gravity, objects placed in an orbit at less than 100 miles above the Earth's surface quickly lose speed and fall back to Earth without sufficient propulsion.

**M-167.** The Earth's atmosphere is divided into regions. The lines between these regions are not distinct and they blend into each other. The sizes of these regions fluctuate depending on the time of the day, the season, and the amount of solar activity.

#### *Troposphere*

**M-168.** The troposphere starts at the Earth's surface and extends upward five to nine miles. This is the densest part of the atmosphere. Above two miles, a person requires supplemental oxygen or a pressurized environment. Almost all weather and clouds occur in the troposphere, the lowest region of the atmosphere, rendering this region somewhat unstable. The upper boundary of the troposphere is called the tropopause, which varies in thickness from 9 to 12 miles at the equator to about 4 miles in the polar areas.

*Stratosphere*

**M-169.** The stratosphere extends from the tropopause to the stratopause, with an upper boundary of 30 to 33 miles above sea level. This region is characterized by the near-absence of water vapor and clouds.

**M-170.** The stratosphere provides advantages for long-distance flight because it is above stormy weather, is quite constant in temperature, and has strong, steady horizontal winds known as the jet stream. Unlike the troposphere, which gets colder with altitude, the temperature in the stratosphere increases with altitude due to the absorption of ultraviolet radiation. The ozone layer, which absorbs and scatters the solar ultraviolet radiation, is in the stratosphere. The ozone molecules absorb high-energy ultraviolet rays from the sun, warming the atmosphere at that level.

*Mesosphere*

**M-171.** The mesosphere extends from its lower boundary at the stratopause to its upper boundary at the mesopause, at about 50 miles of altitude. The mesopause is where the atmosphere reaches its minimum temperature, approximately 130 degrees below zero Fahrenheit. The mesosphere has an effect on satellite launch operations. It is a transit area that nonair-breathing rockets must thrust through to reach orbital space and beyond. The 30-mile altitude of the mesosphere is low enough in oxygen pressure that rockets require both fuel and an oxidizer to provide burning thrust for the engines.

**M-172.** The mesosphere is the region that receives balanced heating from above and below, cooling off about as fast as it warms up. However, the atmosphere at this high altitude is too thin to provide lift for even a high altitude jet to operate. Most meteors entering the Earth's atmosphere burn up in the mesosphere.

*Thermosphere*

**M-173.** The thermosphere starts just above the mesopause, extending from an altitude of about 50 miles to between 200 and 375 miles. In this layer of the atmosphere, the air is so thin that a small increase in energy can cause a large increase in temperature. The temperature in the thermosphere depends upon solar activity and can reach almost 3,000 degrees Fahrenheit. This is important for satellites since they can be damaged by the temperature fluctuations if they are not properly prepared prior to launch.

**M-174.** The thermosphere includes the region called the ionosphere. The ionosphere is the region of the atmosphere that is filled with charged particles. Elevated temperatures from ultraviolet radiation can sometimes cause a molecule to become ionized, so the ionosphere and thermosphere can overlap. Different regions of the ionosphere make long-distance radio communication possible by bouncing radio waves back and forth between the Earth and the ionosphere. The waves then travel around the world. The ionosphere helps protect humans from unhealthy levels of sun-produced ultraviolet radiation. Within the region of the thermosphere is the lowest altitude at which a satellite in a circular orbit can circle the Earth for at least one revolution without propulsion (93 miles). At this altitude, one revolution of the Earth takes 89 minutes.

*Exosphere*

**M-175.** The exosphere begins where the thermosphere ends and has no definite outer limit. As distance from Earth increases, the already thin atmosphere within the exosphere gradually and almost completely dissipates into the vacuum of space. The density of atoms and molecules that make up the atmospheric gases in this region is so low that all of the particles of atmospheric matter surrounding the Earth at an altitude of 1,000 miles could be contained in one cubic centimeter at sea level. However, even at this 1,000-mile level, atmospheric drag caused by friction from collisions with individual particles in the exosphere slows satellites.

### Where Does Space Begin?

**M-176.** No clear line marks the beginning of space. Gravity and atmospheric density gradually decline as objects move away from the surface of the Earth, but both are still present well into what many think of as space.

**M-177.** There are several specific estimations of where space begins, ranging between 60 and 100 miles above the surface of the Earth. It is more accurate to say that space begins at the altitude where the velocity necessary to keep an object in orbit is no longer countered by so much friction of atmospheric drag that the object is immediately brought down by gravity.



### Near Space

**M-178.** The U.S. Air Force is focusing attention on an area above the surface of the Earth where nothing flies—no aircraft or satellites. This is a virtual no man's land. This region is sandwiched between an altitude of approximately 12 miles and about 60 miles. It is referred to as "near space." In near space, the air is too thin to support aircraft, and gravity is too strong for satellites to remain in a stable orbit. Yet, initiatives and studies are underway to see if this area can be exploited to become a key operational area for quick and less-expensive communications capabilities. This could include balloons, airships, or anything else that is cost-efficient, survivable, persistent, and responsive.

## Solar Effects on the Earth

**M-179.** Geomagnetic storms occurring between one and four days after a solar flare or other solar prominence event comprise clouds of solar material and magnetic fields that buffet the magnetosphere—a region of the extreme upper atmosphere that is dominated by the magnetic field. Charged particles are trapped in the magnetosphere, and it acts as a type of radiation shield for the earth. During geomagnetic storms, the interaction of the solar winds with the Earth's magnetosphere causes energy transfers. This causes the Earth's magnetic field to change rapidly in both direction and intensity.

**M-180.** Auroras are a visible sign of the atmospheric changes that can wreak havoc on technological systems. They result from geomagnetic storms. They illuminate the sky with glowing visual displays. The solar wind energizes particles in the magnetosphere that then enter the Earth's atmosphere near the polar regions. When the particles strike the molecules and atoms of the thin, high atmosphere, they produce colorful streams of light. An aurora will typically manifest itself between 60 and 80 degrees latitude. An increase in the intensity of the geomagnetic storm spreads the aurora toward the equator.

## Satellites

**M-181.** Although anything in orbit around Earth is technically a satellite, the term is normally used to describe a useful object deliberately placed in orbit to perform some specific mission or task. Virtually everyone in today's Army, either directly or indirectly, uses satellites. Satellite use is so embedded in today's global technology that it is virtually impossible for anyone not to be affected by it. However, the impact of satellites is not intuitively obvious to the average person:

- Satellites are not easily visible. A Soldier making a phone call does not think about the path the call takes to get to its recipient, nor does the Soldier particularly care as long as the call gets through.
- The cost of operating a satellite is distributed over so many customers that no one seems to have any claim of responsibility for it.
- The design, launch, and operation of a satellite is well beyond the means and knowledge of all but the largest and best-financed institutions and government agencies.
- For Soldiers to take full advantage of satellite capabilities in peace and war, they must use and understand those capabilities.

### What a Satellite Does

**M-182.** Satellite function depends on the type of satellite. Satellites come in many shapes and sizes and are designed for a variety of missions. Some satellites serve one specific purpose while others handle several tasks. In all cases, satellites communicate. Every satellite is built with components specific to the function and mission of that particular satellite. However, two components are common to all satellites:

- **Bus.** The platform or structure supporting the payload from the launch until the end of the satellite's life. The bus consists of the frame and subsystems, which include attitude control, power system, and orbital and thermal controls, as well as the tracking, telemetry, and command system.
- **Payload.** The payload comprises specialized equipment needed to perform the mission. For instance, a communications satellite has antennas, receivers, amplifiers, multiplexers, and other equipment required to perform the designed communications mission.

**M-183.** Most communications satellites carry active microwave repeaters, or transponders. (The word "transponder" is a contraction of "transmitter-responder.") The satellite receives signals from an Earth-station transmitter, amplifies them, translates them to another frequency, and then retransmits the signals to other terminals on the ground. The signal transmitted by a ground terminal is degraded during the signal's long-distance path through the atmosphere on its way to the satellite. Amplification on board the satellite ensures that the weak, distorted signal received at the satellite is restored to an accurate signal with sufficient strength to be relayed back to, and be successfully received by, an Earth station. The signal returning to Earth loses signal strength, but special equipment in a ground station amplifies the weak signal received from the satellite, processes it, and provides the recipient a sufficiently clear signal. Examples of differing characteristics, capabilities, and limitations of satellites are illustrated in figure M-34.

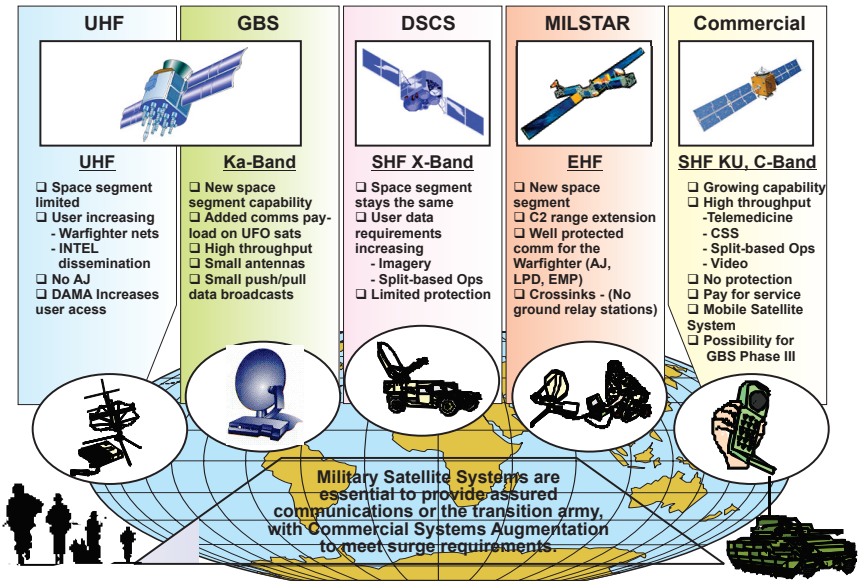



**Figure M-34. Different communications satellites for different missions**

## Satellite Orbits

**M-184.** An orbit is the path along which a satellite moves above the surface of the Earth. All Earth satellites orbit around a point at the center of the Earth. Each type of orbit allows satellites to perform their distinct missions. A constellation of weather satellites in low-Earth orbit (LEO) can pass over the same areas several times daily to update forecasters on conditions. Global Positioning System (GPS) satellites in medium-Earth orbits (MEOs) ensure that users on the ground have access to precise navigation information from several satellites at once. Military communications rely on geostationary satellites for constant global communications.

**M-185.** Although the weightlessness of space might appear to provide freedom to roam at will, nothing could be further from the truth. The laws of motion and the presence of gravity determine the motions of every object in space. It is possible for spacecraft to change their motions, but only after careful planning, great care, and expenditure of a tremendous amount of energy. Every change must be perfectly calculated.

**M-186.** Satellites are deliberately placed into predetermined orbits around the Earth. Successfully launching a satellite into a planned orbit is a major technical accomplishment. Normally, users are not concerned with how satellites get into orbit, but it is useful to have a basic knowledge of the process.

### *Attaining Orbit*

**M-187.** A ball straight up from the surface of the Earth would rise until gravity's pull stopped it, and then the ball would fall back to the Earth. If that ball were thrown straight up again at a faster speed (velocity), it would rise higher than before and then again return to the Earth. There is a speed called the escape velocity. If the thrown ball exceeds that speed, it will rise to an altitude high enough to resist atmospheric drag and the pull of gravity and will not return to Earth. If a ball were thrown instead with an arcing trajectory, at just enough initial velocity so that it would resist being slowed by gravity and air resistance, it would reach an altitude where its remaining outward velocity would exactly balance against the weaker pull of gravity and the small amount of atmospheric drag. The ball's motion away from the center of the Earth actually would stop, but the ball would be falling around the Earth rather than back toward it. It would be in a free fall in a low orbit around the Earth. The launch velocity (called orbital velocity) to achieve such an orbit is approximately 19,000 miles per hour.

**M-188.** Launching a satellite into a minimal LEO requires a period of powered flight during which the satellite is lifted above the Earth's atmosphere and accelerated to orbital velocity by a rocket or launch vehicle. Powered flight concludes at burnout of the launch vehicle's last stage, at which time the vehicle begins its free flight.

