*FM 2-19.4

Brigade Combat Team Intelligence Operations

25 NOVEMBER 2008

Headquarters Department of the Army

This publication is available at
Army Knowledge Online (www.us.army.mil) and
General Dennis J. Reimer Training and Doctrine
Digital Library at (www.train.army.mil).

*Field Manual
No. 2-19.4

Headquarters
Department of the Army
Washington, DC 25 November 2008

Brigade Combat Team Intelligence Operations

Contents

***This publication supersedes FM 34-80, dated 15 April 1986.**

Figures

Tables

Preface

This manual provides developmental doctrine for the Brigade Combat Team (BCT) and Stryker Brigade Combat Teams (SBCTs) intelligence operations. It describes the brigade intelligence fundamentals, roles, and responsibilities of the intelligence staff, and the operations of the Military Intelligence (MI) company. This manual—

- Establishes the doctrinal foundation for BCT and SBCT intelligence operations.
- Addresses requirements expanding on doctrine in FM 2-0, FM 3-0, FM 5-0, FMI 5-0.1, FM 6-0, and FM 34-130. Incorporates intelligence and operational doctrine and terminology from FM 3-90.6, and FM 3-20.96.
- Provides a basic framework for intelligence professionals on the evolving doctrine, tactics, techniques, and procedures (TTP), material and force structure, institutional and unit training, and standing operating procedures (SOPs) for BCT echelon intelligence support and intelligence, surveillance, and reconnaissance (ISR) operations.
- Introduces the new six step intelligence process, a detailed explanation will be incorporated into the new FM 2-0.
- Is divided into three parts:
  - Part One – Brigade Intelligence Fundamentals.
  - Part Two – Intelligence Processing.
  - Part Three – Intelligence Organizations.
- Provides additional information in the appendices:
  - Appendix A – BCT Intelligence Readiness Training.
  - Appendix B – Reports.
  - Appendix C – Captured Enemy Documents, Media, and Equipment.
  - Appendix D – Intelligence Oversight.
  - Appendix E – Operational Environment.
  - Appendix F – Force Projection.
  - Appendix G – DCGS-A Overview.

This manual is designed primarily for the intelligence staffs and Soldiers in transforming heavy brigade combat teams (HBCTs), infantry brigade combat teams (IBCTs), SBCT, and subordinate units. It can also be used by commanders, staffs, and intelligence personnel at the BCT echelon and below, and applies equally to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR). It is not intended for use by BCTs or units that have not yet begun transforming to the new Army BCT structure.

No two transforming BCTs look alike. There are notable differences between HBCT, IBCT, and SBCT organizational designs. This manual focuses on the functions and processes necessary in providing intelligence support to BCT operations, regardless of its specific organization. The term “BCT” refers to all organization types unless stated otherwise.

The proponent of this publication is the United States Army Training and Doctrine Command (TRADOC). Any comments and recommended changes, please email them directly to the US Army Intelligence Center and Fort Huachuca at ATZS-FDC-D@conus.army.mil or mail them to Commander, ATTN: ATZS-CDI-D, US Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

This publication does not implement any Standardization Agreements (STANAGs). It complies with all applicable STANAGs and Quadripartite Standardization Agreements. This document does not contain copyrighted material.

This page intentionally left blank.

PART ONE

Brigade Intelligence Fundamentals

This chapter identifies the modular concept and gives a brief BCT background. It specifically provides an overview of the BCT's intelligence support mission. The BCT uses current and emerging technology to execute offensive, defensive, stability operations, and civil support operations. These operations are adaptable within any multidimensional, precise, noncontiguous, distributed, simultaneous, and unique environment. Intelligence in the BCT is part of an integrated ISR effort that emphasizes the development of situational understanding prior to contact with the threat. This is accomplished by leveraging the intelligence warfighting function enabled by the Distributed Common Ground System-Army (DCGS-A) enterprise and accessing unprecedented amounts of information and databases. Through situational understanding the maneuver forces can be positioned for maximum effect rather than used to develop a threat picture. Information digitization allows the BCT to control ISR operations, provide continuous situational understanding, and support the commander's ability to make sound decisions.

Chapter 1

Fundamentals of Brigade Combat Team Intelligence Operations

BRIGADE COMBAT TEAM INTELLIGENCE SUPPORT OVERVIEW

1-1. To effectively execute missions in full spectrum operations, the commander requires intelligence about the enemy and other conditions of the operational environment prior to engaging in operations. The 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). Intelligence assists the commander in visualizing the operational environment, organizing forces, and controlling operations to achieve the desired tactical objectives or end state. Intelligence supports protection by alerting the commander to emerging threats and assisting in security operations.

1-2. The BCT will deal with multiple threats. The commander must understand how current and potential enemies organize, equip, recruit, train, employ, and control their forces. Intelligence provides an understanding of the enemy, which assists in planning, preparing, and executing military operations. The commander must also understand the operational environment and its effects upon both friendly and enemy operations. The BCT commander receives mission-oriented intelligence on threat forces and on the operational environment from the S-2. The S-2 depends upon ISR assets to collect and provide information on the enemy and other conditions of the operational environment.

1-3. One of the most significant contributions that intelligence personnel can accomplish is to accurately predict future enemy courses of action (COAs). Although this is an extremely difficult task, predictive intelligence enables the commander and staff to anticipate key enemy actions or reactions and develop corresponding plans or counteractions. Intelligence is vitally important in influencing operational decision making. Commanders must receive the intelligence in a timely manner, understand it (because it is tailored

to the commander's critical information requirements [CCIRs]), believe it, and act upon it. Through this doctrinal concept, intelligence drives operations.

1-4. Every BCT must operate in an operational environment that extends beyond the physical battlefield. Operational environments are 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 goes beyond the traditional physical dimensions of width, depth, and height; it encompasses physical areas and factors of the air, land, maritime, and space domains. It also includes the information environment and enemy, adversary, friendly, and neutral systems.

1-5. The operational environment extends beyond the brigades' physical boundaries through its communications and digital connectivity to other Army, joint, interagency, and multinational elements. This connectivity includes information "reach" to other organizations and assets in the continental United States (CONUS) or other locations outside the brigade's area of operations (AO). This reach capability is specifically important for collaborative efforts between the SBCT and other elements. The DCGS-A enterprise-provides the BCT access to a net-centric ISR Enterprise, providing access to joint, interagency, and multinational data and products as well as supporting reach operations.

1-6. Precision includes every aspect of military operations from deployment through combat and redeployment, or transition to other operations. In force projection, precision means getting the right force, effectively trained and rehearsed, to the right place on time for any given situation. In combat operations, precision means precise maneuver and munitions that not only strike the intended target but also achieve the desired effect. Three capabilities enable precise operations:

- The DCGS-A net-centric enterprise, provides Soldiers and leaders at all echelons the information required for making the best decision in each situation.
- A full suite of strategic, operational, and tactical sensors, linked to analytical teams that can fuse the increasing amounts of combat information into intelligence products to provide situational understanding with greater clarity than previously possible.
- Simulation, which enables Army elements to be tailored based on an emerging situation or crisis; plan operations based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC); and wargame and rehearse those operations yielding precision in execution.

NONCONTIGUOUS

1-7. Operations in noncontiguous AOs do not conform to the traditional battlefield framework. Instead, the battlefield is fluid, changing as METT-TC change through planning, preparing, and executing an operation. Synchronization of near-simultaneous operations is another component necessary to achieve noncontiguous effects across the battlefield. The BCT and/or SBCT battlefield may or may not be contiguous with other BCT organizations, Army forces or joint contingency force elements. There may be gaps between unit boundaries that require coverage by sensors either organic to the brigade or other Army force units.

DISTRIBUTED

1-8. Additionally, BCT and/or SBCT operations are distributed; that is, executed throughout the three-dimensional battlefield. In practice, operations are executed where and when required to achieve simultaneous effects at multiple decision points (DPs) vice concentrated effects at a single DP. Distributed operations—

- Empower subordinates to operate independently within the commander's intent, leading to synergistic effects that exceed the effects of a centralized headquarters.
- Can execute numerous integrated tasks simultaneously across the battlefield. Some functions, such as resource management, are best executed centrally, and the brigade seeks to execute each function using the best operational scheme.

1-9. The BCT develops a central intent and concept, conducts parallel planning and coordination enabled by digitization, and executes distributed precision operations to accomplish the mission.

SIMULTANEOUS

1-10. Decentralized operations that are multidimensional, precise, noncontiguous, and distributed yield the capability to conduct simultaneous operations across the full spectrum of operations. Simultaneous operations seize the initiative and present the enemy leadership with multiple crises and no effective response. Rather than a single, concentrated attack, the BCT executes a series of attacks (lethal and nonlethal) as simultaneously as possible. Digitization, intelligence automation, and vertical and horizontal integration provide brigade units the ability to plan, coordinate, and execute actions simultaneously. Each of these actions creates an effect, the sum of which is greater than if the actions were sequential.

INTEGRATED

1-11. The BCT is fully integrated into joint, interagency, and multinational operations. Integrated operations enable the Army to leverage the full suite of capabilities the services bring to the operational environment. An interdependent relationship exists in this integrated environment. Each echelon or organization collaborates with others to achieve and maintain a continuous situational understanding and determine the right COA. The integrated environment also encompasses the integration of ISR capabilities into a unified effort within the brigade operations that answers the CCIRs. ISR operations are a fundamental aspect of achieving an accurate and comprehensive understanding of the threat and other conditions of the operational environment that is necessary to gain information superiority over the threat force.

DIGITIZATION

1-12. Digitization enables the BCT to direct and control operations, including ISR operations, more effectively. DCGS-A enhances the brigade's ability to manage the large volume of data, information, and intelligence that flows within the brigade staff and among the brigade command posts (CPs), its subordinate commands, lateral units, and higher headquarters. The staff can parse much of this information directly into a shared Joint Common Data Base (JCDB) for use throughout the brigade. BCT units gain at least three distinct advantages from the digitized environment:

- Control Operational Pace. Digitization provides the capability to electronically store and transmit information that would otherwise have to be written or drawn on a hardcopy product. An obvious advantage of digitization is the timesavings that come from being able to transmit this data via radio or landline instead of having to hand carry the product. This enables different echelons to conduct parallel planning and allows a faster operational pace.
- Continuous Situational Awareness. A database of information contains the location, identification, status, and activity of each friendly entity. Enhanced collection and reporting capabilities provide a more timely and accurate picture of the threat situation. These elements facilitate continuous situational understanding.
- Enhanced Battle Command. With continuous situational understanding comes the knowledge and understanding that commanders need to visualize, describe, and direct operations through more precise (in some aspects) but also more flexible orders. Digitization also allows commanders to more accurately reposition and redirect assets, and provides positive control of assets responding to changes in the scheme of maneuver.

1-13. Another advantage of digitization is the ability to automatically store transmitted data in a database from which it may be retrieved, processed, and manipulated with minimal manual effort. For example, non-digital units send reports via voice radio message. In the BCT, digitally equipped units generate the report on a computer, transmit it rapidly to multiple addresses through a robust digital network, and both reporter and user can receive and act on the information and then store the report in a database for later evaluation, analysis, and presentation.

1-14. When these advantages are leveraged by modern communications and automated processing systems available in the brigade, other advantages become apparent. Data that is critical to commanders, staff, and intelligence analysts can be transmitted and shared by multiple users at multiple echelons. This common data when combined with new collaboration tools facilitates a common interpretation and understanding of the common operational picture (COP) of the area of interest (AOI). Additionally, digitization creates new applications and a new paradigm in the relationship between intelligence, fires, and maneuver.

INTELLIGENCE WARFIGHTING FUNCTION

1-15. 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). This complement of equipment, personnel, and organizations individually and collectively produce relevant, timely information, and intelligence required to provide the commander. Its fundamental purpose is to provide visualization and situational understanding of the operational environment and direct military actions.

1-16. The intelligence warfighting function is comprehensive and reaches across full spectrum operations and levels of war to produce the intelligence required to win on the battlefield. The DCGS-A enabled intelligence enterprise provides specific intelligence and communications structures. A combination of space, aerial, seaborne, and ground-based systems provide the most comprehensive intelligence possible. Inherent within the intelligence warfighting function is the capability to plan and prepare intelligence operations, collect and process information, produce relevant intelligence, and disseminate intelligence and other critical information on the threat and other conditions of the operational environment in an understandable form to those who need it, when they need it.