**M-189.** Launching a satellite is a two-part process: the launch phase, and the orbit insertion phase. In the launch phase, the satellite itself is placed aboard some type of expendable launch vehicle, such as a multistage rocket or the space shuttle (more formally known as the Space Transportation System [STS]). An expendable launch vehicle has multiple propulsion stages that separate from the vehicle after their propulsion is expended. After the stages separate, either they are destroyed or they burn up in the atmosphere. The upper stage booster rocket is lifted into a transfer orbit, where the satellite separates from it upon reaching the desired final orbital altitude. Some expendable launch vehicles can perform direct insertion of a satellite into a final LEO.

**M-190.** Attaining a higher altitude orbit—such as a geosynchronous orbit—requires additional energy. This energy is supplied by thrusters on board the upper stage booster. These fire repeatedly in small increments until the correct orbit is reached. This requires careful monitoring by ground controllers. Except for periodic minor adjustments, no more propulsion is necessary to keep the object in orbit after the final orbit is achieved. Once in space and stabilized in orbit, most satellites obtain power for their payloads from the Sun, using solar panels. If a satellite is in deep space, nuclear power supplies are sometimes carried on board for additional power.

*Orbital Characteristics*

**M-191.** Selection of the proper orbit depends upon the mission and purpose of the satellite. There are an infinite number of possible orbit configurations for a satellite. Orbits are not always circular. In fact, most orbits are elliptical, looking like a slightly squashed circle. The term eccentricity is a measure of how circular a satellite's orbit is. For a perfectly circular orbit, the eccentricity is zero; elliptical orbits have eccentricities between zero and one.

**M-192.** Inclination refers to the angle at which a satellite's orbit is tilted in relation to the Earth's equator. A 90-degree angle of inclination is a polar orbit. A zero degree angle of inclination is an equatorial orbit.

**M-193.** A satellite's orbital altitude determines how much of the Earth's surface is seen by a satellite. This altitude is selected based upon the mission of the satellite.

*Low-Earth Orbit*

**M-194.** Satellites in LEO are the closest to Earth, flying several hundred miles overhead. LEO systems are commonly used for observation, environmental monitoring, small communications satellites, and scientific payloads. LEO satellites are normally used for short, burst, narrowband communications using radio frequencies below one GHz. A satellite in LEO is generally considered to have an apogee (the highest point of its orbit) of no more than approximately 530 miles. At these distances, satellites need to be moving to service the entire coverage area. Usually, a single LEO satellite can only cover a surface area of 2,000 to 5,000 square miles.

**M-195.** LEO satellite may only spend tens of seconds over a given geographical area, which means that any given transmission may have to be picked-up and passed on by multiple satellites.

**M-196.** Most LEO orbits are nearly circular. LEO satellites tend to be slowed down by the thin atmosphere that remains at LEO altitudes. Without propulsion, the life span of a LEO satellite is less than five years.

**M-197.** LEO radio systems require less transmitter power to successfully send a quality signal because of the shorter signal path to Earth. Shorter signal paths also mean shorter signal delays, which is an advantage in the responsiveness of services such as cellular telephone or two-way interactive paging systems.

**M-198.** LEO radio systems can also be maneuvered with increased precision, which allows for the establishment and manipulation of fixed constellations. LEO satellites have the advantage of passing relatively close to areas on the Earth. Time delay is decreased for communications traffic. It is estimated that LEO satellites require between 1,200 and 3,500 times less power to communicate than do GEO satellites.

**M-199.** Because of their continuous motion relative to the Earth and their spot-beam antenna footprints, satellites in LEO have the disadvantage of not providing continuous coverage for a specific location on Earth. While LEOs can individually cover much smaller swaths of the Earth's surface, they are far less expensive to build and therefore can be launched in large numbers.

**M-200.** The satellite is in view from any given portion of its ground trace for only a short period before it passes out of view. Because of this, many LEO satellites are required to provide continuous service. Earth coverage is limited at lower altitudes and tracking antennas or omnidirectional antennas are required for ground terminals that access LEO satellites. NASA's Space Shuttle travels in LEO.

*Medium-Earth Orbit*

**M-201.** MEO is approximately 6,250 miles to 12,000 miles above the surface of the Earth. The orbit is just above the Van Allen radiation belts. Satellites in MEO orbit higher than LEO satellites, but lower

than geostationary satellites. A fleet of several MEO satellites with orbits properly coordinated can provide global wireless communication coverage.

**M-202.** Because MEO satellites are closer to the Earth than geostationary satellites, Earth-based transmitters with relatively low power and modest-sized antennas can access the system. MEO satellites orbit at higher altitudes than LEO satellites, so the useful footprint (coverage area on the Earth's surface) is greater for each satellite. Ten MEO satellites could provide communications coverage of the entire surface of the Earth. There is less chance of a "dropped call" using a MEO satellite constellation because the satellites are in sight for longer periods of time. A disadvantage of MEO satellites is that their orbits have them spending much of their time over empty areas, such as oceans, where few customers desire service.

***Geosynchronous Orbit***

**M-203.** In a geosynchronous orbit, a satellite completes an orbit in the same 24-hour period that the Earth rotates. From the Earth, such a satellite appears to be stationary in the sky. A satellite in this orbit is considered to be in a high altitude orbit at approximately 22,300 miles above the surface of the Earth. At this elevation, the gravitational force pulling a satellite towards the Earth is exactly balanced by the centrifugal force pushing it outward.

**M-204.** A geosynchronous satellite's orbit can have any inclination. This inclination factor differentiates a geosynchronous orbit from a geostationary orbit. A geosynchronous orbit is said to be inclined when the plane of the satellite's orbit is at an angle to the plane of the Earth's equator. For inclinations other than zero degrees, a geosynchronous satellite's ground trace will be a figure-eight straddling the equator. Satellites in geosynchronous orbit include communications, weather, and surveillance or warning satellites.

***Geostationary Orbit***

**M-205.** A geostationary orbit is a special type of geosynchronous orbit in which satellites are positioned at approximately 22,300 miles above the surface of the Earth, directly over the equator. The satellite completes an orbit in the same 24-hour period as the Earth's rotation with an inclination that is very near to zero. For any orbit to be geostationary, it must first be geosynchronous.

**M-206.** While all geostationary orbits must be geosynchronous, not all geosynchronous orbits are geostationary. Unfortunately, these terms are often used incorrectly and interchangeably. The geostationary satellite remains motionless over a single spot on the Earth's equator and provides a continuous view of the same portion of the Earth. The beams transmitted by the satellite to the Earth, and from an Earth station to the satellite, can remain fixed without ground station antennas having to track the satellite. This simplifies the design and operating requirements of both satellites and ground stations.

**M-207.** The fact that there is only a single geostationary orbit presents a serious limitation. Just as in putting beads onto a loop of string, there are only so many slots into which geostationary satellites can be placed usefully. Satellites must be spaced along the geostationary ring and have frequencies allocated to them in such a way that their transmissions do not interfere with the uplinks or downlinks of the satellites adjacent to them. Additionally, they must be spaced so that the satellites avoid collisions.

**M-208.** The uniqueness of a geostationary orbit lies in the fact that there is only one precisely geostationary Earth orbit, yet it has become the world's popular standard for the flying of most communications satellites that require maximum Earth coverage. There are already many satellites positioned in geostationary orbit and, because of the advantages this orbit provides, the numbers will continue to increase. Therefore, it is difficult for providers to obtain desirable locations for their new satellites. This orbit is highly controlled to prevent overcrowding, cluttering by orbital debris, and unauthorized use of this orbital resource.

**M-209.** It takes more time and energy for a launch vehicle to put a satellite in geosynchronous orbit than for any other type of orbit used for communications satellites. Although, theoretically, a geosynchronous orbit is an orbit in which the satellite does not move with respect to the Earth, in reality this condition would not be true for very long. Over time, the orbit becomes degraded from an ideal geostationary balance by disturbances from the moon and solar activity. More fuel is required to keep a satellite in the proper geostationary orbit at near-zero inclination to maintain the orbital plane close to the equator.

**M-210.** The geostationary orbit is also named the "Clarke" orbit after the visionary science fiction writer Arthur C. Clarke who, in 1945, first described its use for orbiting communication stations.

### *Elliptical Orbits*

**M-211.** A satellite in an elliptical orbit swings closer to the Earth at one extreme of its orbit and further away from the Earth at the other extreme. The speed of a satellite traveling in an elliptical orbit increases as it gets closer to the Earth and slows as it travels away from the Earth. Satellites in such an orbit must be hardened because they pass repeatedly through the Van Allen radiation belts.

**M-212.** A highly elliptical orbit that was first used by Russia is called a Molniya orbit. A satellite in Molniya orbit is semi-synchronous, "dwelling" about six to eight hours of every 24-hour period over a particular region of the Earth. This is ideal for communications satellites used to provide coverage in the extreme northern latitudes where access to geostationary satellites can be difficult. By calculating and setting a Molniya orbit properly, a great deal of control can be gained over how much time the satellite dwells over any given place and at any given altitude. There are systems of other satellites in Molniya orbits in which ground systems switch among three or four such satellites in order to receive continuous coverage. Advantages of Molniya orbits include providing good coverage in the north polar areas and long dwell times. Disadvantages include the need for multiple satellites for continuous coverage and the poor coverage they provide of the Southern Hemisphere. There can also be a problem in transmission delays and signal losses when the satellite is at the near-apogee part of the orbit because of the great distance from the surface of the Earth.

### *Polar Orbits*

**M-213.** A polar orbit is any orbit that has an inclination of, or very close to, 90 degrees. Mapping and surveillance satellites are frequently placed in this type of orbit. Because the Earth rotates below a polar orbit, the satellite has low-altitude access to virtually every point on the surface of the Earth. Much more propellant, or energy, is required to put a satellite into polar orbit. Because of the inclination of a polar orbit, the launch vehicle must provide all of the energy needed to attain orbital speed.

### Other Factors Influencing Orbital Selection

**M-214.** Other factors that influence the selection of an orbit include—

- Radiation.
- Transmission latency.
- Orbital parking.
- Satellite stabilization.

### *Radiation*

**M-215.** The two Van Allen radiation belts require spacecraft traveling in and near them to be heavily protected against radiation. Launch costs are increased because the protective shielding that is required adds a great deal of weight to the spacecraft. The location and size of the two Van Allen belts vary, depending on the season and solar activity. The lower belt starts at between 250 and 750 miles and goes out to about 6,200 miles. After a gap, the second belt resumes at about 37,000 miles and extends out to 52,000 miles. Orbits are planned outside these belts, and the amount of time a satellite might spend in the radiation zones is kept to a minimum.

*Transmission Latency*

**M-216.** Another factor influencing orbital selection is transmission latency. The higher the altitude, the longer it takes for a signal to or from the satellite to reach its destination. In a LEO, it takes 20 to 40 milliseconds for a signal to go from a terrestrial location up to the satellite and then have the retransmitted signal travel down to a terrestrial receiver elsewhere. For a satellite in a geostationary orbit, it takes about a one half of a second for a signal to travel to it from a station on the ground and then down to another ground station. For the most part, geosynchronous satellites are no longer used to carry telephone conversations because the half-second latency has proven distracting to voice conversations.

*Orbital Parking*

**M-217.** A satellite placed into geostationary orbit is said to be "parked" in a preassigned slot. This is similar to parking cars in a parking lot. Some parking slots are better than others, and the best slots fill up first. A slot consists of a frequency allocation coupled with a given geostationary orbital position. Satellites can be positioned in slots where they can cover the greatest area for specific types of communications.

**M-218.** Satellite parking slots are assigned by domestic and international agencies. The agencies give full consideration to frequency band, power levels, and coverage areas in order to minimize interference with other satellites. Countries are allocated slots within an "arc" of the geostationary orbit by negotiation with the ITU. Then, a national regulatory body can assign specific orbital slots. In the case of geostationary satellites over the continental United States, the Federal Communications Commission (FCC) assigns the slots within the allocated arc.

**M-219.** For communications satellites operating in the same frequency bands, the spacing between their orbital slots must be great enough to assure minimal interference between transmissions to and from adjacent satellites. It is interesting to note that the FCC has progressively reduced the spacing required between satellites due to the demand for orbital slots. This is driven by the requirement for additional capacity as well as by improvements made in antenna and filter technologies, enabling tighter spacing of satellites.

**M-220.** A geostationary parking slot is designated by the line of longitude over which it is positioned at the equator. Skill and precision are needed to maneuver a satellite into its parking slot and then keep it there. Controllers on the ground must constantly monitor the satellite once it is in position to ensure it does not wander too far away from its assigned position. A satellite is not be allowed to shift position from its assigned parking slot by more than about one-tenth of one degree of orbital arc. This ensures that satellites do not interfere with other satellites' signals within each frequency band.

**M-221.** An important point to remember with orbital parking slots is that in geostationary orbit, there is only room for a finite number of satellites. There is a limit to how effectively technology can increase the capacity of the orbit to accept new satellites with such measures as narrow transmission beams, polarization schemes, and precision launching and positioning. Packing more satellites into geostationary orbit would ultimately affect the efficiency of the orbit's use and the quality of communications it supports.

*Satellite Stabilization*

**M-222.** Once a satellite has attained the proper orbit, it must be stabilized. If a satellite is not stable and moving predictably, then it cannot function properly. For instance, a communications satellite must have its antennas pointed toward its receiving station on the surface of the Earth. Reconnaissance satellites must have their sensors pointed toward the right countries. There are two techniques used to stabilize satellites: spin stabilization, and three-axis stabilization.

**M-223.** Spin stabilization works similar to a gyroscope. A satellite remains stable as long as it is

spinning at a relatively fast speed. Satellites using spin stabilization are often cylindrical in shape and make about one revolution per second. If sensors detect any deviation in the spinning, thrusters correct the spin and restore stability. Any antennas mounted on the satellite are designed not to spin.

**M-224.** Three-axis stabilized satellites have small spinning wheels that rotate in such a way that they keep the satellite in the same orientation to the Earth and the Sun. If any of a satellite's sensors detect a deviation on any of the three axes, a control signal is sent to the satellite to instruct the wheels to spin faster or slower in order to make the correction and reorient the satellite.

### Solar Effects on Satellites

**M-225.** Geomagnetic storms and increased solar winds heat the Earth's upper atmosphere, causing it to expand. Increased density of particles in the exosphere induced by the temperature increase causes drag on satellites in LEO. This drag slows a satellite and causes a slight change in orbit. Unless satellites are boosted to a higher orbit, they slowly fall and eventually burn up in the atmosphere.

**M-226.** Computers on board satellites can be affected by energetic solar particles. The miniaturized components on the satellites are vulnerable, and the physical damage caused by solar particles can affect software commands to the satellite. Many electrical devices are so tiny that the passage of even one particle can cause data corruption. Although radiation-hardened components have been created for satellites in recent years, their high cost and low availability can be a problem for satellite manufacturers who are under pressure to reduce costs.

**M-227.** Another effect of solar activity on satellites is called differential charging. During geomagnetic storms, the number and energy of electrons and ions increase. When a satellite travels through this energized environment, the charged particles striking the satellite cause different portions of the satellite to become differentially charged. Eventually, electrical discharges can arc across internal satellite components, causing enormous damage.

**M-228.** Satellite shielding is available, but is heavy and costly to put into space. Designers construct satellites with the minimum amount of shielding they deem necessary to keep the satellite functioning without excessive costs. This strategy is probably acceptable if the gamble pays off and the predicted environmental conditions are accurate for the life of the satellite. If the predictions are incorrect, however, and the protective shielding is inadequate, the satellite may be lost.

### Advantages of Satellite Use

**M-229.** The importance of satellites is based on several characteristics. When used in the proper applications, several features give satellites unique advantages.

#### *Economical, Long Distance Communications*

**M-230.** The cost of transmitting information between two users via satellite is essentially the same, regardless of the distance. A signal can be relayed across the country or across the ocean by satellite as cheaply as across the street using a satellite.

#### *Broadcast Capability*

**M-231.** Satellites can be used as broadcast transmitters. The signals from an Earth station, relayed by a satellite, can be received over a wide area by multiple stations within the coverage area.

#### *Uniform Service Characteristics*

**M-232.** Satellites can deliver the same consistent set of services at costs that are potentially much lower than those of terrestrial systems.

*Wideband Capability*

**M-233.** Satellites are usually wideband (high throughput) devices that can relay large amounts of information within a given amount of time.

*Broad Coverage*

**M-234.** Technically, a satellite can serve any suitably equipped ground station within its footprint (the area of the Earth within view of the satellite's antenna). A satellite can provide the same type of service to cities and to rural areas. Transmission from a satellite to a broad area of the Earth's surface is not constrained by natural or manmade barriers, such as mountains, oceans, or cities. However, there may be some locales within the broad coverage area where a ground terminal antenna cannot get an unobstructed view of the satellite because of the proximity of mountains or buildings. This can be more of a problem near the fringes of the broad coverage area, where the satellite appears closer to the horizon.

*New Services*

**M-235.** The capabilities of satellites are rapidly giving rise to new communications concepts. Soldiers now have a greater variety of information at their disposal in different forms such as voice, data, video, and imagery, than ever before. Commanders are able to select from a rich variety of satellite-relayed information and services to aid in their decisionmaking processes and to accomplish their missions.

*Mobile Users*

**M-236.** Satellites are uniquely positioned to offer services to users on land, sea, or in the air. Although satellites can be connected to the terrestrial infrastructure to extend the range of services, satellites are distant enough from the terrestrial infrastructure to be unaffected by its outages.

*Rapid Deployment of Service*

**M-237.** Satellites that are already deployed and operational can be activated quickly to provide service to the Soldier when required. This can be done faster than installing a comparable capability using the terrestrial infrastructure. On the horizon are microsatellites that can be launched quickly to augment capabilities in an area of operations (AO) or to replace a satellite that has malfunctioned.

**Disadvantages Associated with Satellites**

**M-238.** There are a number of problems associated with satellites.

*Cost*

**M-239.** Satellite networks are usually expensive. On board computers for satellites to communicate with each other and/or ground stations must be designed and then maintained. These computers must have backups and extensive memory. Each satellite must be monitored constantly. Eventually all satellites need replacement.

*Solar Effects*

**M-240.** Heating, thermal cycling, material damage, and sensor noise all affect satellite hardware. The Sun emits electromagnetic radiation that produces noise in a communication link. Fast charged particles from solar weather events can produce radiation damage, internal charging, single-event upsets, and arcing within components.

*Rain and Ice Effects*

**M-241.** Rain acts as a curtain between the antenna on the ground and the satellite. Raindrops absorb energy from the waves, reducing the signal when it is transmitted over long distances. Antennas are designed to reflect the signal to a focal point. When ice accumulates on the antenna, the signals may not reflect to that one point. The original signal is distorted upon its reception at the satellite.

*Latency*

**M-242.** Signals travel between the transmitter and receiver; the time between transmission and receipt

of the signal is called latency. The latency time varies based on the type of orbit.

***Orbital Debris***
**M-243.** Mechanical damage can occur from collisions and induced arcing within internal components of the satellite.

***Atmospheric Effects***
**M-244.** Drag, torque, material degradation, vacuum, and contamination are effects to which satellites in LEO are particularly vulnerable.

***Obsolescence***
**M-245.** Many satellites require years to construct. What was originally state-of-the-art technology providing significant capabilities may have been outstripped during building.

***Repair Difficulties***
**M-246.** Satellites cannot be brought into a maintenance facility for repairs or periodic maintenance. Any repairs must occur through remote commands from ground stations.

***Limited Ability to Alter Orbit After Launching.***
**M-247.** Altering a satellite's flight path or orbit is not as simple altering the same for an airplane. Consequently, there is a minimal likelihood of changing a satellite's access time to a target.

## Military Applications of Satellites

**M-248.** Satellites have many uses, including weather observation and forecasting, navigation, sensing and communications.

**Weather Satellites**
**M-249.** The U.S. launched the world's first weather satellite—Television and Infrared Observation Satellite (TIROS)—on 4 April 1960. TIROS was very small, weighing only 122.5 kilograms and was shaped like a hatbox. The first transmitted weather picture showed clouds over the Gulf of St. Lawrence. Before it died, TIROS produced 22,500 photographs of the Earth's weather. By 1965, nine additional TIROS satellites, carrying better sensors, had been launched to measure weather patterns.

**M-250.** In 2005, Soldiers deployed in Iraq received warnings of sandstorms, rain, winds, and other forms of severe weather through weather satellites that were equipped with more modern sensors. Weather satellites help meteorologists predict the weather or see what is happening meteorologically at the moment in any part of the world. These satellites carry cameras that can return photos of the Earth's weather patterns, either from fixed geostationary positions or from polar orbits.

**M-251.** NOAA operates numerous meteorological satellites in unique constellations (orbits). Military meteorologists receive valuable environmental information from these satellites.

**M-252.** Although the use of satellites to observe, monitor, and report solar activity has revolutionized knowledge about the complex physical forces that drive space weather systems, there is still much to learn. Reliance on technological systems, particularly in satellite communications, is growing exponentially. These systems are susceptible to failure or unreliable performance because of the extreme conditions of space. Reliable space weather forecasting is not yet possible, but observations of solar activity and rapid dissemination of critical information through the Internet is possible. Bulletins, forecasts, alerts, warnings, and data are routinely disseminated to a broad range of recipients, including satellite operators, navigational systems users, and telecommunications operators.

**M-253.** The Air Force Weather Agency (AFWA) provides timely, accurate, and continuous air and space weather information for all Department of Defense (DOD), multinational, and national users in any AO around the world and in space. This includes space weather analyses, forecasts, and alert notifications.

**M-254.** The mission of Air Force weather observatories is to monitor solar flares, noise storms, and other releases of energy from the sun and—when necessary—notify military and civilians concerned with space, weather, power, and communications in countries throughout the world. Some solar monitoring is done in space. AFWA is the primary user of the Defense Meteorological Satellite Program (DMSP) and works in partnership with National Oceanic and Atmospheric Administration (NOAA) to continually improve this developing science. AFWA has observatories in Australia, Italy, Puerto Rico, Massachusetts, New Mexico, and Hawaii. This allows Air Force space weather technicians to constantly monitor the sun.

**M-255.** The DMSP is used for strategic and tactical weather prediction. The DMSP aids the U.S. military in planning operations at sea, on land, and in the air. Each of four DMSP satellites has a 101-minute, near-polar orbit at an altitude of 830 kilometers above the surface of the Earth.

**M-256.** Equipped with a sophisticated sensor suite that can capture visible and infrared images, DMSP satellites can "see" such environmental features as clouds, bodies of water, snow, fire, and pollution. Scanning radiometers record information that can help determine cloud types and heights, land and surface water temperatures, water currents, ocean surface features, ice, and snow. Communicated to ground-based terminals, the data is processed, interpreted by meteorologists, and ultimately used in conducting U.S. military operations worldwide. These polar orbiting weather satellites produce extremely high-resolution images and provide weather coverage in areas of the world not normally viewable by geostationary weather platforms.

**M-257.** Operational interests in weather data vary. Army tank commanders want to know the moisture content of soil in a potential AO. Navy ship commanders are interested in winds and sea states. Air Force pilots want to know about thunderstorms that may be in their projected flight path or they may seek to avoid flying in areas where conditions are susceptible to telltale contrails. DMSP can provide all of this information.

### Geostationary Operational and Polar-Orbiting Environmental Satellites

**M-258.** DOD weather forecasters rely on additional environmental satellites to augment weather information from DMSP. These additional space-based platforms are geostationary operational environmental satellites (GOES) for short-range warning and real-time forecasting and polar-orbiting environmental satellites (POES) for longer term forecasting. Both systems are necessary to provide a complete global weather monitoring system. The satellites also carry search and rescue instruments, and have helped to save the lives of about 10,000 people to date. They are also used to support aviation safety (volcanic ash detection), and maritime/shipping safety (ice monitoring and prediction).

**M-259.** A consolidation of military and civilian weather satellite programs is currently underway. However, it is unclear what the new merger will look like. Extensive budget concerns prompt continuous evaluation of how many and what kind of DOD-weather satellite capabilities are practical for military use in the out-years. The DOD's overall goal is to increase the timeliness and accuracy of severe weather event forecasts as well as achieve cost effectiveness of weather satellite operations.