RECENT INTELLIGENCE OPERATIONS

1-17. Intelligence and operations have a dynamic relationship. Effective intelligence drives effective operations. Effective operations produce information, which generates more intelligence. One of the key functions of intelligence within recent operations is to facilitate an understanding of the operational environment, with emphasis on the elements of the populace, host nation (HN), and insurgents and how those elements interact. The intelligence to support this function requires presenting a greater level of detail to the commander and staff and an ability to explain complex relationships. Commanders and staffs require insight into cultures, perceptions, values, beliefs, interests, and the decision-making processes of varied individuals and groups. These insights are a critical component to the planning and conduct of all operations.

The Warfighting Functions
- Movement and maneuver
- Intelligence
- Fires
- Sustainment
- Protection
- C2
- Protection

1-18. All operations have an intelligence component. When conducting surveillance or reconnaissance, Soldiers actively observe details related to the CCIR. Soldiers must be competent in reporting their experience, perceptions, and judgments concisely and accurately. To accommodate this task, the leadership must train Soldiers and foster an environment that encourages small unit and individual Soldier reporting.

1-19. All Soldiers report their observations through the chain of command even when not specifically tasked to conduct surveillance or reconnaissance. The Soldier remains an indispensable source for much of the information needed by the commander. Observations and experiences of Soldiers often working with the local population provide depth and context to information collected through surveillance or reconnaissance. Commanders and staff must ensure information collected from Soldiers within their AO is integrated into the overall intelligence warfighting function. Focusing on effective integration will contribute to more detailed and accurate intelligence.

1-20. As Soldiers learn to regularly report relevant information battalion and brigade intelligence staffs can quickly become overwhelmed with information if not sufficiently trained and prepared to handle the large volumes of reports. Lessons learned collected from BCT Battalion and Brigade level S-2s who served in

Operation Iraqi Freedom (OIF) attest to the tremendous volume of information reported. They related that while every Soldier and leader who was exposed to Iraqis was a potential information collector, it fell on the Battalion or Brigade S-2 to parse, vet, link, and package the information into useable intelligence. SOPs must be written and trained in order to prepare S-2s to handle large volumes of information. In many cases S-2s required additional personnel to adequately support operations.

1-21. Analysis within complex stability operations follows generic doctrinal methodologies; however, the analysis requires a much greater emphasis on civil considerations, especially demographic groups and formal or informal leaders. Whenever possible, planning and preparation for operations should include a thorough and detailed execution of the intelligence preparation of the battlefield (IPB) process. Often the in-depth IPB process in recent operations has had to consider areas like economics, social anthropology, and the effects of governance. Therefore, the integrating staff must draw on the experience of non-intelligence personnel and external experts with local and regional knowledge.

1-22. In order to bring clarity to the broad scope of information available, all staff members work to improve the knowledge base used to develop an understanding of the AOI and AO. For example, civil affairs (CA) personnel receive training in analysis of populations, cultures, and economic development. The process to describe the operational environment in recent operations is articulated well in FM 3-24, chapter 3.

1-23. Open-source intelligence (OSINT) is often a source of potentially important information covering aspects of civil considerations like culture, languages, history, current events, and actions of the government. Open sources include books, magazines, encyclopedias, web sites, and tourist maps. Academic sources, such as articles and university personnel, can also provide critical information.

1-24. Pushing quick reaction capabilities (QRC) down to the lowest possible level has generated an operational need to form intelligence teams at the company level. Unmanned ground sensors, weapons intelligence teams, Signals Intelligence (SIGINT) terminal guidance, detainee handling and processing, data exploitation and document and media exploitation (DOMEX) provide unprecedented ISR capabilities and opportunities below the battalion level. Some commanders have opted to form company intelligence support teams (ad hoc) to improve timely processing and access to perishable information.

1-25. With the continuing growth in the world's urban areas and increasing population concentrations in urban areas, the probability that the US Army will conduct full spectrum operations in urban environments is ever more likely. As urbanization has changed the demographic landscape, potential enemies recognize the inherent danger and complexity of this environment to the attacker, and may view it as their best chance to negate the technological and firepower advantages of modernized opponents. Given the global population trends and the likely strategies and tactics of future threats, Army forces will likely conduct operations in, around, and over urban areas—not as a matter of fate, but as a deliberate choice linked to national security objectives and strategy. Stability operations—where keeping the social structure, economic structure, and political support institutions intact and functioning or having to almost simultaneously provide the services associated with those structures and institutions is the primary mission—may dominate urban operations. This requires specific and timely intelligence support, placing a tremendous demand on the intelligence warfighting function for operations, short-term planning, and long-term planning.

This page intentionally left blank.

Chapter 2

Brigade Combat Team Intelligence Staff

The BCT's intelligence staff is an essential component of the ISR and security effort. Its operational success relies upon the ability of the S-2 to develop and integrate the threat situation into the brigade's COP. 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.

MISSION

2-1. The BCT S-2 facilitates situational understanding of the operational environment for the commander and staff and assists the commander in synchronizing intelligence with operations by assisting the S-3 with the ISR integration effort. The S-2 uses the intelligence capabilities available to the brigade and an understanding of the operational environment to provide intelligence products and recommendations to the brigade commander.

2-2. The operational environment can be defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decision of the commander. The operational environment encompasses physical areas and factors of the air, land, maritime, and space domains. It also includes the information environment and enemy, adversary, friendly, and neutral systems. Analysis of the operational environment—in terms of political, military, economic, social, information, and infrastructure with the addition of physical environment and time (PMESII-PT) variables—provides relevant information that senior commanders use to understand, visualize, and describe the operational environment. As a set, these operational variables are often abbreviated as PMESII-PT.

2-3. The S-2 also exercises staff responsibility for intelligence training. See appendix A for more information on BCT Intelligence Readiness Training.

ORGANIZATION

2-4. The BCT intelligence staff is discussed below.

BRIGADE INTELLIGENCE STAFF

2-5. 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.

2-6. The ISR Requirements Section and the Situation and Target Development Section, of the MI Company's Analysis and Integration Platoon, are normally collocated with and under operational control (OPCON) of the BCT S-2 during operations. The organic engineer topographic (MI Company) terrain team provides the geospatial support. The S-2 will normally designate an individual or team to manage the intelligence operations, planning, and production missions. The staff is responsible for producing intelligence that depicts the current threat situation and predicts future threat objectives, capabilities, and COAs. The intelligence staff works with other staff elements to synchronize intelligence operations with planning, preparing, executing, and assessing the brigade's ISR operations.

S-2 INTELLIGENCE OFFICER

2-7. The S-2 is the brigade's senior intelligence staff officer for all ISR synchronization matters. The S-2 ensures the brigade's complex ISR operations satisfy the CCIRs, specifically the commander's PIRs, 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 (EAB) 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. Some of the specific responsibilities of the S-2 are to—

- Provide situation development, target development, support to lethal and nonlethal targeting, support to indications and warnings (I&W), support to combat assessment, and support to protection to include force protection (FP).
- Provide the commander and staff with assessments of threat capabilities, intentions, and COAs as they relate to the brigade and its mission.
- Identify gaps in intelligence and advise the commander on developing collection strategies.
- Disseminate intelligence products throughout the brigade.
- Answer requests for information (RFIs) from subordinate commanders, staffs, and higher and adjacent units.
- Coordinate the brigade's intelligence requirements with EABs.

S-2 OPERATIONS

2-8. 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 AO and AOI that affect the current operation. The S-2 operations team uses the 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 COP. The S-2 operations team assists the S-2 in tracking threat COAs and alerting the commander of changes to predicted threat COAs, capabilities, or intentions. The S-2 operations team is also tasked to—

- Develop the current situation template, ensuring that relevant elements of the threat, terrain, weather, and civil considerations are included.
- Present the current situation and project threat and neutral COAs that may impact operations.
- Assess public opinion of friendly COAs.
- Assist in identifying opportunities for friendly branches and sequels by monitoring the current operational environment within the brigade's AO and identifying when the planning assumptions for the threat, terrain, weather, and civil considerations begin to diverge from the predicted COA.
- Manage ISR operations within the brigade's AO.
- Maintain the intelligence portion of the brigade's COP.
- Support the distributed and collaborative production of the EAB G-2's assessment of the operational environment by reporting and analyzing the brigade's operational environment.
- Disseminate intelligence products from the brigade to higher, subordinate, and adjacent units.
- Receive, evaluate, and act upon relevant information and intelligence reporting from higher, subordinate, and adjacent units.
- Manage intelligence staff input to lethal and nonlethal targets.
- Track threat attrition, track current threat TTP, and present estimates of threat combat effectiveness.
- Assume specific S-2 planning responsibilities, by exception, based on the S-2's direction.

S-2 PLANS

2-9. The S-2 plans team is responsible for threat COA development and wargaming. The S-2 plans team—

- Works with the S-3 planner and other staff elements to plan for future operations using the military decision-making process (MDMP) and recommends PIR for approval.
- Works with the S-3 planner to coordinate with reconnaissance assets (reconnaissance squadron for HBCT or IBCT and reconnaissance, and reconnaissance squadrons for SBCT) for incorporation of planning into the brigade's overall ISR effort.
- Refines and presents threat COAs, as part of an integrated staff effort, during mission analysis, COA development, and wargaming.
- Writes the intelligence annex (B) and the intelligence portions of the brigade operations order (OPORD) to include the ISR Integration Plan.
- Coordinates with the MI Company for the development and publication of the intelligence running estimate and intelligence support package (ISP).
- Coordinates with the S-2 operations team to ensure future COAs are reflected in the current situation.
- Monitors the current situation to continually assess the impact of the threat, terrain, weather, and civil considerations of future COAs.
- Wargames threat COAs against friendly COAs during staff planning and decision making.
- Assists the brigade's fire support coordinator (FSCOORD) by identifying threat high-value targets (HVTs) and recommending potential high-payoff targets (HPTs) for both lethal and nonlethal attack (to include command and control [C2] warfare).
- Conducts detailed horizontal and vertical planning and collaboration with the other brigade staff members and with higher, lower, and adjacent organizations.
- Identifies intelligence that may affect the assured mobility of the BCT and its subordinate elements.

S-2X

2-10. 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 collection requirements.

2-11. The S-2X consists of the S-2X Officer, the HUMINT Operations Cell (HOC), and the Counterintelligence Coordinating Authority (CICA). The S-2X section provides the expertise for the conduct of HUMINT and CI operations in the brigade's operational environment. While the MI Company (and reconnaissance squadron for 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 (DS) and advice from the Brigade Operational Legal Team (BOLT). The S-2X —

- Supports requirements management (RM) through developing HUMINT specific information requirements (SIRs) from the commander's PIRs.
- Deconflicts and synchronizes all HUMINT activities in the brigade's AOI.
- Assists the brigade and squadron commander in developing HUMINT ISR tasks based on the integrated ISR plan.
- Coordinates technical support as needed for the HUMINT assets in the brigade's AOI.
- Conducts analysis of HUMINT reporting and provides input to the Analysis and Integration Platoon.
- Oversees the source registry for the operational environment.
- Manages the intelligence contingency fund (ICF) and source incentive program.

- Acts as system administrator for HUMINT specific automation systems to ensure connectivity with higher and adjacent HUMINT entities.
- Reviews HUMINT operations, funding requests, and collections to ensure compliance with legal, regulatory, and procedural guidelines.
- Oversees the reporting of questionable activities by HUMINT assets through command channels to the Department of the Army (DA) pursuant to AR 381-10, Procedure 15.

2-12. Within a BCT there are no organic CI Operational Management Teams (OMTs) or CI teams. CI teams may be pushed down from the Battlefield Surveillance Brigade (BFSB) or other higher echelon unit to a BCT. These teams must be controlled by the Brigade S-2X CICA. If augmented, the mission of the CI teams is to conduct—

- CI assessments.
- Limited CI investigations.
- CI collection
- Limited CI analysis.