### Navigational Satellites

**M-260.** Satellite technology provides a new perspective on the surface of the globe. The public has been the beneficiary of the extensive research and developments in navigation pioneered by the military. The impetus behind the development of satellite navigation was primarily the need of nuclear submarines for an alternative navigation system to update their inertial navigation system.

This need led the U.S. Navy to establish the transit program in 1958. Operating in near-polar orbit at an altitude of 600 miles, Transit satellites transmitted a navigation message on two frequencies. The multiple frequencies served to compensate for any signal distortion due to the atmosphere. In 1962, the Navy declared the system operational, and in 1967, civilians were able to enjoy the benefits of transit satellites that could tell them where they were within 80 feet.

**M-261.** The best-known navigational satellite system is the GPS. Advanced military applications of GPS technology range from guiding cruise missiles and smart bombs to helping Soldiers locate their precise positions in the desert or in rugged terrain. Practical commercial uses include land surveying, transportation monitoring, and precision navigation. Anyone with a few hundred dollars to spend on a GPS receiver can use the system. In 1993, the former Soviet Union established a GPS-equivalent system known as the Global Orbiting Navigation Satellite System (GLONASS). GLONASS uses the same number of satellites, relatively the same frequencies, and similar orbits to the GPS system. Many handheld GPS receivers can also use the GLONASS data, if equipped with the proper processing software.

**M-262.** Galileo is a planned European-satellite navigation system similar to GPS and GLONASS, but it will be operated on a purely civilian basis. It is being developed by the European Space Agency in collaboration with the European Union. It is the first such joint project.

**M-263.** The applications for navigation satellite systems, particularly GPS, are on the rise. For the Soldier, navigation satellite systems have proven advantageous in aerial surveys and targeting data. There has been considerable work done using GPS technology in search and rescue applications. Automobile manufacturers integrate GPS technology into new automobiles. Soldiers have GPS receivers as part of standard issue equipment when deployed.

### Reconnaissance or Remote Sensing Satellites

**M-264.** Satellites designed for geospatial intelligence (GEOINT) provide multispectral remote sensing from space for Earth resource management applications, as well as for intelligence collection. One of the most important aspects of GEOINT satellites is the resolution of the images provided.

**M-265.** During the late 1950s through the early 1970s, CORONA, Argon, and Lanyard were U.S. photographic reconnaissance satellites designed to assess how rapidly the former Soviet Union was producing long-range bombers and ballistic missiles, and where they were being deployed. The satellites' global coverage helped produce maps and charts for the DOD and other U.S. Government mapping programs. These early reconnaissance satellites used film canisters that were returned to Earth in capsules. The capsules were recovered by specially equipped aircraft during parachute descent, but were also designed to float and permit recovery from the ocean if necessary. All film was black-and-white, with the exception of some small samples of infrared and color film carried on some missions as experiments.

**M-266.** Today, the technology has matured. Reconnaissance satellites are an absolute necessity in conducting major military operations. There are three major types of reconnaissance satellites—photographic, signals intelligence (SIGINT), and infrared.

**M-267.** Photographic intelligence satellites use telescopes to take extremely clear, high-resolution pictures from high orbit. The United States relies heavily on its reconnaissance satellites in all of its worldwide operations.

**M-268.** SIGINT satellites pick up radio signals and microwaves. They can also trace both the source and recipient of transmissions. Analysts can often determine whether an important activity or event is occurring by the number of transmissions from or to a specific location.

**M-269.** Defense Support Program (DSP) satellites use infrared imaging to detect changes in the amount of heat coming from sources on, or near, the Earth's surface. The military uses these to track heat blooms, the sudden bursts of heat created by a missile launch. DSP satellites were instrumental in defending against SCUD launches during Operation Desert Storm.

### Communications Satellites

**M-270.** The Army can take credit for launching the world's first communications satellite, Score. It was by no means a true communications satellite in that it had only limited capability for real-time relaying of voice communications between two ground stations. However, by transmitting President Eisenhower's prerecorded Christmas greetings to the world, Score proved the concept that communications could be broadcast from space. The world's first true communications satellite was a 100-foot diameter Mylar balloon launched on 12 August 1960. Echo 1 was a passive communications satellite because signals sent from a ground transmitting station were bounced off Echo 1 and reflected to another ground receiving station. Again, President Eisenhower recorded a global message that became the first transmission received from the Echo satellite. Echo 1 remained in orbit until 24 May 1968.

**M-271.** Communications satellites are divided into two groups: active and passive. When satellites were first developed, passive communications satellites showed the most promise. With the advent of advanced semiconductor circuitry, active satellite payloads aboard a single satellite could carry the electronics needed to support thousands of telephone calls, data transmissions, and television programs. As this technology flourished, passive satellites were no longer used.

**M-272.** Today, communications satellites are an invisible, but indispensable, part of everyday life. Satellites have tremendously improved the quality and efficiency the operations of people, businesses, and governments. For example, worldwide, satellite-supported communication reduces the need for long-distance travel. The Soldier primarily uses Defense Satellite Communications System (DSCS), UFO, and Milstar communications satellite constellations. There are, however, many commercial satellite providers augmenting DOD satellite systems. Inmarsat, Iridium, and INTELSAT are only a few of the commercial satellite systems in use by Soldiers. Figure M-35 depicts an operational overview of satellite communications.

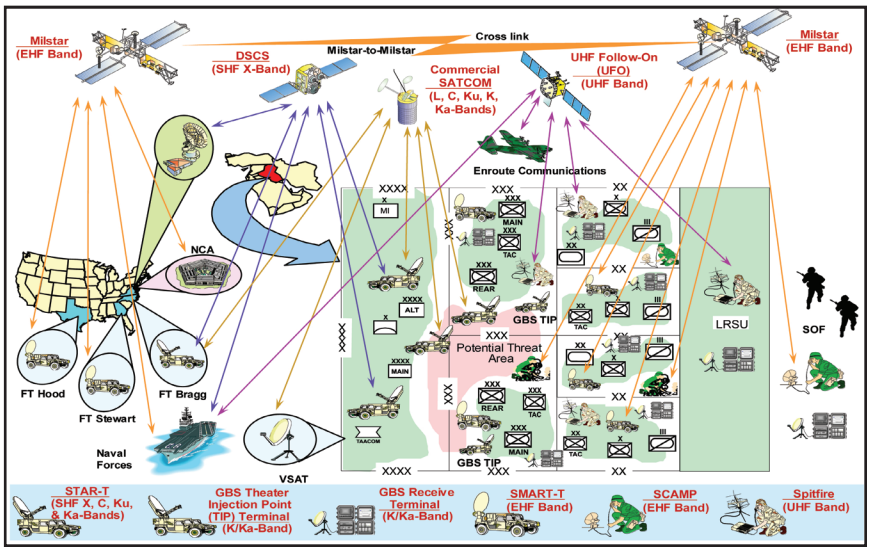



**Figure M-35. Operational overview of satellite communications**

### Space Systems

**M-273.** Space systems are not launched and left to perform their missions without further caretaking. Satellites are complex pieces of equipment that cost millions of dollars to design and launch. To keep a satellite functioning over its expected lifespan requires almost constant attention through a complex network of equipment and people. There are three distinct segments in a space system: the space segment, the control segment, and the ground segment.

#### *Space Segment*

**M-274.** There are two parts to the space segment: the satellite platform (the basic load-bearing frame of the satellite) and the payload. The payload's functions and capabilities are the reasons a satellite is placed in orbit. The payload—the specialized equipment needed to perform the mission— provides space-based capabilities to the users and distinguishes one type of satellite from another.

#### *Control Segment*

**M-275.** The control segment is responsible for the operation of the overall system, which includes platform control, payload control, and network control. The control segment consists of ground satellite control facilities, systems on board the satellite, and communications networks linking the control facilities.

#### *Ground, Terminal, or User Segment*

**M-276.** This segment comprises the actual equipment on the ground that receives and transmits signals to the satellite. Ground terminals can vary from a hand-held or man-packable terminal to a fixed or mobile shelter containing the equipment.

## Satellite Communications Frequencies of Interest to the Army

**M-277.** Many different frequencies are used in satellite communications. The most useful frequencies lie in the microwave bands between approximately 300 MHz and 300,000 MHz. The frequency bands of interest for Army satellite communications are UHF, SHF, and EHF. A valuable advantage exists in these frequency ranges—the atmospheric interactions with the physical properties of the electromagnetic waves provide propagation characteristics that can be used to transfer information.

### Ultra High Frequency Satellite Communication

**M-278.** The Army uses UHF for its tactical narrowband satellite communications. Military UHF SATCOM, in particular, refers to communications in the band of frequencies from 225 to 400 MHz. (The lower portion of this military UHF band is technically in VHF band according to the ITU definitions.) Access to UHF channels can be difficult because this is an overcrowded part of the spectrum. UHF is also vulnerable to jamming. Figure M-36 shows UHF satellite constellations, coverage areas, and capabilities.

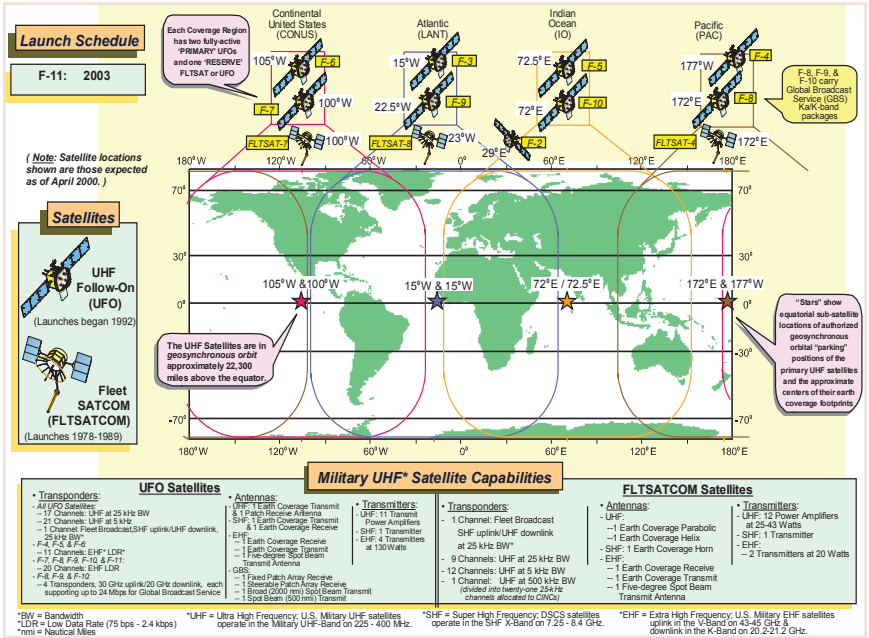



**Figure M-36. Military UHF satellite and coverage areas**

### Super High Frequency Satellite Communications

**M-279.** The SHF frequency band is used by the Army for wideband satellite communications and spans the C-, X-, and Ku-bands, and a portion of the Ka-band.

### *C-Band*

**M-280.** C-band, the most developed frequency band, is used for commercial SATCOM ranging from 3.7 to 6.425 GHz. C-Band is further divided into separate halves, one for ground-to-space links (uplink), which is from 5.925 to 6.425 GHz, and one for space-to-ground links (downlink),which is from 3.7 to 4.2 GHz. C-band frequencies are also allocated to terrestrial radio relay microwave systems used by telephone companies to interlink switching centers. Power flux density limits of satellite downlink transmissions are set and enforced by international agreements to minimize interference from satellites into terrestrial radio relay networks.

### *X-Band*

**M-281.** Within the SHF band, the military commonly uses the term X-band to mean the specific band of frequencies from 7.25 to 8.4 GHz. This band is strictly for military use. Although the lower portion of this band of frequencies actually falls within the C-band, calling it X-band distinguishes it from the rest of the C-band and the Ku-band, the frequencies used predominantly for commercial SATCOM. The U.S. Government has used the X-band for years for military communications services.
Military use includes both fixed and mobile satellite services, as well as terrestrial mobile services. In this band, attenuation due to rain and other atmospheric conditions is negligible. The Army uses the X-band for communications via the DSCS satellite constellation.

### *Ku-Band*

**M-282.** The Ku-band's opening as a useful SATCOM spectrum came as a result of the lack of enough available C-band frequencies to meet growing requirements. The frequency range allocated

for Ku-band is 11.7 to.5 GHz. Ku-band is also further divided into separate halves, one for uplinks (14 to 14.5 GHz) and the other for downlinks (11.7 to 12.2 GHz). Greater attenuation due to rain and other atmospheric conditions in this band becomes a factor in designing for adequate satellite communications. Such attenuation is usually overcome by designing extra power margins into the links. This means that additional power must be available on board the satellite for more powerful transmissions and more sensitive reception to overcome the attenuation caused by rain. The Army makes extensive use of C-band through multiple leases and service agreements with commercial service providers and commercial satellite companies. With the increasing congestion of the Ku-band, commercial satellite providers are shifting their focus to other portions of the electromagnetic spectrum, most notably Ka-band.

### *Ka-Band*

**M-283.** Because it is a fairly untapped portion of the electromagnetic spectrum, the Ka-band (30 GHz uplink and 20 GHz downlink) is attractive for wide band applications. Ka-band antennas can be smaller; however, transmissions in this band can be significantly degraded by rain attenuation. Ka-band development has been slow due to a host of factors, not the least of which is the downturn in the global economy. This reduction has forced the cancellation of some service rollouts and significant delays/modifications to others. For the Army, commercial Ka-band is being leveraged for use in mobile voice applications. Global Broadcast Service (GBS) uses Ka-band via special packages which were placed on UFO satellites eight, nine, and ten specifically for interoperating with GBS. The DOD wide band Gapfiller Satellites (WGS) will provide commercial Ka-band capabilities to Army users.

### Extremely High Frequency Satellite Communications

**M-284.** The Army uses EHF for protected communications over the Milstar satellite constellation. Its use has been expanded to other communications applications. EHF is not yet a widely used portion of the spectrum, so there is more bandwidth available. Bands within EHF are even more sensitive to attenuation because of the shorter wavelength; higher power is required for transmissions. (See figure M-37.)

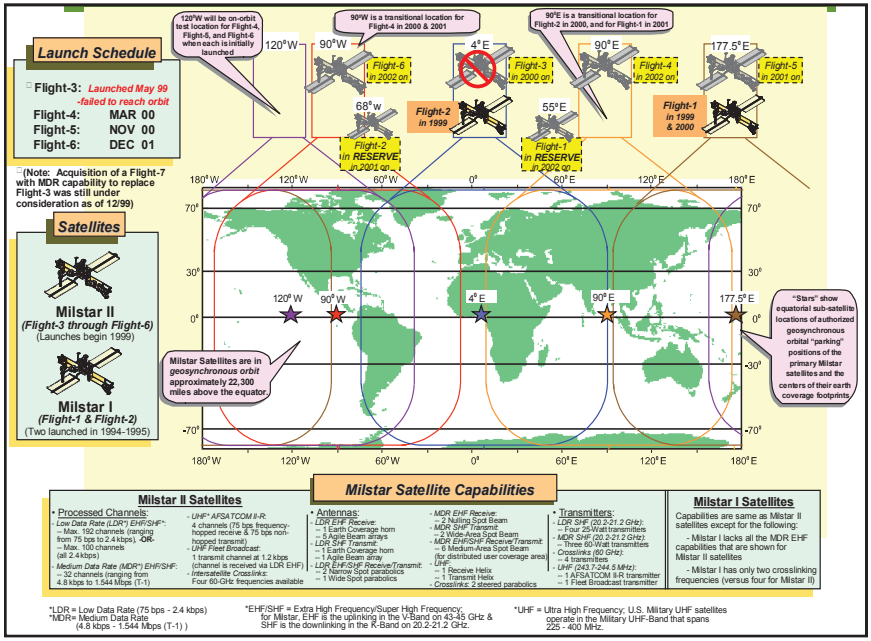



**Figure M-37. MILSTAR coverage and capabilities**

## Transponders and Techniques

**M-285.** Successful intelligence Soldiers understand how the characteristics of channels relate to satellite transponder power and bandwidth, and how the bandwidth is used. These factors influence how many channels a satellite can provide. Bandwidth has already been discussed. Increasing the transmitting power of a satellite transponder—also known as amplification—can expand the number of available channels. Because greater power requires more weight, the number of channels is also related to the launch weight limitation of the satellite. Polarization diversity techniques can also increase the number of channels per satellite while staying within the bandwidth limitation.

**M-286.** Current satellite transponders provide wide bandwidth—enough to accommodate thousands of voice circuits—when links to ground terminals are optimized to achieve high throughput capacity. There are several common multiple access techniques. There are benefits and limitations of each method and they become more apparent when they are applied in specific network applications. Selection of a specific technique depends upon the network application, the traffic profiles of each subscriber, and how traffic throughput delays are tolerated. Techniques include—

- Frequency division multiple access (FDMA).
- TDMA.
- Polling/round robin/roll-call.
- CDMA.
- Demand-assigned multiple access (DAMA).
- Contention.

### *Frequency Division Multiple Access*

**M-287.** This is a static multiple access technique where transponder bandwidth is subdivided into smaller frequency bands (or subchannels). Each subchannel is then assigned to a specific user. This


FOR OFFICIAL USE ONLY

method is frequently used but it does not readily adapt to changing traffic loads.

***Time Division Multiple Access***

**M-288.** TDMA is a static multiple access technique where a transponder's full bandwidth is assigned to each user during a specific time slot in a cyclic period. This method, frequently used, does not readily adapt to changing traffic loads. (See figure M-38.)

***Polling/Round Robin/Roll-Call***

**M-289.** This is a dynamic multiple access technique where the total transponder bandwidth is made available to a user for the duration of time that the user requires. Upon transmission completion, channel access is passed to the next user on the polling list in a cyclic manner. The polling techniques are not suitable for networks having a large number of users because of the time needed to cycle through the polling list.

***Code Division Multiple Access***

**M-290.** CDMA is a dynamic multiple access technique that employs a separate and distinct code for each user to access a traffic channel at any instant in time using the full bandwidth of a satellite transponder. Overall bandwidth is shared with other users. This technique is also called spread spectrum. CDMA has an inherent resistance to electronic countermeasures but is expensive to implement.

***Demand-Assigned Multiple Access***

**M-291.** DAMA is a family of multiple access techniques where each user can dynamically reserve communications space on a channel upon demand, based on individual need. DAMA methods are the most efficient of the techniques for networks of users with varying traffic loads, but the automated reservation (control) system technologies are complex and still undergoing refinement. (See figure M-38.)

***Contention***

**M-292.** Contention is a family of dynamic multiple access techniques where a user competes with all other users for channel space by transmitting when required. If separate transmissions collide, the corrupted transmissions are attempted again after a random delay. This technique is economical to implement but is suitable only for small-to-moderate sized networks of low-demand users.

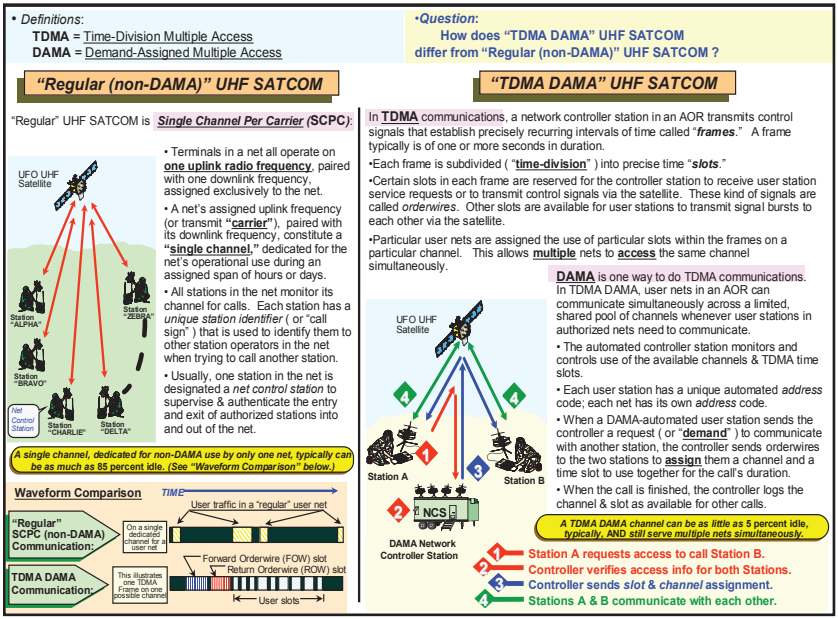



**Figure M-38. Explaining UHF, SATCOM, TDMA, and DAMA**

## Transmission and Information Rate

**M-293.** There are significant demands on the communications transport structure. These vary, depending upon the mission requirements, available assets, desired services, and systems capacity. Wider bandwidth does not necessarily mean that information can flow at a proportionally higher rate. It is important to know this when planning for SATCOM resources.

**M-294.** Transmission (or data) rate and information rate (or information throughput rate) are not necessarily equivalent. Typically, for a given number of bits of original information to be conveyed, many more bits must be transmitted through a communication channel than the number of original information bits. This is because encoding schemes and error detection and correction techniques may be applied to the data before it is transmitted. Such processes increase the number of bits actually transmitted. Theoretically, information rate could equal but never exceed the transmission rate and, in reality, the actual information rate is always less than the transmission rate.

**M-295.** Many factors determine transmission and information rates. Network planning and routing paths have an effect. The speed of the user's terminal device receiving the incoming information may be slower than the pipe delivering the information. Users must not assume that just because a given transmission system operates at a particular speed that the information they need to send will pass from point A to point B at the same speed. It usually will not.

## Satellite Antennas

**M-296.** Antennas are essential components of a satellite system. They are located on board satellites and as part of the ground equipment suites. A common question that often arises concerns the distance of the transmitter (satellite) from the receiver (Earth station) and the signal quality that makes up that specific link. Consider a local radio station that has a radiating power of 50 kilowatts. At 70 miles distance from the radio station's transmitter, a runner wearing AM/FM receiver headphones

can easily pick up that station's broadcast using a simple antenna on the headphones. A satellite in geosynchronous orbit possesses nowhere near thousands of kilowatts of power to transmit, yet that satellite's signal must travel thousands of miles using no more than from 20 to 50 watts of radiated power. How is this possible?

**M-297.** Part of the answer lies in the fact that microwave frequencies are used and the signal power of the satellite is concentrated into a narrow, directed beam. The energy of the beam is focused by the shape of the antenna and transmitted in one direction—instead of broadcasting in all directions—to a receiving Earth antenna. However, when these signals reach the Earth, they are very weak. Reflectors, low-noise amplifiers, and sophisticated receivers that are part of the antenna suite can restore the signal to a useful level, at which it can be detected and processed.

**M-298.** The signal transmitted from a ground terminal antenna up to a satellite is called an uplink, and the transmission from a satellite to a ground terminal antenna is called a downlink. The frequencies of the uplink and downlink are always different from each other. The uplink frequency is normally a higher frequency than the downlink. The reason for this is that it is easier to generate radio frequency power on the ground than it is aboard the satellite, where weight and power are limited. A large dish reflector antenna on the ground, using the higher frequency and shorter wavelength for the uplink maximizes the signal power transmitted to the satellite. The signal will be received by a much smaller antenna that is more efficient for receiving the shorter wavelength signals. This is important because the satellite's communications suite, being much smaller and much less powerful in comparison to the ground terminal, will be more disadvantaged in its ability to strongly receive and transmit signals. The larger ground antenna will have the advantage of more effectively collecting the weaker, lower frequency downlink signals transmitted by the satellite.

**M-299.** Trade-offs in ground terminal antenna technology can affect the power of the satellite. Antennas on board a satellite have two basic purposes. One is to receive and transmit communications signals to support users on the ground. The other is to communicate telemetry, tracking, and control signals that ground control systems and their operators use to ensure the satellites are properly maintained in orbit. Antennas on board the satellite use the majority of the available on board power to transmit and receive signals to and from Earth. Satellites have communications equipment that performs essentially the same functions as the ground station's receiving, processing, and transmitting equipment. The antennas on the satellites used for communications services are the largest and most complex, while the telemetry, tracking, and control antennas are usually horn-shaped and smaller. A satellite antenna can be designed and shaped to focus and concentrate a signal into a desired geographical area (its footprint).