HUMINT OPERATIONS CELL (HOC)

2-13. The HOC assists the S-2X in coordinating all organic HUMINT activities and ensuring those activities are deconflicted and synchronized with all EAB HUMINT activities within the BCT's AO. The HOC—

- Provides technical expertise to support the control of HUMINT entities in the designated AO.
- Is the deconfliction authority for HUMINT activities in the designated operational environment.
- Accomplishes all responsibilities through coordination with the operational units and the CICA.
- Coordinates with the S-2 and the RM team to identify and refine requirements for HUMINT collection operations.
- Develops indicators and requirements for HUMINT entities in the AO and disseminates required technical data to support the tasked collection.
- Coordinates with the CICA to provide CI support to HUMINT operations.
- Ensures HUMINT collector contact with an adversary intelligence service is reported to the CICA.
- Routinely evaluates HUMINT operations to ensure proper handling by case officers or special agents, validates source ability to satisfy requirements, and determines value for continuing the operation.
- Establishes and maintains connectivity with national and multinational HUMINT organizations.
- Provides oversight to HUMINT support to vulnerability assessments and other FP initiatives.
- Establishes and executes quality control mechanisms for all HUMINT reporting.
- Routinely provides feedback to the HUMINT entities in the designated operational environment regarding their collection activities.
- Interacts with the CICA to ensure HUMINT activities do not conflict with CI activities in the AO.
- Establishes and maintains connectivity and a deconfliction relationship with organizations that potentially interact with the CI and HUMINT source pool (for example, Civil Affairs [CA], psychological operations (PSYOP), and Special Forces Liaison Teams).
- Maintains duplicate dossiers for all sources and contacts.

CI COORDINATING AUTHORITY

2-14. The CICA coordinates, synchronizes, and provides CI expertise to support the control of CI activities and entities in the designated AO. As such, the CICA is the deconfliction authority for CI activities and entities in the designated AO. When the BCT is augmented with nonorganic CI teams the CICA controls their activities. The CICA, through coordination with the operational units and the HOC, will—

- Coordinate with the S-2 and RM team to identify and refine requirements for CI collection, operations, or investigations.
- Develop specific requirements or ISR tasks or RFIs to CI entities in the AO and disseminate required technical data to support the tasked collection.
- Ensure registration of all CI sources.
- Routinely evaluate CI military source operations to ensure proper handling by special agents, validate source ability to satisfy requirements, and determine value in continuing the operation.
- Ensure a robust Subversion and Espionage Directed Against the Army (SAEDA) reporting program.
- Ensure exploitation opportunities are preserved while conducting an assessment.
- Coordinate with BOLT to ensure investigations are planned, coordinated, and executed in accordance with applicable directives and regulations.
- Establish and maintain connectivity with the Sub-Control Office and Army Central Control Office.
- Provide oversight to CI support to vulnerability assessments and other protection initiatives.
- Ensure CI support is provided to debriefing centers and/or interrogation facilities.
- Establish and execute quality control mechanisms for all CI reporting.
- Routinely provide feedback to the CI entities in the designated AO regarding their collection activities, operations, and investigations.
- Interact with the HOC to ensure CI activities do not conflict with HUMINT activities in the AO.
- Ensure coordination and deconfliction between the Provost Marshal Office and intelligence entities when conducting liaison with HN law enforcement agencies.
- Maintain duplicate dossiers for all sources and contacts.

S-2 WEATHER TEAM

2-15. 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 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.

2-16. During situation development, particularly the current operations, weather will support readjustment of sensors (including weather sensors) to fill information gaps and support the targeting process. That will drive a decision-making cycle much shorter than in the past. The dynamic collection asset retasking such as the unmanned aerial system (UAS) requires immediate forecast assessment of the weather effects in the new mission area.

2-17. The Air Force Weather (AFW) team provides accurate, timely, and reliable meteorological support to all facets of the brigade force planning, training, deployment, employment, and evaluation. The BWT is the main source of weather support for the brigade. As a member of the commander's special staff, the staff weather officer (SWO) (of the BWT) is responsible for coordinating operational weather support 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.

2-18. BWTs are tactical mission and operations specialists, experts in the art of applying weather to the customer's mission. They evaluate and apply operational weather squadron (OWS) forecasts to specific brigade missions, weapons systems, strategies, tactics, and applications; deploy with the brigade; and, in general, provide both direct and indirect tailored customer support. Specifically, the BWT will—

- Coordinate, prior to deployment, both in-garrison and deployed weather support procedures in a memorandum of understanding with the supported Army command.
- Advise the brigade commander on AFW capabilities, limitations, and the ways in which weather can enhance combat operations.
- Advise the Air Force on Army command operational weather support requirements.
- Assist the S-2/S-3 in monitoring the weather support mission, identifying responsibilities, and resolving weather support deficiencies.
- Coordinate with the MI Company for logistics-related support and equipment issues (for example, Multiple Integrated Laser Engagement System [MILES] gear, ammunition).

2-19. The Air Force provides direct weather support using a dedicated BWT. BWT manning may hinge on available (pooled) Air Force manpower, and required support to cope with BCT Army force generation cycle rotations (see FMI 3-0.1). The BWT will likely use the Army Integrated Meteorological System-Light (IMETS-L)/DCGS-A configuration, plus Air Force equipment, to support all customers from the brigade tactical operations center (TOC). The BWT relies on the MI Company Analysis and Integration Platoon for all transportation of personnel and equipment.

2-20. To effectively support the brigade's warfighting capabilities, the SWO is allocated workspace and power within the brigade. The SWO routinely interfaces with the entire brigade commander's staff to tailor weather products to meet the challenges of a rapidly changing warfighting environment. The SWO works with the S-2 to determine the best location for the SWO work center. This location must optimize the SWOs interaction with both planning and operations functions. For example, the SWOs should be positioned to monitor the dynamic battlefield situation to assimilate weather intelligence into the full battlefield picture.

2-21. At home station BWT members may train Soldiers, selected by the brigade commander, on how to take limited battlefield weather observations. The brigade commander may purchase handheld weather observing equipment to distribute to the select Soldiers. While deployed (and if the battlefield situation allows) the brigade commander ensures these Soldiers take weather observations and forward them to the BWT. The following discuss weather team capabilities and limitations.

- Capabilities:
  - Translate the current and future state of space and the atmosphere into impacts on a commander's wartime missions.
  - Assist the S-2 and staff in producing weather visualizations, graphic overlays for the COP, and weather effects tactical decision aids (for example, effects of weather on Army platforms, components).
  - Assist the S-2 in arranging for indirect weather support for subordinate operations such as tactical unmanned aircraft systems (TUASs).
  - Evaluate and disseminate weather products and data and make them available in DCGS-A for integration into other Army Battle Command Systems (ABCSs).
  - Produce weather effects decision aids, graphical overlays, and tailored products on the DCGS-A weather portal or an electronic homepage.
  - Provide weather effects information with emphasis on critical threshold values which limit weapon systems, tactics, and operations.

- Limitations:
  - A small BWT is minimally sized to perform its core functions as outlined in this manual. To effectively maintain meteorological battlefield awareness will require near-constant monitoring of information data flow from the AFW Agency, the supporting regional OWS,

headquarters and headquarters company (HHC), and other BWTs and deployed weather-sensing equipment in the vicinity. Any non-weather duties assigned to the BWTs would adversely affect the quality of weather support. BWTs should not be assigned to duties inconsistent with their core functions.

- BWTs currently rely on a tactical-very small aperture terminal provided by the Air Force but are being replaced with the Global Broadcast System to receive theater and strategic data and products. Communications outages require BWTs to use alternate communications (for example, TROJAN Special Purpose Integrated Remote Intelligence Terminal [SPIRIT]). In the absence of high-bandwidth communications, the BWT's ability to support all warfighting functions is severely diminished.
- Without immediate access to equipment upon arrival at the deployed location, the BWT is unable to provide weather support.

OPERATIONS

2-22. The operations of the BCT intelligence staff are discussed below.

PLANNING OPERATIONS

2-23. There are two processes available to develop operational planning. One is the MDMP which commanders and staff routinely execute; the other is the rapid decision-making and synchronization process (RDSP) (see FMI 5-0.1) that is routinely employed by commanders and staff when MDMP and troop- leading procedures are not necessary. The RDSP is based on an existing order while the MDMP is not.

2-24. Intelligence support to the RDSP focuses on experience and situational awareness in predicting activities or events and managing assets dynamically to rapidly adapt to a changing threat environment. The brigade plans operations using the MDMP depicted in figure 2-1. The brigade staff working with the reconnaissance squadron (SBCT Reconnaissance Squadron) and other supporting elements in a parallel and collaborative process support each step of the MDMP from receipt of mission to orders production, with a variety of intelligence products and activities.

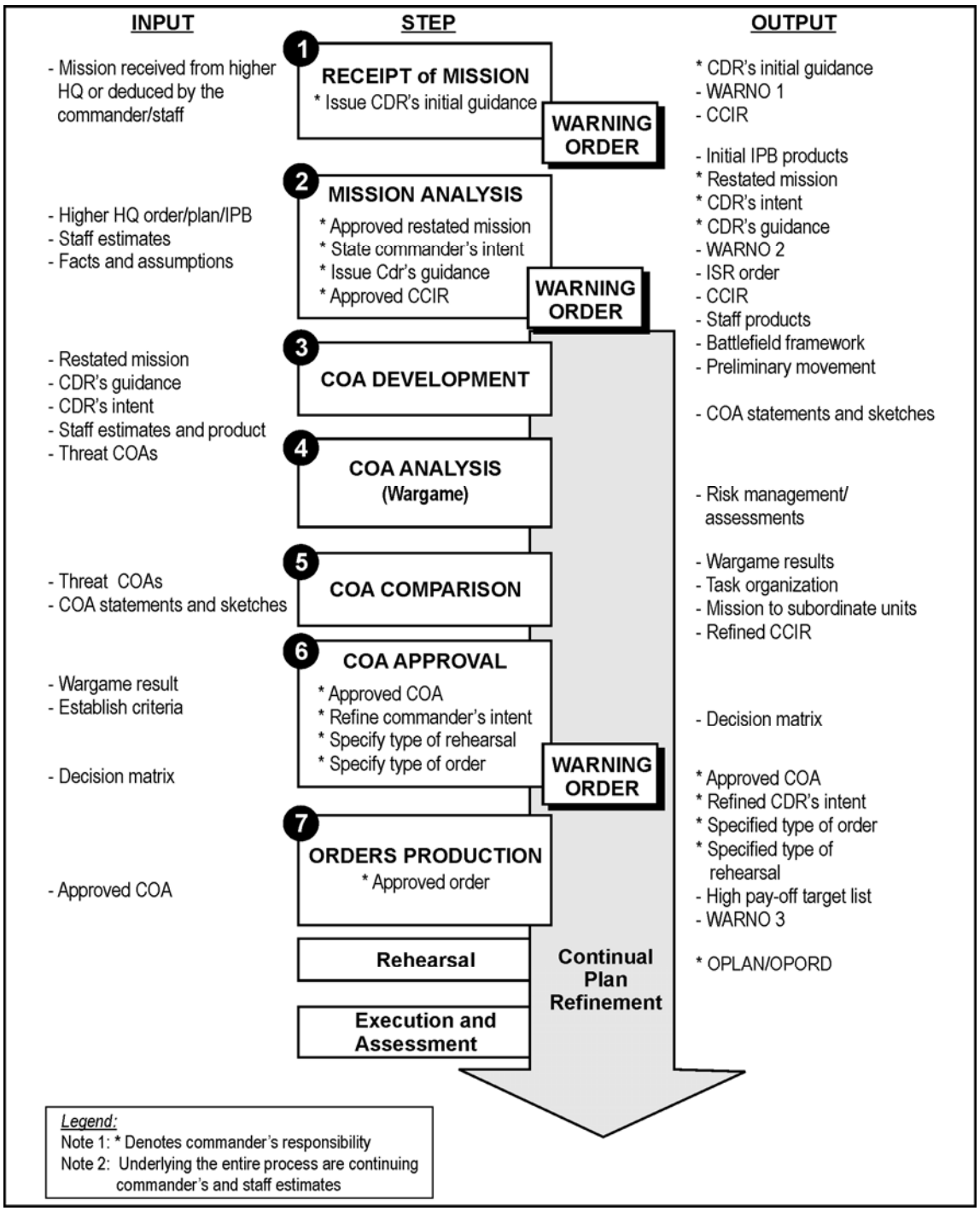


Figure 2-1. The military decision-making process

2-25. The MDMP is a 7-step analytical process with each step building upon the previous steps. Within each step, the commander and staff assess the operation based on their understanding, monitoring, and evaluation of the situation and operation. Each step in the process has different intelligence requirements

and imposes different tasks on the supporting ISR organizations at all levels. The intelligence staff assists the commander in planning, preparing, executing, and assessing operations by—

- Providing timely, relevant, accurate, and predictive intelligence.
- Making estimates and recommendations.
- Preparing the intelligence portions of the operations plans (OPLANs) and OPORDs.
- Monitoring the execution of ISR operations.