### Satellite Coverage Areas and Footprints

**M-300.** Coverage refers to that portion of the Earth's surface where SATCOM services are provided from the set of communications antennas on board a satellite.

**M-301.** Global coverage is defined as the coverage of all longitudes and latitudes and geographic regions. There are five primary overlapping geographical regions to which common reference is made regarding Army SATCOM. These regions are called the continental United States, Atlantic, Indian Ocean, Pacific, and North Polar regions. A sixth region, the South Polar Region has not had any Army SATCOM requirements to date but it may receive increased emphasis as new requirements emerge for that part of the world.

**M-302.** Worldwide coverage encompasses the first four mid-latitude regions and is defined as the surface of the Earth between 65 degrees south latitude and 65 degrees north latitude and at all longitudes. The North Polar region is defined as the area above 65 degrees north latitude and at all longitudes. The South Polar region is the area south of 65 degrees latitude.

*Note.* A minimum practical elevation angle for an Earth station antenna is five degrees. So, for communication with a geosynchronous satellite, the maximum practical latitude, either north or south, for an Earth station would be about 76 degrees.

**M-303.** The area of coverage on the Earth's surface that is effectively irradiated by a satellite's antenna is called its footprint. This footprint is also the Earth coverage area from which a satellite's antenna can effectively collect signals transmitted to it. Theoretically, like the beam from a flashlight, a footprint should be circular. However, the Earth's terrain is uneven, the thickness of the atmosphere changes, and different satellite antennas may have differently shaped beam patterns. The footprint, in reality, usually has an irregularly shaped beam pattern with signal intensity strongest in the central parts of the projected ground coverage pattern. Signal intensity tapers off towards the edges of the pattern.



**M-304.** Signals transmitted from a satellite can be unevenly distributed. It is impractical to build a satellite whose antenna coverage area is large and whose signal strength is entirely uniform across the footprint. The cost would be enormous. Instead, it is more practical to build ground terminals with larger dish antennas that enable them to catch more of the signal from the satellite the farther away the ground terminals may be from the center of the satellite's footprint.

**M-305.** Special antennas on board the satellite can project spot beams that more efficiently direct concentrated signals to specific locations. For instance, spot beams may be pointed to cover both Hawaii and Puerto Rico, so that power is not wasted covering the oceans that separate these islands from the mainland. Some satellites use motor-driven antennas that can steer spot beams towards specific areas on the Earth upon demand. Steerable beam antennas, which can shift a satellite's coverage area, are particularly suitable for supporting the Soldier since changing missions demand flexibility in SATCOM coverage. Milstar satellites have this capability.

## Defense Satellite Communications System

**M-306.** The DSCS is considered the backbone of the U.S. military's global satellite communications capability and is the primary transmissions path for much of the DOD's highest priority communications. The DSCS system consists of five primary satellites in geosynchronous orbit, ground control stations, and user terminals. Providing worldwide strategic, operational, and tactical communications, DSCS satellites generate large earth coverage footprints that are linked to large, fixed strategic ground terminals. Those large ground terminals are then linked into the Defense Information Systems Network (DISN). This earth coverage supports fixed and mobile users with communications capabilities.

**M-307.** DSCS spot beams focus in on a very narrow portion of the Earth's surface and can provide range extension for tactical users who may be deployed in areas not served by large strategic terminals. DSCS connects to ground mobile forces vehicle-mounted tactical terminals, which are TRI-TAC based at echelons above corps or other tactical terminals at echelons corps and below. The GMF terminals provide commonality among the Army, Air Force, and Marine Corps. On an extended battlefield, MSE mobile subscriber radio terminals provide on-the-move communications through the MSE-to-GMF terminal links. Equipment at specially configured fixed strategic terminals called standardized tactical entry points (STEPs) provides an interface between the GMF tactical terminals and the worldwide DISN. Under normal operating conditions, DSCS provides substantial worldwide capacity for high quality voice circuits and wideband data circuits.

### Global Broadcast Service

**M-308.** GBS provides worldwide, high capacity, one-way transmission of video, imagery and other information supporting deployed forces in transit and in an area of operation. It employs readily available, satellite-based broadcast commercial technologies that are relatively inexpensive and easily

integrated into existing systems and processes, yet not so unwieldy as to be unusable by smaller and more mobile units. (See figure M-39.)

**Relationship Between Global Broadcast Service and Integrated Broadcast Service**

**M-309.** The difference between GBS and Integrated Broadcast Service (IBS) is that GBS is designed to disseminate large data files, such as imagery, video, and data. Bandwidth for GBS is not an issue. IBS cannot disseminate large data files due to bandwidth constraints; it only disseminates data in the form of messages—such as United States message text format (USMTF) and common message format (CMF). In the future, IBS will disseminate data in CMF. IBS data can be disseminated using GBS, but GBS data will never be disseminated using IBS. This is the primary difference between the two:

- GBS—
  - Uses commercial direct broadcast satellite technology.
  - Is a space-based, high-data-rate communications link for simplex flow.
  - Only distributes information.
  - Uses push technology.
  - Has no interaction from producer to producer.
- IBS—
  - Disseminates timely intelligence using narrow-band text.
  - Permits producer to producer interaction.
  - Uses a CMF.
  - Uses common track/report/event numbers.
  - Complies with DOD, Joint Chiefs of Staff, and Congressional mandates, and adheres to national policy including provision of data on broadcast to second party partners.

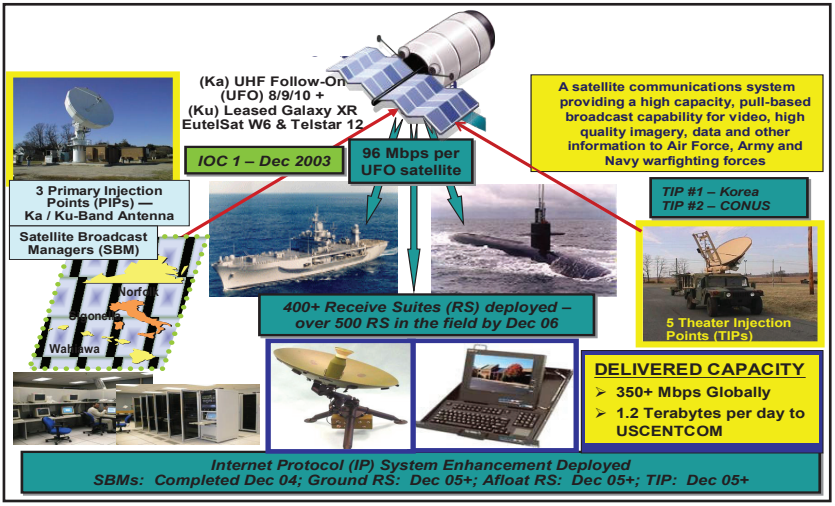



**Figure M-39. Global broadcast service**


FOR OFFICIAL USE ONLY

# Appendix N

# Non-U.S. Small Arms and Light Weapons Effects in the Urban Environment

## INTRODUCTION

**N-1.** The U.S Army Materiel Systems Analysis Activity (USAMSAA) provided the data in this appendix to use as a reference for planning and training. The charts were compiled to assess a variety of threat (non-U.S.) weapons against many structures or materials found in an urban environment. This assessment was based on a review of limited test data, comparisons to U.S. weapons data against urban structures and materials, subject matter expertise, and professional military judgment. The USAMSAA also provided the acronym list and note at the end of this appendix that pertain to these tables.

## Table N-1. Rifles, machine, and submachine guns

| Target and Thickness | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Model # | Round/Bullet | Reinforced Concrete | Triple Brick Wall | Brick over Block | CMU Filled | Double Brick | Double Sandbag Wall | Log Wall | Mild Steel Door |
| | | 8” | 14” | 12” | 12” | 9.5” | 24” | 16” | 3/8” |
| AK-74 RPK74 | 5.45x39mm Ball | ◐ | ○ | ○ | ◐ | ○ | ○ | ● | ● |
| | Armor Piercing (AP) | ◐ | ○ | ○ | ◐ | ○ | ○ | ● | ● |
| AK-74 | 7.62x39mm Ball | ◐ | ○ | ○ | ◐ | ○ | ○ | ● | ● |
| | AP | ◐ | ○ | ○ | ◐ | ○ | ○ | ● | ● |
| RPD/RPK | 7.62x39mm Ball | ● | ◐ | ◐ | ● | ◐ | ○ | ● | ● |
| | AP | ● | ◐ | ◐ | ● | ◐ | ○ | ● | ● |
| SKS | 7.62x39mm Ball | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● |
| | AP | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● |
| DRAGUNOV SVD | 7.62x54mm R Ball | ○ | ○ | ○ | ○ | ◐ | ○ | ● | ● |
| | Heavy Ball (LPS) | ○ | ○ | ○ | ○ | ◐ | ○ | ● | ● |
| | AP | ○ | ○ | ○ | ○ | ◐ | ○ | ● | ● |
| PKM MG SVD | 7.62x54mmR Ball | ● | ● | ● | ● | ● | ◐ | ● | ● |
| | Heavy Ball (LPS) | ● | ● | ● | ● | ● | ◐ | ● | ● |
| | AP | ● | ● | ● | ● | ● | ◐ | ● | ● |
| NSV/NSB-T | 12.7x108mm Ball (B-32) | ● | ● | ● | ● | ● | ● | ● | ● |
| | API | ● | ● | ● | ● | ● | ● | ● | ● |
| DshK | 127x108mm Ball (B-32) | ● | ● | ● | ● | ● | ● | ● | ● |
| | API | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◐ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier’s vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.

– No Munitions will clear re-bar.

– Worst case scenario = Perpendicular contact with CMU.



FOR OFFICIAL USE ONLY

## Table N-2. Grenade launchers

| Model # | Round | Target and Thickness: Reinforced Concrete | Triple Black Wall | Concrete Block w/ Single Brick Veneer | Cinder Block (Filled) | Double Brick Wall | Double Sandbag Wall | Log Wall | Mild Steel Door |
|---|---|---|---|---|---|---|---|---|---|
| | | 8" | 14" | 12" | 12" | 9" | 24" | 16" | 3/8" |
| AGS-17 | 30-mm FRAG-HE Grenade | ○ | ◐ | ○ | ◐ | ◐ | ○ | ◐ | ● |
| W-87 (Chinese) | 35-mm FRAG-HE Grenade | ○ | ◐ | ○ | ◐ | ◐ | ◐ | ◐ | ● |
| | HEAT Grenade | ◐ | ◐ | ● | ● | ● | ● | ● | ● |
| GP-30 | 40-mm FRAG-HE (Impact) Grenade | ○ | ◐ | ○ | ◐ | ◐ | ◐ | ◐ | ● |
| | FRAG-HE (Bounding) Grenade | ○ | ◐ | ○ | ◐ | ◐ | ◐ | ◐ | ● |
| | Smoke Grenade | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| RPO (A/Z) | Napalm Projectile | ● | ● | ● | ● | ● | ● | ● | ● |
| | Thermobaric-flammable Mixture Projectile | ● | ● | ● | ● | ● | ● | ● | ● |
| | Incendiary | ● | ● | ● | ● | ● | ● | ● | ● |
| SPG-9M Recoilless Gun | 73-mm RA HEAT | ● | ● | ● | ● | ● | ● | ● | ● |
| | RA HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | FRAG-HE (Bounding) Grenade | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◐ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.



FOR OFFICIAL USE ONLY

## Table N-3. Antitank guided missiles

| Model # | Round | Target and Thickness: Reinforced Concrete | Triple Brick Wall | Concrete Block w/ Single Brick Veneer | Cinder Block (Filled) | Double Brick Wall | Double Sandbag Wall | Log Wall | Mild Steel Door |
|---|---|---|---|---|---|---|---|---|---|
| | | 8" | 14" | 12" | 12" | 9" | 24" | 16" | 3/8" |
| AT-3 | ATGM (Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | Malyutka (tandem shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-4/AT-5 | ATGM (Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | Tandem Shaped charge HEAT | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-7 | ATGM (Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-10 | ATGM | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-11 | ATGM (Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | Tandem Shaped charge Heat | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-13 | ATGM (Tanderm Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | HE Thermobaric (Metis-M) | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-14 KORNEL | ATGM (Tandem Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | HE Thermobaric | ● | ● | ● | ● | ● | ● | ● | ● |
| HOT/HOT2/ HOT3 | ATGM (Shaped charge HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| | Tandem shaped charge Heat | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◐ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.



FOR OFFICIAL USE ONLY

## Table N-4. Antitank grenade launchers (RPGs)

| Model # | Round | Target and Thickness: Reinforced Concrete | Triple Brick Wall | Concrete Block w/ Single Brick Veneer | Cinder Block (Filled) | Double Brick Wall | Double Sandbag Wall | Log Wall | Mild Steel Door |
|---|---|---|---|---|---|---|---|---|---|
| | | 8" | 14" | 12" | 12" | 9" | 24" | 16" | 3/8" |
| RPG-7V | 40-mm PG-7V Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | PG-7VM Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | PG-7VS Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | PG-7VL Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | PG-7VR Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | TBG-7V Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | OG-7V Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| | OG-7VM Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| RPG-22 | 72-mm HEAT Grenade | ● | ● | ● | ● | ● | ● | ● | ● |
| RPG-29 | 105-mm HEAT (Tandem) Grenade | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◔ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.

- No Munitions will clear re-bar before penetration occurs
- Will create loophole (8 inch in diameter)



FOR OFFICIAL USE ONLY

## Table N-5. Artillery

| Model # | Round | Target and Thickness: Reinforced Concrete | Triple Brick Wall | Concrete Block w/ Single Brick Veneer | Cinder Block (Filled) | Double Brick Wall | Double Sandbag Wall | Log Wall | Mild Steel Door |
|---|---|---|---|---|---|---|---|---|---|
| | | 8" | 14" | 12" | 12" | 9" | 24" | 16" | 3/8" |
| ZIS-3 (Towed AT Gun) | 76-mm HVAP-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEAT | ● | ● | ● | ● | ● | ● | ● | ● |
| | APC-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | FRAG-HE | ● | ● | ● | ● | ● | ● | ● | ● |
| D-44 (Towed AT Gun) | 85-mm HVAP-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEAT-FS | ● | ● | ● | ● | ● | ● | ● | ● |
| | AT-HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | FRAG-HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | Smoke | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| MT-12 (Towed AT Gun) | 100-mm APFSDS-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEAT | ● | ● | ● | ● | ● | ● | ● | ● |
| | FRAG-HE | ● | ● | ● | ● | ● | ● | ● | ● |
| 2A45M (Towed AT Gun) | 123-mm APFSDS-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEAT | ● | ● | ● | ● | ● | ● | ● | ● |
| | Frag-HE | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

● A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.



FOR OFFICIAL USE ONLY

## Table N-6. Antiaircraft

| Model # | Round/Bullet | Target and Thickness: Reinforced Concrete | Triple Brick Wall | Concrete Block w/ Single Brick Veneer | Cinder Block (Filled) | Double Brick Wall | Double Sandbag Wall | Log Wall | Mild Steel Door |
|---|---|---|---|---|---|---|---|---|---|
| | | 8" | 14" | 12" | 12" | 9" | 24" | 16" | 3/8" |
| S-60 (Towed AA) | 57-mm FRAG-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | APT | ● | ● | ● | ● | ● | ● | ● | ● |
| ZPU-4 | 14.5-mm AP-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | API | ● | ● | ● | ● | ● | ● | ● | ● |
| | API-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEI | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEI-T | ● | ● | ● | ● | ● | ● | ● | ● |
| ZU-23 | 23-mm HE-I | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEI-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | API-T | ● | ● | ● | ● | ● | ● | ● | ● |
| | TP | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◔ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.



FOR OFFICIAL USE ONLY

## Table N-7. Weapons systems on helicopters

| Model # | Round/Bullet | Target and Thickness: Reinforced Concrete 8" | Triple Brick Wall 14" | Concrete Block w/Single Brick Veneer 12" | Cinder Block (Filled) 12" | Double Brick Wall 9" | Double Sandbag Wall 24" | Log Wall 16" | Mild Steel Door 3/8" |
|---|---|---|---|---|---|---|---|---|---|
| AT-2C | ATGM | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-6C | ATGM (Tandem HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-9 | ATGM (Tandem HEAT) | ● | ● | ● | ● | ● | ● | ● | ● |
| AT-16/VIKhR | ATGM | ● | ● | ● | ● | ● | ● | ● | ● |
| 12.7-mm gun/ YaKb-12.7 | HEFI | ○ | ◐ | ◐ | ◐ | ◐ | ○ | ● | ● |
| | APT | ○ | ◐ | ◐ | ◐ | ◐ | ○ | ● | ● |
| | Duplex | ○ | ◐ | ◐ | ◐ | ◐ | ○ | ● | ● |
| | Duplex T | ○ | ◐ | ◐ | ◐ | ◐ | ○ | ● | ● |
| GSh-23L/ 23-mm Gun Pods | HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | AP | ● | ● | ● | ● | ● | ● | ● | ● |
| GSh-30L/ 30-mm Gun Pods | HEFI | ● | ● | ● | ● | ● | ● | ● | ● |
| | HEI | ● | ● | ● | ● | ● | ● | ● | ● |
| | APT | ● | ● | ● | ● | ● | ● | ● | ● |
| | APE | ● | ● | ● | ● | ● | ● | ● | ● |
| | CC | ● | ● | ● | ● | ● | ● | ● | ● |
| 2A42/30-mm Auto Cannon | HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | AP | ● | ● | ● | ● | ● | ● | ● | ● |
| 57-mm S-5 Rocket Pods | HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | AP | ● | ● | ● | ● | ● | ● | ● | ● |
| 80-mm S-8 Rocket Pods | HE | ● | ● | ● | ● | ● | ● | ● | ● |
| | AP | ● | ● | ● | ● | ● | ● | ● | ● |

*Legend*

○ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier without need to seek greater ballistic protection.

◐ A combatant can fight, using applicable tactics, techniques, and procedures, from a position protected by this barrier for a limited time due to the barrier's vulnerability to projectile penetration.

● A combatant would select this barrier as a last resort for protection.

The CC round listed for the GSh-30L/30-mm gun pods is a cargo-carrier round. It contains small pellets (about 3.5g each) that are dispersed from a projectile by a fuze. The energy of each of these pellets is similar to that of a 5.56-mm bullet. The pellets alone are probably capable of perforating the steel door listed in the charts and could chew up sandbag walls.



FOR OFFICIAL USE ONLY

**Table N-8. Acronyms used in the tables**

| | |
|---|---|
| **AP** | Armor Piercing |
| **APE** | Armor Piercing Explosive |
| **APFSDS-T** | Armor Piercing, Fin Stabilized, Discarding Sabot-Tracer |
| **API** | Armor Piercing Incendiary |
| **API-T** | Armor Piercing Incendiary-Tracer |
| **ATGM** | Antitank Guided Missile |
| **AT-HE** | Antitank-High Explosive |
| **CC** | Cargo Carrier |
| **CMU** | Concrete Modular Unit |
| **Duplex T** | Duplex Tracer |
| **FRAG** | Fragmentation |
| **FRAG-HE** | Fragmentation-High Explosive |
| **HE** | High Explosive |
| **HEFI** | High Explosive Fragmentation Incendiary |
| **HEI** | High Explosive Incendiary |
| **HEI-T** | High Explosive Incendiary-Tracer |
| **HEAT** | High Explosive Anti Tank |
| **HEAT-FS** | High Explosive Anti Tank-Fin Stabilized |
| **HVAP-T** | Hypervelocity Armor Piercing-Tracer |
| **Incendiary-T** | Incendiary-Tracer |
| **RA** | Reactive Armor |
| **RPG** | Rocket Propelled Grenade |
| **TP** | Target Practice |

***Note.*** The CMU used in the worst case scenario is a cinderblock filled with concrete and reinforced with one-half inch rebar placed at 8- to 10-inch intervals. The limited test data that is available is primarily focused on perpendicular engagements. Engagements at reasonable oblique angles (less than 45 degrees) would have the biggest impact on small arms, probably some limited impact on medium caliber AP rounds, and no impact on large caliber rounds, missiles, or RPGs.

# Glossary

## SECTION I – ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **10 USC** | Title 10, United States Code |
| **32 USC** | Title 32, United States Code |
| **2X** | human intelligence and counterintelligence staff element |
| **AFDD** | Air Force doctrine document |
| **AO** | area of operations |
| **AOC** | area of concentration |
| **AR** | Army regulation |
| **ARFORGEN** | Army force generation |
| **ARFOR** | Army forces |
| **ARNG** | Army National Guard |
| **ARNGUS** | Army National Guard of the United States |
| **ASCOPE** | areas, structures, capabilities, organizations, people, events (civil considerations) |
| **ATCAE** | Army Technical Control and Analysis Element |
| **BCT** | brigade combat team |
| **BDA** | battle damage assessment |
| **BFSB** | battlefield surveillance brigade |
| **CA** | civil affairs |
| **CBRNE** | chemical, biological, radiological, nuclear, and high-yield explosives |
| **CCIR** | commander's critical information requirement |
| **CI** | counterintelligence |
| **CIA** | Central Intelligence Agency |
| **CICA** | counterintelligence coordinating authority |
| **CIED** | counter-improvised explosive device |
| **CGS** | Common Ground Station |
| **CJCS** | Chairman of the Joint Chiefs of Staff |
| **COA** | course of action |
| **COMINT** | communications intelligence |
| **CONUS** | continental United States |
| **CONPLAN** | concept plan, operation plan in concept format |
| **CONPLAN** | contingency plan |
| **COP** | common operational picture |

| | |
|---|---|
| **CSS** | Central Security Service |
| **CTL** | critical task list |
| **CTSSB** | Critical Task Site Selection Board |
| **CyD** | cyber defense |
| **DA PAM** | Department of the Army pamphlet |
| **DCGS-A** | Distributed Common Ground System-Army |
| **DCID** | Director of Central Intelligence directive |
| **DCS** | deputy chief of staff |
| **DCyD** | dynamic cyber defense |
| **DEA** | Drug Enforcement Administration |
| **DHE-M** | Defense HUMINT Enterprise-manual |
| **DHS** | Department of Homeland Security |
| **DIA** | Defense Intelligence Agency |
| **DIAM** | Defense Intelligence Agency manual |
| **DNA** | deoxyribonucleic acid |
| **DNI** | Director of National Intelligence |
| **DOD** | Department of Defense |
| **DODD** | Department of Defense directive |
| **DOJ** | Department of Justice |
| **DOMEX** | document and media exploitation |
| **DOS** | Department of State |
| **DP** | decisive point, decision point |
| **DST** | decision support template |
| **DTT** | doctrine and tactics training |
| **EEFI** | essential element of friendly information |
| **ELINT** | electronic intelligence |
| **e-mail** | electronic mail |
| **EO** | executive order |
| **EPW** | enemy prisoner of war |
| **ES** | electronic warfare support |
| **EW** | electronic warfare |
| **FBI** | Federal Bureau of Investigation |
| **FEMA** | Federal Emergency Management Agency |
| **FFIR** | friendly force information requirement |

| | |
|---|---|
| **FISINT** | foreign instrumentation signals intelligence |
| **FISS** | f oreign intelligence and security services |
| **FM** | field manual |
| **FM** | frequency modulation |
| **FMA** | foreign materiel acquisition |
| **FME** | foreign material exploitation |
| **FMI** | field manual interim |
| **FSO** | full spectrum operations |
| **FSO-METL** | full spectrum operations-mission essential task lists |
| **GEOINT** | geospatial intelligence |
| **GIG** | Global Information Grid |
| **GMI** | general military intelligence |
| **GPC** | geospatial planning cell |
| **GSA** | general services administration |
| **HCT** | human intelligence collection team |
| **HPT** | high-payoff target |
| **HUMINT** | human intelligence |
| **HVI** | high-value individual |
| **HVT** | high-value target |
| **HVTL** | high-value target list |
| **I&W** | Indications and warning |
| **IC** | intelligence community |
| **IED** | improvised explosive device |
| **IGO** | intergovernmental organization |
| **IMINT** | imagery intelligence |
| **INFOSEC** | information security |
| **INSCOM** | United States Army Intelligence and Security Command |
| **INTSUM** | intelligence summary |
| **IPB** | intelligence preparation of the battlefield |
| **ISR** | Intelligence, surveillance, and reconnaissance |
| **ITO** | international terrorist organizations |
| **IWF** | Intelligence warfighting function |
| **ITO** | international terrorist organizations |
| **IWF** | intelligence warfighting function |