2-26. See FM 3-0, FM 5-0, and FM 6-0 for more information on the operations and planning process.

Receipt of Mission

2-27. Planning begins with the issuance of the higher headquarters commander's intent, guidance, and/or orders for an operation. The commander provides guidance to the staff and supporting ISR organizations. The commander identifies the brigade's mission, commander's intent, AOs, AOIs, and intelligence requirements. Based on this information, the S-2, S-3, and the rest of the staff begin to prepare IPB and ISR planning products, in collaboration with the reconnaissance squadron (SBCT Reconnaissance Squadron) staff, to support the next step of the MDMP.

Mission Analysis

2-28. Upon receipt of the mission, the brigade staff reviews general military intelligence (GMI) products, the current threat situation, ISR asset status, and EAB warning orders (WARNOs) or fragmentary orders (FRAGOs). The DCGS-A enterprise facilitates unprecedented access to numerous tactical to national databases. Prior to tasking assets, the S-2 must identify gaps in the current intelligence holdings and determine which collection asset can answer the commander's PIR in a timely manner. This information is made immediately available to the reconnaissance squadron (SBCT Reconnaissance Squadron) and other subordinate elements to begin their planning process. The S-2 and staff identify gaps in the intelligence effort and determine what assets are available to collect on these gaps. The S-2 and S-3 turn this into an initial ISR plan that tasks ISR assets as soon as possible to begin the collection effort.

2-29. During the mission analysis brief, the commander approves the initial CCIR and initial ISR plan. To facilitate effective planning, the unit develops and issues the initial ISR plan as soon as possible. The ISR plan may be issued as part of a WARNO, FRAGO, or OPORD.

2-30. The brigade S-2, supported by the MI Company, develops IPB products to support COA development and the intelligence running estimate. The S-2 coordinates with the reconnaissance squadron (SBCT Reconnaissance Squadron) to determine the current status of the brigade's ISR effort to make recommendations to the commander on future collection requirements. The S-2 determines the status of the rest of the brigade's ISR capabilities and available EAB resources to recommend use of available resources to the S-3 that support the ISR effort. The S-2 focuses the S-2 staff efforts and the brigade ISR assets by defining the AO and AOI.

2-31. In the SBCT, the reconnaissance squadron serves as the commander's primary eyes, ears, and sensors and as the first-line military assessment for information gathered through reconnaissance and surveillance. The surveillance troop assets are normally retained under the surveillance troop commander's immediate control to retain flexibility of support to the brigade and its subordinate battalions. As a general rule, the SBCT does not task organize ISR assets from the reconnaissance squadron to infantry battalions.

2-32. Additionally, the brigade headquarters does not assume C2 of subordinate units' ISR assets. Intelligence requirements and surveillance and reconnaissance requirements are missions tasked to units. However, based on METT-TC, the brigade commander may task organize ISR assets as the commander deems necessary. Significant collaborative planning between the brigade S-2/S-3 and the reconnaissance squadron S-2/S-3 is essential to ensure the brigade's ISR plan is synchronized with and integrated into the brigade's operational plan.

2-33. The brigade S-2 collaborates with the MI Company, and the reconnaissance squadron (SBCT Reconnaissance Squadron) staff to develop the brigade's ISR plan. This begins with using intelligence

products from EAB intelligence organizations, as well as available open-source material. It evolves into the development of a reconnaissance effort by the MI Company and reconnaissance squadron (SBCT Reconnaissance Squadron) and eventually a brigade ISR plan. During this planning cycle the brigade reevaluates what it needs to know and refocuses the ISR effort accordingly.

2-34. The ISR planning process is a joint effort by the entire staff. The ISR plan is initially developed during mission analysis, and continuously refined through the MDMP, in conjunction with the maneuver plan and through the execution of the operation. The brigade S-2 and S-3, along with the entire staff, are responsible for ISR synchronization and ISR integration to ensure the ISR plan meets the operational needs of the commander to facilitate decision making. Intelligence support to the ISR planning process encompasses continuous ISR asset assessments identifying what resources and collection tasks need modification as the concept of the operation unfolds during mission execution.

2-35. The subordinate battalions are responsible for developing and executing an ISR plan within their assigned areas. The supporting ISR organizations begin their own MDMP parallel to that of the brigade to reduce the time between planning and executing the ISR operation. This also allows the commander to rapidly develop an integrated and executable ISR plan that can enable the brigade to achieve its objectives. Parallel planning relies on accurate and timely WARNOs and fully sharing information between the brigade staff and subordinate staffs as it becomes available.

2-36. Table 2-1 provides a checklist for S-2 actions.

COA Development

2-37. The S-2 uses the IPB process to systematically analyze the threat and variables of the operational environment. This analysis results in products that identify threat centers of gravity (COGs), HVTs, tactical objectives, and potential COAs. These threat-based products form the basis of friendly COAs, schemes of fire and maneuver, and ISR plans developed during the remaining steps of the MDMP. The S-2's ability to understand, articulate, and integrate into the MDMP how the threat operates, sees the friendly force, and makes decisions is an important factor in how well the brigade shapes and decisively engages the threat on the battlefield.

2-38. During COA development, the S-2 and the MI Company work with other brigade staff elements and the staffs of supporting ISR organizations and subordinate battalion S-2s to refine IPB products and recommend ISR priorities that support the future operation. The S-2 plans team ensures that the S-2 operations team and the MI Company elements are kept abreast of planning assumptions and projected requirements.

2-39. The S-2 works with other brigade staff planning elements to refine IPB products and integrate them into their COA development. The S-2's primary role is to highlight threat objectives, DPs, COGs, HVTs, and potential vulnerabilities. This threat awareness helps the staff planning elements develop friendly COAs and associated risks, task organizations, and schemes of maneuver, fire, and support.

2-40. After developing threat COAs, the S-2 and MI Company develop the intelligence running estimate. The IPB products make up the basis of the intelligence estimate. The intelligence running estimate—

- Forms the basis for the facts and assumptions of the MDMP, driving various staff section running estimates and the remaining steps in the MDMP.
- Is a logical and orderly analysis of the terrain, weather, and civil considerations of the operational environment and its effects on friendly and threat COAs, threat capabilities and vulnerabilities, analysis of threat capabilities, TTP, and COAs, and probability of adoption.
- Provides the best possible answer to the commander's PIRs that are available at the time.
- Is dynamic and changes constantly with the situation.

2-41. The S-2 briefs the intelligence running estimate results to the brigade commander and staff. Upon conclusion of the staff briefings, the commander states his or her intent for the operation and provides additional planning guidance to the staff. The commander's guidance to the S-2 could include—

- Additional threat COAs and objectives to consider.
- Additions or deletions of threat DPs and HVTs.
- Approval or modification of recommended PIRs.
- Specific instructions on priority for and allocation of ISR support.

Table 2-1. S-2 actions checklist

Receipt of Mission

- Begin parallel planning and collaborate with higher and lower headquarters before and during receipt of the mission to facilitate the IPB process.
- Identify gaps in EAB headquarters ISR plan, intelligence database, and IPB products.
- Identify specified and implied tasks from EAB headquarters.
- Check databases for current threat, terrain, weather, and civil consideration data.
- Coordinate with the terrain and weather teams to ensure the required products are being developed and refined.
- Assess and recommend necessary adjustments to the ISR plan.
- Develop and submit initial RFIs based on gaps in the intelligence.
- Develop or update IPB products in coordination with the other staff elements.
- Recommend PIR for commander's approval.
- Complete initial ISR synchronization.

COA Development

- Integrate confirmed intelligence based upon the initial ISR effort.
- Refine and prioritize the situation templates.
- Refine the event templates and matrices.
- Update HVTs for targeting by lethal and nonlethal effects.
- Take an active part in analyzing combat power by providing all available information on the current threat forces and situation.
- Provide information on threat vulnerabilities while analyzing relative combat power.
- Consider as many possible COAs as time permits, starting with the most likely; including the worst case (most dangerous).
- Provide critical input to the MDMP based on information from ongoing ISR operations.

COA Analysis

- Refine the PIR with the latest time information is of value.
- Assist in the development of the HPT list.
- Refine the situation template.
- Redefine the threat COAs based on the developed DPs and the situation template.
- Develop critical threat DPs in relation to the friendly COA.
- Fight as an uncooperative enemy to develop DPs and project enemy losses.
- Address all relevant threat activities. Assist in the development of the target selection standard and attack guidance matrix from the wargamed COAs.
- Update the ISR plan.
- As a result from the wargame, refine the event template to include NAIs and refine the event matrix with corresponding DPs.
- Refine the situation templates from the results.
- Participate in the targeting process.
- Link NAIs to TAIs.
- Display the concept of ISR support during the wargame.
- Assist the S-3 in developing the DST.

OPORD Production

- Assist in preparing the order and submit annex B (Intelligence) as part of the OPORD.
- Submit annex B (Intelligence) as part of the OPORD.

COA Analysis (Wargaming)

2-42. The S-2 is responsible for articulating both the threat mission variables (METT-TC) and ISR aspects of each friendly COA during wargaming. The S-2 role-plays the threat commander, ensuring that well thought-out enemy actions or reactions are addressed for each friendly COA. The requirement manager orchestrates the maneuver of ISR assets during the wargame and establishes intelligence collection priorities that support that COA. The S-2 uses the information gained through staff wargaming to finalize IPB templates and intelligence running estimate, focus target development, and assist in refining the ISR plan.

2-43. During wargaming, the ISR requirements manager synchronizes the intelligence and security requirements, named areas of interest (NAIs), and target areas of interest (TAIs) for each friendly COA. The S-2 ensures the ISR plan is a collaborative product developed by the brigade staff and supporting ISR organizations. The ISR plan must—

- Describe transition from the brigade's current ISR operations and those required for each friendly COA.
- Be integrated into the brigade OPLAN to ensure that the best available combat information and intelligence are available to support the commander's decisions when executing various phases of the planned operation.

COA Comparison

2-44. In COA comparison the S-2, supported by the S-2 plans team and the ISR requirements manager, assists the brigade staff in understanding the risks, capabilities, and limitations of the brigade's ISR assets for each friendly COA under consideration. The S-2 ensures the recommended PIRs are incorporated in the tasking of subordinates and the requests to EAB. The S-2 coordinates with the supporting ISR organizations and battalion S-2s to ensure the ISR plan is understood and executable. When executed, the ISR plan should enable a rapid and seamless transition between the current and future operations.

2-45. The S-2 modifies the initial set of intelligence requirements developed during mission analysis to reflect the results of the wargaming. The S-2—

- Clearly delineates intelligence requirements.
- Ensures the synchronization of all available ISR assets.

COA Approval

2-46. The S-2 briefs updates to the commander and presents recommended PIR and the supporting ISR plan. Based upon the commander's acceptance, modification, or rejection of the staff's recommendation, the S-2 begins to implement, refine, or rework the intelligence running estimate, ISP, and ISR plan.

2-47. Once the commander approves a COA, the S-2 and S-3 coordinate with the reconnaissance squadron (SBCT Reconnaissance Squadron) and other supporting ISR resources to ensure the ISR concept supports the approved COA. The S-2 and S-3 must ensure that the staffs at all levels understand the following:

- ISR scheme of support.
- PIR and essential elements of friendly information (EEFI).
- Collection tasks.
- Production priorities.
- Timelines latest time information is of value (LTIOV).
- Intelligence control measures: target handover, reconnaissance handover, reporting responsibilities, and operational environment.
- Procedures for tasking and reporting.

Orders Production

2-48. The S-2 plans team, assisted by the MI Company, develops annex B (Intelligence) of the brigade OPORD. The S-2 plans team assists other brigade staff members in preparing the threat or ISR aspects of their annexes. Annex B, paragraph 3d(3), explains measures for handling personnel, documents, and material. The S-2 reviews the OPORD and annex B for accuracy and completeness. The S-2 forwards the annex to the S-3 to incorporate and disseminate in the brigade's OPORD. The ISR requirements manager, supported by the MI Company Analysis and Integration Platoon, develops RFIs (intelligence production) and, with S-2 approval, forwards them to the next higher echelon and adjacent units.

2-49. See FM 3-0, FM 5-0, and FM 6-0 for more information on the operations and planning processes.

PREPARING FOR OPERATIONS

2-50. ISR operations are the most important part of the preparation phase of operations. During this phase, commanders take every opportunity to improve their understanding of the threat and the military aspects of terrain and weather to verify planning assumptions and to refine the plan. It is also during the preparation period that the commander wants to defeat threat ISR operations to prevent the discovery of the brigade's plan and to protect against unforeseen threat actions. Therefore, ISR, if not already in motion, must begin during the preparation phase, while the majority of the brigade is completing the final OPORD and preparing for the upcoming operations.

Maintaining Continuity

2-51. Continuity of operations within the S-2 staff and the brigade ISR elements reduces turmoil and ensures sustained support to the brigade. The S-2 section must be capable of sustained 24-hour operations at each brigade CP under a variety of conditions (for example, digital or analog operations, reduced staffing, and chemical environment). Development, practice, and enforcement of S-2 SOPs ensure continuity. S-2s should cover the following procedures:

- Shift change briefings or meetings.
- Sleep and eating rotation schedules.
- Staff drills for actions such as ISR planning, orders production, and retasking.
- Standard report and graphic product formats.
- CP organization and operation.
- Battle drills for continuation of operations (TOC displacement, loss of equipment or personnel).
- Succession of staff supervision (command).

Managing Information

2-52. The S-2 staff is responsible for maintaining the brigade's threat database and situation graphics. While the S-2 staff is capable of preparing and presenting intelligence products, it depends on the Analysis and Integration Platoon's data management capability (see chapter 8) to maintain the current situation. However, when the brigade is conducting split-based operations, these tasks are accomplished in the forward CP by the S-2 operations team augmented by MI Company assets as required. The MI Company (-) provides analytical support to the brigade Main CP focused on future operations. The data managers will conduct data mining activities enabled by the DCGS-A enterprise to answer the BCT's intelligence gaps. The S-2 section may also maintain hardcopy maps and overlays as directed by the command or as analog backups to the digital graphics. Whether digital or analog, the S-2's situation graphics and map overlays must be compatible with the S-3 operations graphics.

2-53. The S-2 staff may not post each report or image to the situation map. As the S-2's primary analysis and presentation tool, the S-2 section must have procedures in place to keep the situational graphics updated and free of irrelevant data. The brigade commander and staff must be able to see the disposition of organic ISR assets and the key indicators of threat activity, capability, and intentions that affect the current operation and commander's decision-making capability.

2-54. The S-2 staff maintains only mission-essential digital and analog charts on the threat and ISR operations. Time spent maintaining information with no apparent value is time taken away from the analysis effort. The section uses the information that resides within the JCDB and Analysis and Integration Platoon's intelligence databases to create charts as required. This information allows the brigade commander and other staff members to quickly assess the strength of the threat in relationship to the current friendly disposition on the S-3 operations map.

Synchronizing Plans and Operations

2-55. The S-2 must ensure that S-2 operations, S-2 plans, and the MI Company know the brigade's mission, the commander's intent, the PIR, EEFI, and the ISR scheme of support. The S-2 provides additional guidance, as necessary, to expand upon the ISR elements of the OPORD. The S-2 works with other brigade staff elements to consider branches and sequels to the planned operation as well as to integrate emerging staff requirements into the current operations. The S-2 reviews the ISR plans of supporting ISR organizations to ensure these plans remain synchronized with the tactical operation and ISR scheme of support.

Identifying Gaps and Requirements

2-56. During ISR planning the S-2 must identify gaps in intelligence knowledge and areas of coverage. As the ISR plan is developed, the S-2 must ensure that it addresses these specific areas as well as other concerns directed by the commander. The S-2 must constantly compare the IPB templates being developed by the S-2 staff with the current situation. Doing this will reveal gaps in the ISR plan and current plan and current ISR operations that could require the development of additional ISR tasks, reallocation of ISR assets, data mining activities, or requests for EAB support. As these gaps are identified, the S-2 ensures that appropriate collection tasks and requests are coordinated through the S-3. The MI Company is the principal organization that assists the S-2 in fulfilling this responsibility.

EXECUTING OPERATIONS

2-57. During execution, the S-2 section assists the commander and brigade staff in timely decision making and battlefield visualization by providing information about the threat, friendly ISR operations, and the environment in the AO. The S-2 ensures the commander has the most up-to-date, accurate intelligence to make such decisions and that the commander understands the implications of that intelligence for the operation.

Monitoring Operations

2-58. The S-2 operations team ensures graphical depictions of the current situation are accurate and up to date to facilitate the commander and staff's situational understanding and battlefield visualization, thereby supporting timely decision making and reducing risk and uncertainty while executing the brigade's plan. As previously mentioned, situation development builds upon the IPB analysis and products developed during planning. The S-2 operations team uses situation development to—

- Answer the commander's PIRs.
- Confirm or deny predicted threat COAs or other threat intentions.
- Explain threat actions in relationship to the current friendly operation.
- Validate planning assumptions from the assessment.
- Recognize opportunities for exploitation.
- Identify triggers for branches and sequels.
- Recommend changes to ISR coverage.
- Look for indications of radical changes in predicted threat COAs that could require the S-2 to recommend to the commander that the brigade significantly alter the current mission or begin a new planning cycle.

2-59. Indicators are the basis of the S-2 operations team situation development; and the situation graphic is the team's primary tool. The operations team integrates relevant information and intelligence products from all available sources to identify indicators of threat activities. Using these indicators, it answers the commander's PIRs and provides insight into the predicted COA. The S-2 operations team's situation graphic provides the S-2 and the team with a tool for identifying, tracking, and analyzing the indicators as well as recognizing new information of uncertain meaning. The graphic also provides a visualization and dissemination mechanism for the intelligence portion of the brigade's COP.

Synchronizing Operations

2-60. The brigade's decision support template, synchronization matrix, and ISR synchronization plan are based on assumptions about threat COAs and the dynamics of the operation. Sometimes the threat executes a COA not completely anticipated during wargaming or the operation's dynamics lead to unexpected branches and sequels. The warfighting functions synchronization matrix serves as the foundation for initiating orders and identifying the framework for synchronizing plans and operations for a particular COA. Each warfighting function is listed and the specific activity, events, status, or functions to take place is clearly delineated. This ensures a near seamless mission execution.

2-61. To anticipate the changes that such events dictate, the brigade staff uses staff meetings (sometimes called huddles) and operation update and assessment briefings to continually reevaluate assumptions and to reinitiate the IPB and MDMP as necessary. When the executive officer (XO) identifies conditions that require the plan to be revalidated or refined, the XO initiates a meeting or operation update and assessment briefing. Other staff members may recommend a meeting or operation update and assessment briefing based on their assessment of the situation. The S-2 prompts these sessions whenever the S-2 develops intelligence that runs significantly counter to planning assumptions. The S-2 section normally conducts a meeting with key leaders to discuss priority of effort as part of its shift during continuous operations. (See FMI 5-0.1 for more information regarding CP and staff operations.)

2-62. The S-2 usually begins the meeting or operation update and assessment briefing by discussing the current state of the common understanding of the battlefield. The S-2 reviews the predicted threat actions or COAs that the S-2 operations team has confirmed or denied. The review usually deals with threat COAs but also might address assumptions about the terrain, weather, or other factors that affect both friendly and threat operations. The S-2 follows the review with a full discussion of the emerging threat picture or action that led to the XO's calling the session. The S-2 emphasizes the significance of the intelligence in terms of what the threat COA indicates or fails to indicate. The S-2 should then present an informal, revised set of threat COAs that account for the new intelligence. The revised COAs usually result from an abbreviated IPB process that the S-2 section may have executed in only a few minutes.

2-63. If the new intelligence is too contrary to the original IPB, the commander may want to initiate a completely new planning session. Otherwise, the personnel present at the meeting or operation update and assessment briefing modifies the current plan based on the revised IPB. Because time is usually limited during an operation, the staff follows an abbreviated form of the MDMP and ISR planning. The S-2 requests support or retasks ISR assets in accordance with the revised ISR plan integrating new tasks into ongoing operations whenever possible. The S-2 prepares and the S-3 issues a FRAGO to incorporate new tasks to subordinate units.

2-64. The brigade XO holds a operation update and assessment briefing as required. The brigade commander or XO convenes a staff meeting at any time that the operation begins to deviate from the plan. The S-2 section conducts shift change briefings and numerous meetings during an operation to review the current situation and the "health" of its current plans.

Directing Action

2-65. As staff members track the battle, they refer to the DST and synchronization matrix to determine which decisions are coming due. The S-2 operations team looks at the intelligence synchronization matrix to determine which ISR assets owe the information and intelligence that will enable the decision to be made

in a timely manner. The S-2 operations team, through the ISR requirements manager, may have to re-prompt the ISR asset to the upcoming intelligence requirement. This is especially true if the course of the operations is occurring faster than anticipated.

2-66. As the ISR assets report, the S-2 operations team and the ISR requirements manager evaluates the report and analyzes the threat situation to determine if decision criteria have been met. If not, the RM team coordinates with the S-3 to retask the collector or makes an assessment based on available information. As each decision criteria is satisfied, the S-2 operations team and the ISR requirements manager refers to the decision support template and warfighting functions synchronization matrix to ensure that all decision makers receive the appropriate intelligence.

Making Recommendations and Decisions

2-67. The S-2 may recommend refocusing the ISR effort when the threat situation changes, an ISR task is satisfied, or the brigade executes a branch or sequel. Some changes to ISR operations are beyond the S-2's ability to influence through routine management. The S-2 must provide the commander with recommendations regarding—

- Additional intelligence resource requests from EAB or repositioned organic ISR units.
- ISR operations for which the S-2 lacks the resources or authority to direct.
- The commander's intent to facilitate future operations.
- The advantages, disadvantages, risks, supportability, and overall impact on the brigade's operations.
- Action intervention that is not in the S-2's delegated authority to task.
- Resources for commitment or acquisition which are not under the S-2's control.
- Changes to the scheme of ISR support.

2-68. See FM 5-0 and FM 6-0 for additional information on staff duties and responsibilities during planning, preparing for, and executing operations.

This page intentionally left blank.

Chapter 3

Plan and Prepare Intelligence, Surveillance, and Reconnaissance Operations

The CCIRs must not only be stated by the commander but also be anticipated by the staff. The BCT S-2 must anticipate the commander's PIRs to help drive the planning and directing of ISR operations. The S-2's requirement management techniques focus the collection, processing, and intelligence production on the critical needs of the commander. The intelligence staff assists the commander with battlefield visualization by identifying feasible threat capabilities; confirming or refuting the threat's COAs; and providing accurate descriptions of the effects of the operational environment on friendly and threat activities. In the BCT digital TOC, the C2 system enables a near-continuous assessment of the operations cycle. The S-2's role in ISR synchronization and ISR operations is a continuous activity to obtain information and produce intelligence essential to the commander's decision making.

OVERVIEW

3-1. Planning involves activities that identify IRs and develop the means for satisfying them. The CCIRs drive the planning for the ISR effort. Planning involves identifying, scheduling, and controlling ISR assets and resources. The S-2 and the intelligence staff review mission requirements for sensor and target range, system responsiveness, timeliness, threat, weather, and reporting requirements. These elements are considered with the detailed technical, administrative, and logistical data of the ISR asset to identify and determine asset and/or resource availability and capability. The requirements are then translated into specific mission orders that are forwarded to the S-3 for inclusion in OPORDs and FRAGOs.

3-2. Effective coordination is vital in mission planning operations. With aerial systems in particular, many different staff elements are involved. Operations, weather, maintenance, logistics, and communications must all be closely integrated into the mission planning effort. Planners and managers must fully understand the requirements and mission profile. The intelligence staff must work closely with the ISR unit commander and staff to enable the dynamic tasking of ISR assets.