| | |
|---|---|
| **J-2** | intelligence directorate of a joint staff |
| **JIIM** | joint-interagency-intergovernmental-multinational |
| **JP** | joint publication |
| **MCCEP** | Military Cryptologic Continuing Education Program |
| **MCOO** | modified combined obstacle overlay |
| **MDMP** | Military decisionmaking process |
| **METL** | mission-essential task list |
| **METT-TC** | Mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables) |
| **MI** | military intelligence |
| **MIHB** | military intelligence handbook |
| **MIRC** | Military Intelligence Readiness Command |
| **MOS** | military occupational specialty |
| **MOS-T** | military occupational skills-transfer |
| **MP** | military police |
| **MSO** | military source operations |
| **NAI** | named area of interest |
| **NGA** | National Geospatial-Intelligence Agency |
| **NGIC** | National Ground Intelligence Center |
| **NGO** | nongovernmental organization |
| **NIST** | national intelligence support team |
| **NRO** | National Reconnaissance Office |
| **NSA** | National Security Agency |
| **OAKOC** | observation and fields of fire, avenues of approach, kep terrain, obstacles, cover and concealment. |
| **OPLAN** | operation plan |
| **OPORD** | operation order |
| **OPSEC** | operations security |
| **OSINT** | open-source intelligence |
| **PIR** | priority intelligence requirement |
| **PMESII** | political, military, economic, social, information, infrastructure |
| **PMESII-PT** | political, military, economic, social, information, infrastructure, physical environment, time (operational variables) |
| **POC** | point of contact |

| | |
|---|---|
| **PSYOP** | Psychological operations |
| **PUM** | proper use memorandum |
| **RFI** | request for information |
| **ROE** | rules of engagement |
| **S&TI** | scientific and technical intelligence |
| **S-2** | intelligence staff officer |
| **S-3** | operations staff officer |
| **SCI** | sensitive compartmented information |
| **SIDS** | secondary image dissemination system |
| **SIGINT** | signals intelligence |
| **SIPRNET** | SECRET Internet Protocol Router Network |
| **SIR** | specific information requirement |
| **S//NF** | secret//not releasable to foreign nationals |
| **SOF** | special operations forces |
| **SOP** | standing operating procedure |
| **TAI** | targeted area of interest |
| **TC** | training circular |
| **TCAE** | technical control and analysis element |
| **TECHELINT** | technical electronic intelligence |
| **TECHINT** | technical intelligence |
| **TENCAP** | Tactical Exploitation of National Capabilities Program |
| **TRADOC** | training and doctrine command |
| **TSCM** | technical surveillance countermeasures |
| **TTP** | tactics, techniques, and procedures |
| **UAS** | unmanned aircraft system |
| **UGS** | unattended ground sensor |
| **U. S.** | United States |
| **USAICoE** | U.S. Army Intelligence Center of Excellence |
| **USAR** | United States Army Reserve |
| **USC** | United States Code |
| **WMD** | weapons of mass destruction |

## SECTION II – TERMS

**all-source intelligence**

(Army) The intelligence discipline concerned with all-source products and the processes used to produce them. (joint) 1. Intelligence products and/or organizations and activities that incorporate all

sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (JP 2-0) The intelligence discipline responsible for all-source products and the processes used to produce them. All-source intelligence also refers to intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence (JP 2-0). All-source intelligence is the products, organizations, and activities that incorporate all sources of information and intelligence, including OSINT, in the production of intelligence. All-source intelligence is both a separate intelligence discipline and the name of the process used to produce intelligence from multiple intelligence or information sources (FM 2-0).

**analysis**

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 2-0).

**counterintelligence**

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities (Executive Order 12333 [EO 12333]). CI counters or neutralizes foreign intelligence and security services (FISS) and international terrorist organizations (ITO) intelligence collection efforts. It does this 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 the protection of U.S. interests and equities. CI helps identify EEFIs by identifying vulnerabilities to threat collection and actions taken to counter collection and operations against U.S. forces (EO 12333).

**general military intelligence**

Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or multinational military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilia communications systems; military economics, including foreign military assistance; insurgency and terrorism; military political-sociological intelligence; location, identification, and description of militaryrelated installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) (JP 2-0).

**geospatial intelligence**

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

**human intelligence**

The collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities (FM 2-0).

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

**improvised explosive device**
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores,but is normally devised from nonmilitary components. Also called IED. (JP 3-07.2).

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

**intelligence reach**
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 within and outside the area of operations, unconstrained by geographic proximity, echelon, or command (FM 2-0).

**intelligence requirement**
A type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations. (FM 2-0).

**measurement and signature intelligence**
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 reflected or emitted (JP 2-0).

**open-source intelligence**
The discipline that pertains to intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (FM 2-0).

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

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

# References

## REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.
FM 1-02 (101-5-1). *Operational Terms and Graphics*. 21 September 2004.
FM 2-0. *Intelligence*. 23 March 2010.
FM 3-0. *Operations*. 27 February 2008.
FM 4-0. *Sustainment*. 30 April 2009.
JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001.
JP 2-0. *Joint Intelligence*. 22 June 2007.
JP 3-0. *Joint Operations*. 17 September 2006.
JP 4-0. *Joint Logistics*. 18 July 2008.
JP 5-0. *Joint Operations Planning*. 26 December 2006.

## RELATED PUBLICATIONS

These sources contain relevant supplemental information.
AFDD 2-9. *Intelligence, Surveillance, and Reconnaissance Operations*. 17 July 2007.
AR 27-60. *Intellectual Property*. 1 June 1993.
AR 190-13. *The Army Physical Security Program*. 30 September 1993.
AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.
AR 380-13. *Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations*. 13 September 1974.
AR 380-67. *The Department of the Army Personnel Security Program*. 9 September 1988.
AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.
AR 381-172. (U) *Counterintelligence Force Protection Operations (CFSO) and Low Level Source Operations (LLSO) (S//NOFORN)*. 30 December 1994.
AR 530-1. *Operations Security*. 19 April 2007.
AR 614-115. (U) *Military Intelligence Officer Excepted Career Program (Great Skill) (S//NOFORN)*. 30 April 2010.
ARFORGEN Process. Available online at http://www.army.mil/aps/09/information_papers/army_force_generation_process.html.
CGS DTT. November 2000.
CJCS Memorandum. 19 August 2009.
DA PAM 600.3. *Commissioned Officer Professional Development and Career Management*. 1 February 2010.
DCID 6/9. *Physical Security Standards for Sensitive Compartmented Information Facilities*. 18 November 2002.
DHE-M 3301.001. (U) *Defense Intelligence Agency (DIA) Human Intelligence (HUMINT) Manual, Vol I: Collection Requirements, Reporting, and Evaluation Procedures (S)*. 22 January 2009.
DIAM 58-11. (U) *Department of Defense (DOD) Human Intelligence (HUMINT) Policies and Procedures (S//NF)*. 5 September 2002.
DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Component That Affect United States Persons*. 1 December 1982.
DODD 2310.1E. *The Department of Defense Detainee Program*. 5 September 2006.
DODD 3115.09. *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*. 9 October 2008.
DODD 5100.20. *National Security Agency and the Central Security Service (NSA/CSS)*. 26 January 2010.
DODD 5105.21. *Defense Intelligence Agency (DIA)*. 18 March 2008.

DODD 5105.23. *National Reconnaissance Office (NRO)*. 27 March 1964.
DODD 5105.60. *National Geospatial-Intelligence Agency (NGA)*. 29 July 2009.
DODD 8521.01E. *Department of Defense Biometrics.* 21 February 2008.
EO 12333. *United States Intelligence Activities*. 4 December 1981.
FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009.
FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.
FM 2-22.2 (34-60). *Counterintelligence*. 21 October 2009.
FM 2-22.3 (34-52). *Human Intelligence Collector Operations*. 6 September 2006.
FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*. 10 October 2007.
FM 3-05.40. *Civil Affairs Operations*. 29 September 2006.
FM 3-06. *Urban Operations*. 26 October 2006.
FM 3-06.11. *Combined Arms Operations in Urban Terrain*. 28 February 2002.
FM 3-09.60. *Multiple Launch Rocket System (MLRS) Operations*. 12 August 2008.
FM 3-13. *Information Operations: Doctrine, Tactics, Techniques, and Procedures*. 28 November 2003.
FM 3-34.170. *Engineer Reconnaissance*. 25 March 2008.
FM 3-35. *Army Deployment and Redeployment*. 21 April 2010.
FM 3-36. *Electronic Warfare in Operations*. 25 February 2009.
FM 3-90. *Tactics*. 4 July 2001.
FM 3-90.15. *Sensitive Site Operations*. 25 April 2007.
FM 5-0. *The Operations Process*. 26 March 2010.
FM 6-0. *Mission Command: Command and Control of Army Forces*. 11 August 2003.
FM 6-02.43. *Signal Soldier's Guide*. 17 March 2009.
FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process*. 8 May 1996.
FM 6-99.2. *U.S. Army Report and Message Formats*. 30 April 2007.
FM 7-0. *Training for Full Spectrum Operations*. 12 December 2008.
FM 7-15. *The Army Universal Task List*. 27 February 2009.
FM 34-81. *Weather Support for Army Tactical Operations*. 31 August 1989.
FMI 2-01. *Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization*. 11 November 2008.
FMI 2-01.301 (34-130). *Specific Tactics, Techniques, and Procedures and Applications for Intelligence Preparation of the Battlefield*. 31 March 2009.
FMI 2-22.9. *Open Source Intelligence*. 5 December 2006.
JP 1. *Doctrine for the Armed Forces of the United States*. 14 May 2007.
JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004.
JP 2-01.2. (U) *Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations (S)*. 5 April 1994.
JP 2-03. *Geospatial Intelligence Support to Joint Operations*. 22 March 2007.
JP 3-03. *Joint Interdiction Operations*. 22 March 2007.
JP 3-09. *Joint Fire Support*. 13 November 2006.
JP 3-13.1. *Electronic Warfare*. 25 January 2007.
JP 3-13.3. *Operations Security*. 29 June 2006.
JP 3-16. *Multinational Operations*. 7 March 2007.
JP 3-28. *Civil Support*. 14 September 2007.
JP 3-35. *Deployment and Redeployment Operations*. 7 May 2007.
JP 3-59. *Meteorological and Oceanic Operations*. 24 September 2008.
JP 3-60. *Joint Targeting*. 13 April 2007.
JP 6-0. *Joint Communications System*. 20 March 2006.
MIHB 2-50. *Intelligence Systems*. 22 July 2008.
Modular Force Conversion. Available online at http://www.army.mil/aps/09/information_papers/modular_force_conversion.html.

National Security Act of 1947. Available online at http://www.state.gov/www/about_state/history/intel/intro6.html.
TC 2-22.4. *Technical Intelligence*. 19 November 2009.
TC 2-22.303. *The 2X Handbook*. 31 July 2006.
TC 2-22.601. *Army Radio-Controlled Improvised Explosive Device Electronic Warfare (CREW)*. 9 April 2008.
TC 2-33.4 (FM 34-3). *Intelligence Analysis*. 1 July 2009.
TC 2-50.5. *Intelligence Officer's Handbook*. 6 January 2010.
Quadrennial Defense Review Report 2010. Available online at http://www.defense.gov/qdr/.
10 USC. *Armed Forces*. Available online at http://www.gpoaccess.gov/uscode/browse.html.
32 USC. *National Guard*. Available online at http://www.gpoaccess.gov/uscode/browse.html.

## PRESCRIBED FORMS

None.

## REFERENCED FORMS

None.

# Index

**Entries are by paragraph number unless otherwise specified**



## A







FOR OFFICIAL USE ONLY

## B



## C

## C (continued)



## D



## E

## E (continued)



## F



## G



## H



## I

## I (continued)



## J

## L



## M



## N

## O



## P



## Q



## R



## S

## S (continued)



## T

## U



## V



## W



## Z