3-3. Once an information requirement (IR) has been identified, validated, prioritized, and coordinated between the S-2, S-3, and other appropriate agencies (as required), the brigade orders the subordinate units to carry out the ISR mission. This is normally done through an order or tasking message that contains information the tasked unit needs to execute the mission. It also contains the requester's identification so that the ISR unit can report directly to the requesting unit. ISR orders are normally included in paragraph 3 of the base OPORD, as well as in annex B (Intelligence) and annex L (ISR). Annex L has the ISR tasks, and annex B has the intelligence production requirements.

3-4. Commanders and staffs must be fully aware of the rules of engagement (ROE) restrictions when conducting ISR operations. Tasking normally conforms to the principles of control in that a unit generally tasks one echelon down and tracks units two echelons down. The tasked unit makes the final choice of specific platforms, equipment, and personnel based on operational considerations such as maintenance schedules, training, and experience.

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

3-5. Planning and preparing intelligence operations begins when the commander presents his or her initial assessment and guidance to the staff, following receipt of mission from higher headquarters. The commander's guidance identifies critical information needs regarding the friendly forces, the threat, and

other conditions of the operational environment. Expressed in later steps of the MDMP as the CCIR, these requirements identify the PIRs or critical pieces of intelligence that the commander must know about the threat and other conditions of the operational environment by a particular time to successfully plan, prepare, execute, and assess operations.

3-6. Critical information directly affects the commander's decisions and the successful execution of operations. Critical information requirements (IRs) are based on predictable events or activities that are linked directly to the current and future tactical situation. The commander alone decides what information is critical based on the mission, staff input, the higher commander's intent, and his or her experience and estimate of the situation. CCIRs consists of PIRs and friendly forces information requirements (FFIRs). These assist the commander in controlling the collection and flow of critical information. EEFI are critical to the CI mission because they are the critical aspects of friendly information that would, if known by the threat, compromise, lead to failure, or limit the success of friendly operations. EEFI are not part of CCIRs but they become a commander's priority when the commander states them. Figure 3-1 depicts CCIRs.

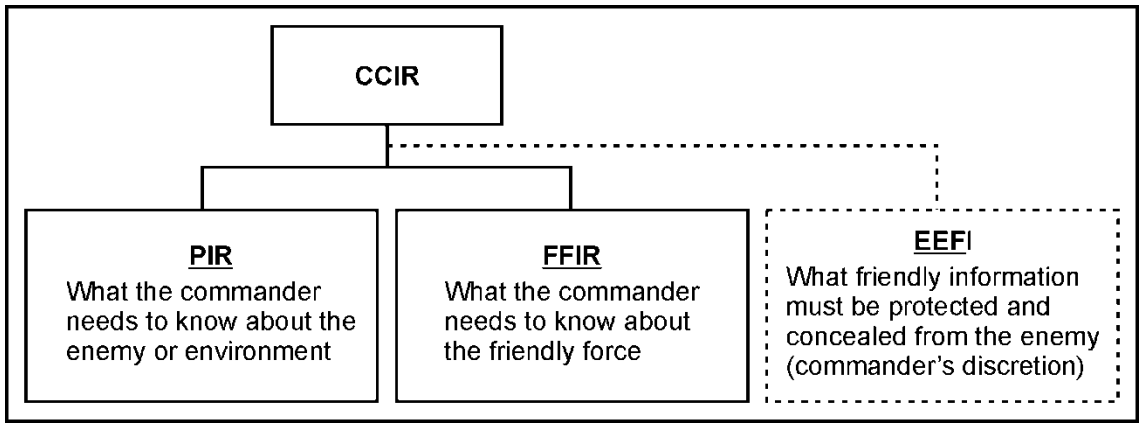


Figure 3-1. Commander's critical information requirements

3-7. Civil affairs (CA) and S/G-9 personnel analyze the level of satisfaction or dissatisfaction of the various population factions to assess the threat to the US and allied forces and mission accomplishment. During stability operations and civil support operations, the focus concentrates less on conventional military capabilities and vulnerabilities and more on the six ASCOPE categories: areas, structure, capabilities, organization, people, and events.

3-8. A significant amount of information and intelligence is collected on the characteristics of the operational environment, to include—

- Press coverage and threat propaganda.
- Sympathies and reactions of local population and organizations to friendly operations.
- Local economy, including "black markets."
- Local legal system.
- Unofficial organizations including clans and tribes.
- Local government including official parties, meeting sites, activities, contentious issues.
- Paramilitary organizations and police forces.
- Governmental and nongovernmental organizations (NGOs) that may interact with the friendly forces during execution of the mission.

3-9. CA and S/G-9 personnel gather information about what a population is experiencing, determines any shift in the population attitude and behavior, and identifies issues that may cause the population to "flash" or adversely react to the presence or efforts of the multinational forces. They use any reliable sources that can provide information related to an issue in the AO. Perceptions, whether based on truth or false impressions or information, must be assumed to be true motivators for actions and reactions within

populations. CA personnel watch the local environments and look for those issues that continue to be reported and those issues which are causing or likely to cause populations to move on the continuum of violence. Collecting relevant civil information and having it readily available is crucial to being able to paint the civil-military operations (CMO) battlefield. Figure 3-2 shows the continuum of satisfaction and action.

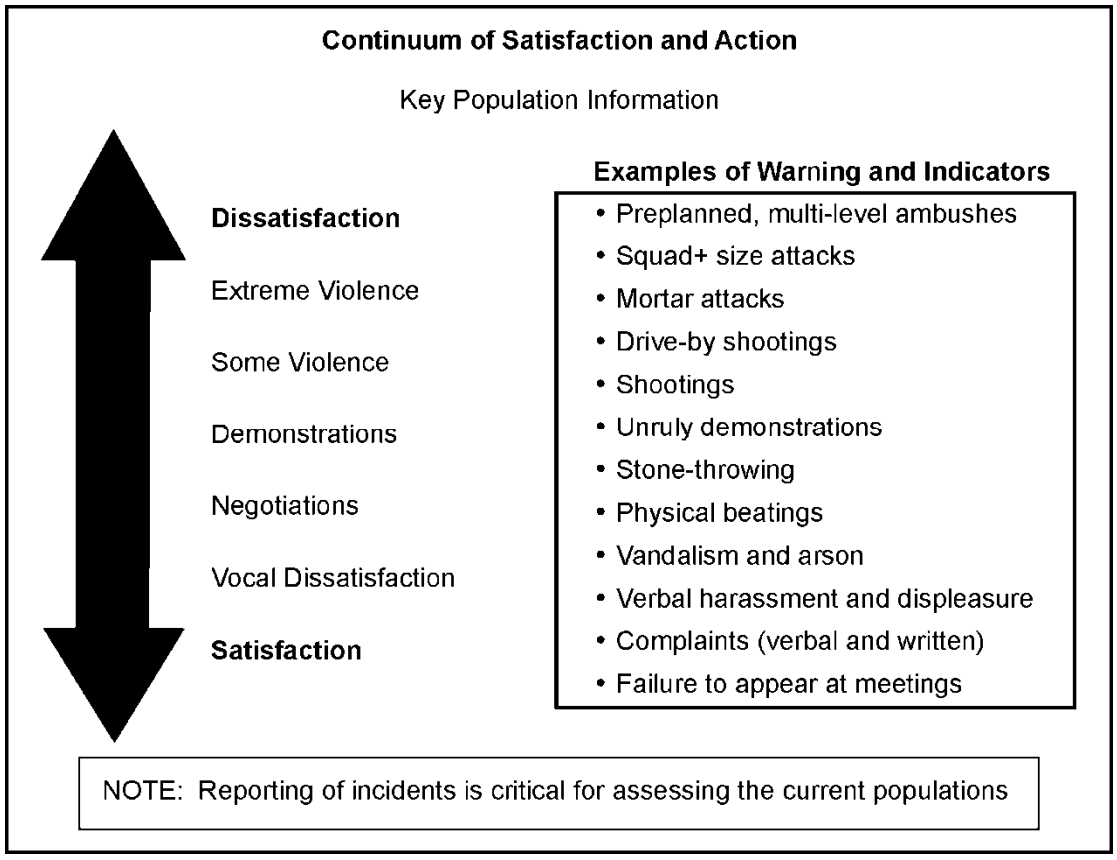


Figure 3-2. Continuum of satisfaction and action

3-10. IPB products and ISR planning are especially critical in the MDMP. Both require cooperation between the commander, the intelligence staff, and other staff elements to ensure the unit's operations are well planned and supported with effective intelligence operations.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

3-11. IPB is a systematic and continuous process for analyzing the threat and environment in a specific geographic area. It is a staff planning activity undertaken by the entire staff to define and understand the operational environment and the advantages and disadvantages presented to friendly and threat forces. IPB supports each staff section's running estimates and the MDMP. The IPB process helps the S-2 support the commander in employing and protecting the commander's combat power at critical points in time and space on the battlefield. The S-2 uses IPB to describe the environment in which the brigade is operating and the effects of the environment on brigade operations. The IPB process supports the S-2 in determining threat capabilities, objectives, and COAs. The S-2, supported by the Analysis and Integration Platoon, conducts IPB prior to and during the brigade's planning for an operation. The IPB process consists of four steps:

- Define the Operational Environment.

- Describe Environmental Effects on Operations.
- Evaluate the Threat.
- Determine Threat COAs.

DEFINE THE OPERATIONAL ENVIRONMENT

3-12. IPB begins with the receipt of a contingency plan (CONPLAN) or OPLAN. Defining the operational environment step includes recognizing and understanding the AO, AOI, and operational environment. The operational variables (PMESII-PT) are analyzed to develop information and insights to define the operational environment. As a set, the operational variables are abbreviated as PMESII-PT; a description of each of the operational variables follows:

- Political. Describes the distribution of responsibility and power at all levels of governance or cooperation.
- Military. Explores the military capabilities of all relevant actors in a given operational environment.
- Economic. Encompasses individual behaviors and aggregate phenomena related to the production, distribution, and consumption of resources.
- Social. Describes the cultural, religious, and ethnic makeup within an operational environment.
- Information. Describes the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information.
- Infrastructure. Is composed of the basic facilities, services, and installations needed for the functioning of a community or society.
- Physical Environment. Defines the physical circumstances and conditions that influence the execution of operations throughout the domains of air, land, sea, and space.
- Time. Influences military operations within an operational environment in terms of the decision cycles, operational pace, and planning horizons (FM 3-0).

3-13. Upon receipt of a WARNO or mission, Army leaders narrow their focus to six mission variables (METT-TC). Mission variables are those aspects of the operational environment that directly affect a mission.

3-14. The BCT AO will be identified in the OPORD or OPLAN. The AOI's limits are based upon the commander's guidance, the AO, and the operational environment. If the commander has not designated an AOI, the S-2 works with the S-3 to identify the command's AOI during the MDMP. The S-2 uses this area to focus the analysis effort on the geographic areas of significance to the brigade's mission.

3-15. The BCT higher headquarters will determine the brigade's AO. If the BCT's higher headquarters did not assign an AO, the S-2 coordinates with the S-3 to develop a recommendation on the AO for the commander's approval and submission to higher headquarters. The BCT commander is responsible for the provision of intelligence within the AO. The BCT commander is responsible for collecting information concerning the threat and other conditions of the AO, as well as analyzing that information to produce intelligence.

- The brigade S-3, in coordination with the S-2, assigns AOs to subordinate units. Subordinate unit AOs may be contiguous or noncontiguous (see figure 303). A common boundary separates contiguous AOs. Noncontiguous AOs do not share a common boundary; the concept of operations provides procedural control of elements of the force.

3-16. Defining the significant characteristics of the AO and AOI also aids in identifying gaps in current intelligence products and the specific intelligence requirements to fill them. The S-2 staff conducts data mining to answer intelligence gaps. DCGS-A allows the BCT S-2 access to required information on the Intelligence Enterprise. Once approved by the commander, these gaps become the commander's initial intelligence requirements.

3-17. The S-2 staff element is the proponent for IPB; however, the entire staff participates in the process. IPB includes input from the staff elements in order to create the most complete picture of the battlefield

possible. The staff assists the commander in recognizing and anticipating battlefield events so that the commander can make better decisions and act on those decisions quickly. The staff provides the commander with a timely and accurate synopsis of the current COP. Once the commander makes a decision, the staff coordinates and synchronizes supporting actions and supervises preparation and execution to ensure that functional responsibilities are carried out within the commander's intent. The BCT HHC has an increased staff and enhanced C2. The BCT staff has embedded liaison officers (LNOs).

3-18. Step 1 of the IPB process focuses the brigade's initial planning efforts and the remaining steps of the IPB process. The S-2 leads the staff in identifying characteristics of the AO and AOI which require in-depth evaluation of their effects on friendly and threat operations, such as terrain, weather, and civil considerations.

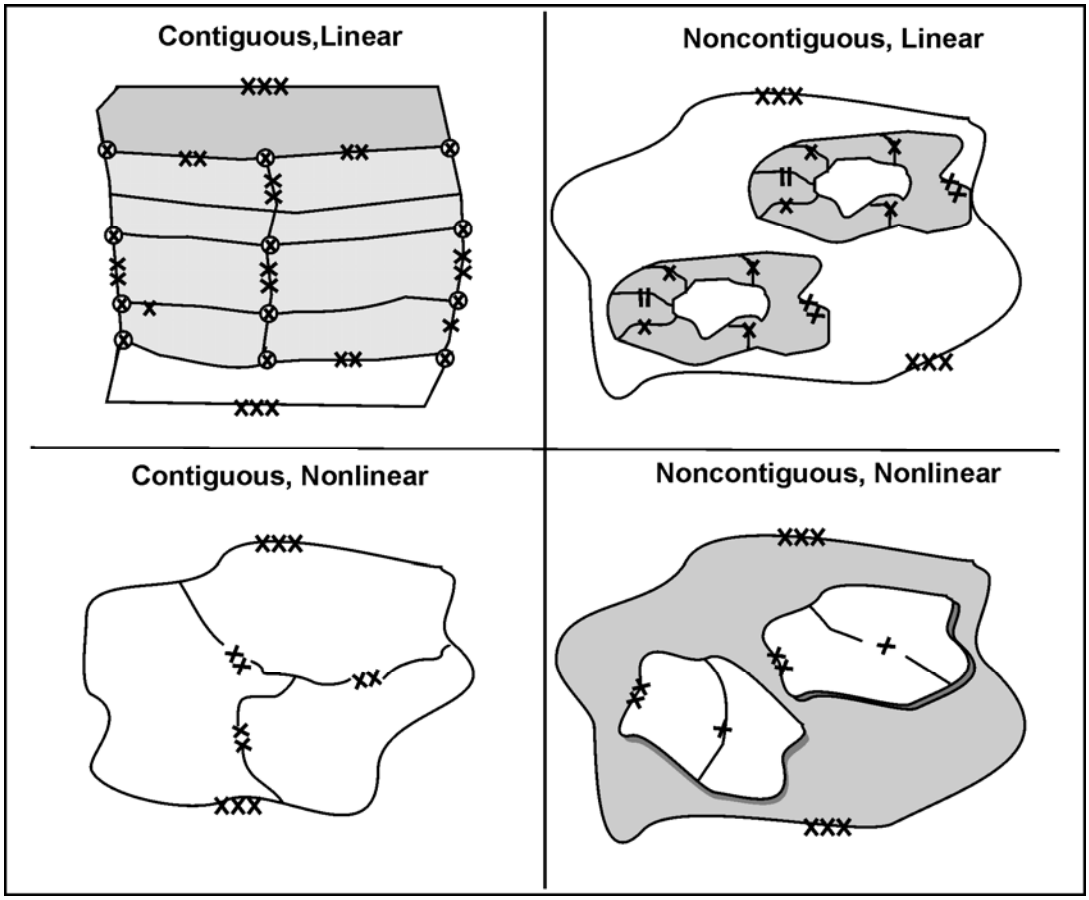


Figure 3-3. Area of operations

3-19. Different types of operations may require different types of products. A variety of these products are detailed below. These products may be used individually or combined, as the mission requires. Many of the products listed will be created in conjunction with multiple staff elements.

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

3-20. In this step of the IPB process, the S-2 analyzes the effects of the terrain, weather, and civil considerations with which US forces, allies, threats, and noncombatants must contend. The S-2 identifies the limitations and opportunities the environment offers to potential operations of friendly and threat forces. This analysis focuses on the general capabilities of each force until COAs are developed in later steps of

the IPB process. Regardless of the subject or means of presentation, the S-2 ensures that the analytic focus is on the environmental effects. Products developed in this step might include, but are not limited to—

- Population status overlays.
- Overlays that depict the military aspects and effects of terrain (for example, LOC, line of sight, imagery, urban terrain, key infrastructure, congregation and mass assembly points overlays).
- Weather analysis and forecast matrices.
- Integrated products such as modified combined obstacle overlay (MCOOs).

3-21. Just as traditional IPB paints the picture of potential enemy actions across the battlefield; the CMO IPB paints the picture of the threats to US mission due to infrastructure problems and the populace sentiment when analyzing civil considerations in this step of the IPB process, the S-2 examines the ASCOPE and their effects on friendly and threat operations. Figure 3-4 shows examples of ASCOPE.

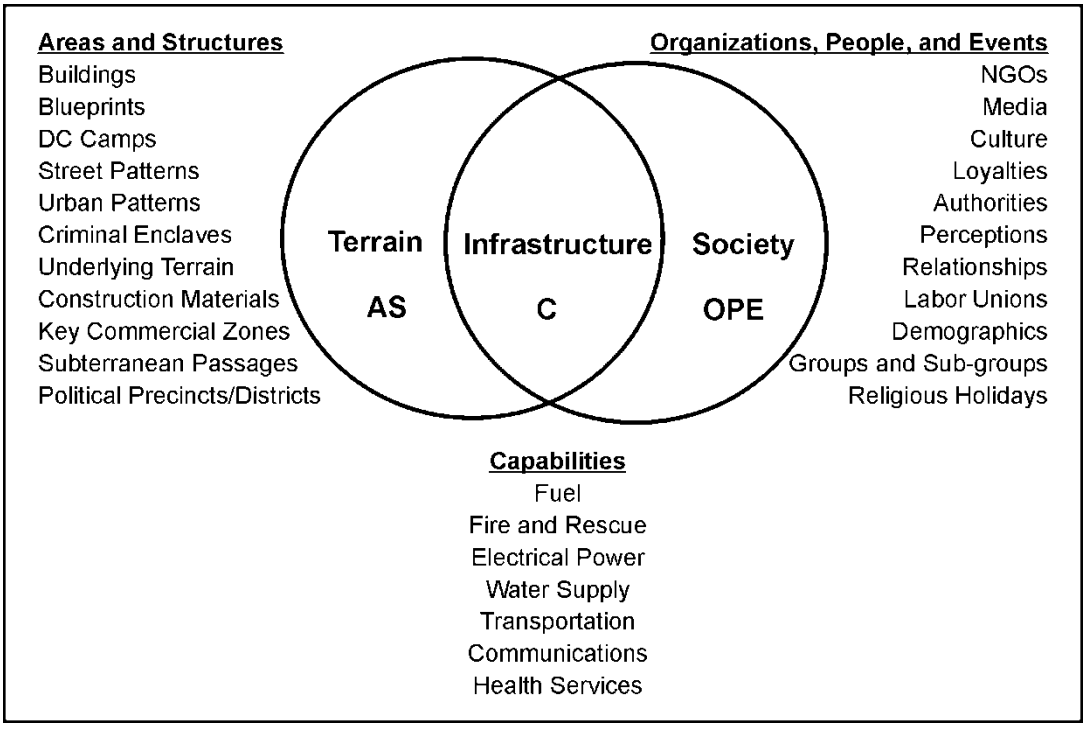


Figure 3-4. Areas, structures, capabilities, organizations, people, and events

Population Status Overlay

3-22. Population status overlays are a group of products rather than a single product. These products depict how the population of a designated area is divided based on a single characteristic such as age, religion, ethnicity, or income. For instance, one population status overlay can show what areas of a city are Catholic, Protestant, Muslim, Hindu, and so on. Another overlay can indicate income levels or areas of known gang membership. There is no limit to the number of overlays that can be created to depict the population characteristics of a chosen area. The benefits of these overlays range from determining possible lines of contention (that can exist between groups) or identifying the population or location in greatest need of a certain activity or asset. (Figure 3-5 is an example of a population status overlay.)

3-23. Many examples of this type of overlay are produced by the United Nations High Commission for Refugees and are readily available on its web site at http://www.reliefweb.com. Population status overlays and descriptions resulting from assessing the demographic characteristics of the host city population might

reveal significant differences between groups which can further enhance situational awareness and situational understanding.

3-24. These overlays can be useful in identifying critical areas of the AOs based on cultural factors such as ethnic breakdown, tribal affiliation, or religious breakdown. One common method of constructing these overlays is to color code sections of an AO based on the majority identifications of that area. This, however, can be misleading in some situations; an alternative method that more accurately reflects the information that needs to be conveyed to the commander may be necessary. An alternative method may entail dividing the AO into specific areas such as the same service or political boundaries that local authorities use—like the local police precincts, municipal districts, or counties—which can often help clarify the situation as well as aid in coordination efforts with the local authorities and then inserting pie charts for each AO showing each group and numbers and/or percentages.

3-25. Population dispersal can vary significantly throughout the day. Another type of population status overlay could indicate the location of population groups during the day, and how this changes over time. This could assist in identifying possibly restrictive operating conditions or reveal times that are most conducive for completion of a given mission.

Lines of Communication (LOC) Overlay

3-26. LOC overlays identify the major LOCs within and around an AO. This includes roads, airfields, mountain passes, waterways, and foot paths. In stability operations and civil support operations, more advanced versions of these overlays can be combined with the traffic conditions overlay and long-term surveillance of LOCs to determine what LOCs are most heavily traveled at different times of the day. Threat forces can take advantage of higher volumes of civilian traffic to use these LOCs for their own purposes.

3-27. These overlays can provide mobility information to assist planners and operators in determining what personnel and equipment can move along the mobility corridors. Pertinent data would include road widths, their load capacity, sharp turns, potential ambush positions, potential sniper positions, and overhanging obstacles.

3-28. In urban operations, creating an LOC overlay that depicts normal traffic conditions can help the unit determine best times to operate. It can also provide an indicator of an unusual event. Even though aerial surveillance can detect heavy traffic and traffic jams, it cannot predict when or why they occur or whether or not they were part of the normal traffic pattern in the urban area.

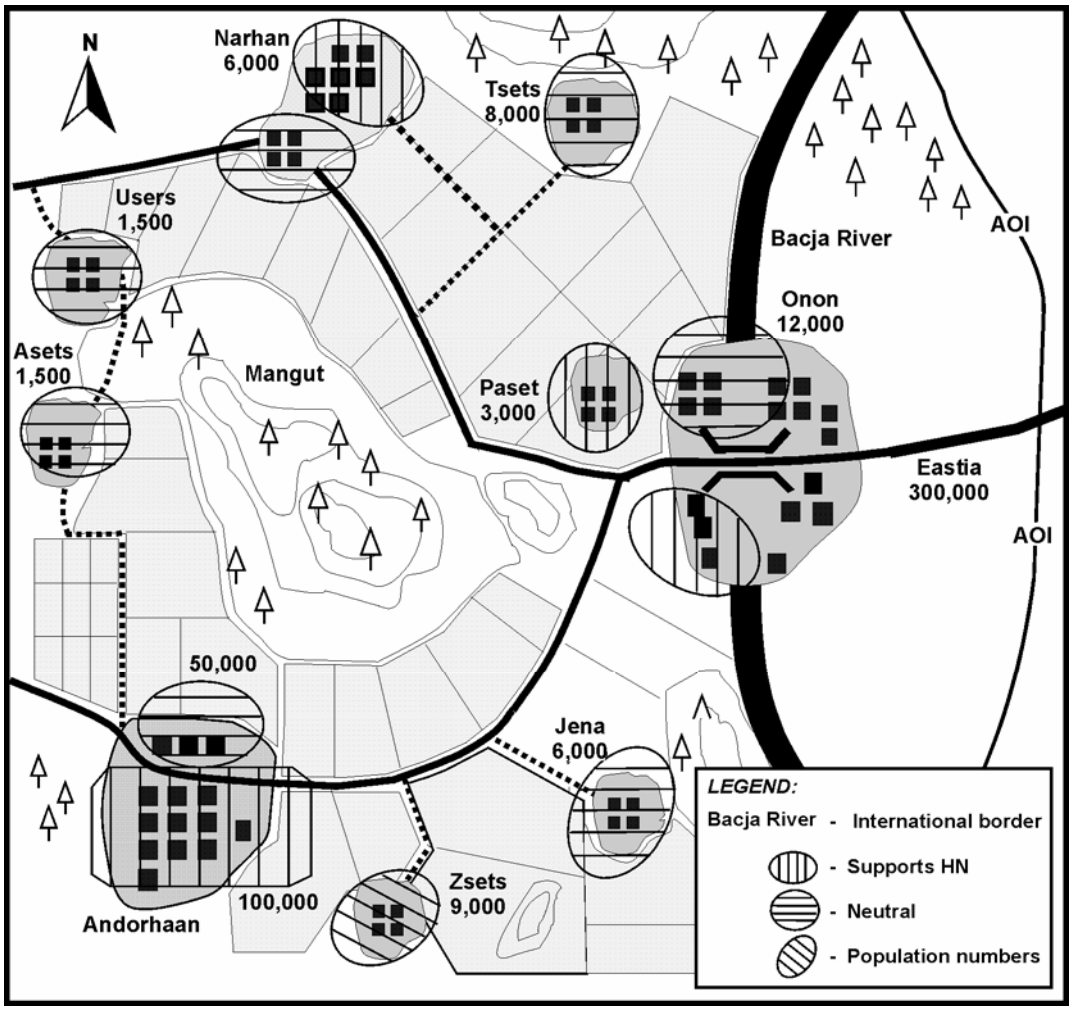


Figure 3-5. Example population status overlay

3-29. Waterways can play a significant role in an AO. Among other things, they can be obstacles or LOCs for infiltration of enemy forces or illicit traffic (for example, arms smuggling, drug smuggling, and black marketeering). An overlay of local water systems can list such important items as the width and depth of the waterway, key crossing sites (depending on the size of the waterway), and key uses of that waterway (such as commerce, water source for crops, drinking water source for the local population).

Line of Sight Overlay

3-30. Perhaps even more important in the complex terrain than in non-complex terrain, line-of-sight overlays can help define avenues of approach (AAs) to an objective. Just as important are reverse line-of-sight overlays that show the friendly AAs from the enemy standpoint. We can expect the enemy to try to cover dead space from the objective area with other positions or devices such as mines or improvised explosive devices (IEDs). If the enemy on the objective simply wants to flee, dead spaces may simply be covered by some type of early warning system.

3-31. Line-of-sight overlays can help pinpoint potential observation or sniper positions along each relevant AA based on the best possible locations given line of sight, elevation, exposure, and other pertinent

considerations. These positions are important because friendly forces can position personnel at these locations to secure them or observe from them as readily as threat forces.

Imagery Overlay

3-32. Imagery is important in the analysis of any situation. Imagery products include both aerial photography and satellite imagery. In many cases, tasked aerial reconnaissance platforms, such as unmanned aircraft systems (UASs), respond directly to the commander, thus ensuring timely and focused data collection. Because of technical limitations or priorities established at the higher echelons, space-based and other national collection assets may not be available to the commander and staff. Additionally, as each collection system has its own unique capabilities, traditional black and white or infrared imagery may offer the best view of the target in a given situation.

3-33. A key element in future operations may be the real-time imagery downlink capabilities of space-based intelligence collection platforms. Space-based systems can provide important information on employing state-of-the-art multispectral, infrared, earth observing-1 (EO-l) imagery, and synthetic aperture radar (SAR) imaging. Additionally, DCGS-A provides the S-2 access to tactical, theater, and national imagery systems as well as the Image Processing Library. Data collected from such sources are transferred in digital format, which then can be manipulated to address specific requirements. Intelligence staffs must be fully aware of the capabilities and limitations of these systems as well as the procedures necessary to request this support.

3-34. Advanced Geospatial Intelligence products are produced using any combination of imaging platforms: visible, infrared, radar, or spectral depending on the requestor's needs. Due to the versatility of these products, they have a wide range of applications. Presenting imagery in an oblique perspective by combining it with digital terrain elevation data provides a perspective view. Using spectral imagery can accomplish discovery and identification of manmade and indigenous activity from patterns of heat distribution and determination of changes in a scene imaged at various times. Other uses include facility analysis, structural analysis, target detection, soil analysis, and damage assessment.

Urban Terrain Overlay

3-35. In the current operational environment, the potential for conducting operations in and around urban areas is very high. Various urban-related products can help bring order to the massive amounts of information required in an urban environment.

3-36. Urban terrain overlays depict specific aspects of terrain unique to the urban environment. These overlays can depict the details of a single building, a group of buildings, a section of an urban area, or even an entire urban area. This type of overlay can also depict the different terrain zones apparent in an urban area. Different types of terrain could be indicated using hatch marks or other indicators on a map or aerial photograph. Zone types may be defined as close, orderly block, or dense random construction (as they are in FM 3-06), or by any other designated characteristics required by the mission, such as zones of threat occupation or zones divided by the types of predicted weapons effects.

3-37. A building type overlay can depict particular types of buildings, such as industrial buildings, government buildings, military buildings, residential areas, businesses, warehouses or storage buildings, religious centers, or media locations. Each of the buildings can be numbered or otherwise identified depending on the needs of the commander and the commander's staff. Additionally, entire sections of a city can be marked depending on the construction type prevalent in a particular area. For instance, an area of dense construction or a shantytown can be identified by appropriately labeling it on an overlay or directly onto an aerial photograph.

3-38. Shantytowns may need to be specifically highlighted because they may be areas with notable food shortages and where disease and pollution are most prevalent. Shantytowns may lack public utility infrastructure (for example, plumbing and electricity). Buildings are often made from miscellaneous materials, and there is no consistent pattern of streets or corridors, complicating military operations. These

types of conditions result in a concentration of population that is generally dissatisfied and is a potential source of unrest.

3-39. Unoccupied locations or buildings should also be identified. These locations or buildings can be used as shelter for troops (friendly or threat) or as locations for friendly forces to demonstrate firepower if necessary. The latter utility was demonstrated in Kosovo when a tank round was shot into an unoccupied building in order to quell an increasingly worrisome civil disturbance. Additionally, unoccupied locations or buildings could be logistics storage sites or meeting sites for threat forces.

3-40. An overlay depicting street widths in terms of major weapon systems can help identify which formations or routes are most advisable for an area. A street wide enough to allow two Abrams tanks to advance side by side enables the vehicles to better cover upper floors on opposite sides of the street, thereby providing security for each other. Also, depicting buildings that exceed the depression or elevation capabilities of vehicle weapons systems can identify areas of concern and potential enemy ambush positions. Routes with such "dead spaces" may enable convoys with additional or alternative weapons systems to eliminate this vulnerability.

Key Infrastructure Overlay

3-41. These overlays depict the locations of key infrastructure in an urban environment. Like population status overlays, this type of overlay is a group of products rather than a single product. These overlays can be produced by using a map, aerial photography, or graphic design that is appropriately marked with a numbering or a color-coded system that indicates the type of asset as well as its specific attributes.

3-42. Key infrastructure required to sustain a city can be used as a tool of warfare both in the physical and information domains. Securing key infrastructure from destruction will often be critical in gaining and maintaining a positive perception of friendly forces by the local populace. The most important part of the key infrastructure is the critical infrastructure. This may include electricity generation plants, government buildings, hydroelectric dams, oil pumping stations, police stations, public markets, pumping stations, water purification plants, sewage treatment plants, and anything that, if harmed, can affect the living conditions of the population.

3-43. Key infrastructure overlays can be useful for identifying protected urban terrain. Protected terrain encompasses areas that should not be destroyed, attacked, or occupied, or that have other use restrictions based on international treaties, ROE, and common sense—such as schools, hospitals, areas with large amounts of phone and/or electrical wiring, and buildings with many stories. For example, medical facilities may be depicted on their own key infrastructure overlay. Medical facilities are generally no-fire areas for friendly forces and should be protected from damage or destruction so that they can continue to take care of the local population once friendly forces have secured the urban area. Inadequate health care for the local population can lead to both a negative perception of friendly forces and an uncontrolled increase in disease which can affect friendly forces personnel working in the urban environment directly.

3-44. Other types of key infrastructure overlays may depict media facilities, transportation facilities, resource sites, culturally significant structures, dangerous facilities, or subterranean infrastructure. Media facilities include locations of transmission stations, antennas, newspaper production and distribution sites, and television and radio stations. Transportation facilities include rail hubs, major bus connection sites, subway lines, freeways, major thoroughfares, and intersections that are significant to the operation. A resource sites key infrastructure overlay can depict locations where resources or supplies can be obtained, such as building material locations, car lots, and appliance warehouses. This can include petroleum and natural gas processing plants. Generally, these are the resources and infrastructure that are used to support the critical resource needs of a population.

3-45. A key infrastructure overlay could highlight culturally significant structures such as places of religious worship (for example, churches, temples, mosques), all relevant government buildings and internationally significant buildings (for example, embassies, consulates), and other structures or areas of notable cultural importance. A key infrastructure overlay of dangerous facilities could depict structures with known chemical, biological, or incendiary features. These are primarily toxic industrial material sites,

such as pharmaceutical plants, oil refineries, or fertilizer plants, but can include military-related areas like ammunition storage sites. Finally, an overlay depicting key subterranean infrastructure can include underground railways, sewer systems, electrical wiring, or any other underground feature of significance for the operation.

Congregation Points/Mass Assembly Points Overlay

3-46. Congregation points/mass assembly points overlays depict the numbers, types, and locations of sites where large numbers of people can be gathered for demonstrations, protection, or feeding in the event of a disaster. These sites may be depicted on maps of an urban area. These sites include places of religious worship, parks, schools, restaurants, squares, recreational centers, sports facilities, or entertainment centers. If normally used for large gatherings of people, these locations can also be coded with information on the population group that frequents them, days and hours of operation, and type of activity that occurs.

Weather Analysis Matrix

3-47. An integral element within the IPB process is weather analysis. Weather data pertaining to IPB is either climatological information or current forecasts. This climatological data is fused with terrain information to produce collaborative weather and terrain products. The SWO identifies the commander's requirements and must fully understand the mission as well as commander's intent. Discerning the threshold weather values that can affect BCT operations is identified through a weather factors/forecast matrix. The weather matrix identifies the specific operations the unit performs and is usually tailored for each type mission. Figure 3-6 is an example of a weather effects forecast matrix.

Modified Combined Obstacle Overlay (MCOO)

3-48. The MCOO forms the foundation for evaluating a geographic battlefield area. It fuses the combined obstacles overlay, AA overlay with mobility corridors, operational graphics, key terrain, and known threat objectives into a comprehensive terrain product.

EVALUATE THE THREAT

3-49. The S-2 analyzes the brigade's intelligence database to determine how the threat normally organizes for combat and conducts operations under similar circumstances. When facing a well-known threat, the S-2 can rely on historical databases and well-developed threat models. When operating against a new or less well-known threat, the S-2 may need to develop intelligence databases and threat models concurrently. The S-2's analysis is portrayed in a threat model that includes doctrinal templates that depict how the threat operates when unconstrained by the effects of the battlefield environment. Although they usually emphasize graphic depictions (threat templates), threat models sometimes emphasize matrices or simple narratives.

Weather Effects										
Operation		06-09	09-12	12-15	15-18	18-21	21-24	00-03	03-06	Comments
INTEL	EAC RECON									Transitional period between Northeast and Southwest Monsoons. Northeast Monsoons provide favorable weather for operations with decreased rain and thunderstorms. Also during the transitional period Tropical Cyclone frequency increases.
	TACTICAL RECON				C	C	C			
	UA - Hunter				C	C	C			
	UA - Predator				C	C	C			
	GROUND RECON									
MANEUVERABILITY (ARMOR/INFANTRY)					P	P				
AVIATION	HELO, CAS (A-10), C-130 (Non-AWADS)									
	CAS (Non A-10)									
	C-130 (AWADS)									
AIRBORNE OPS										
ARTILLERY/AIR DEFENSE										
ENGINEERS					P	P				
LASER/THERMAL				P	P	P				
MOPP IV			T	T	T	T	T	T	T	

LEGEND:
– Moderate degradation
– Severe degradation
T – Temperature
W – Wind
V – Visibility
P – Precipitation
C – Ceiling

Figure 3-6. Weather effects forecast matrix

DETERMINE THREAT COAS

3-50. The S-2 develops enemy COAs and prioritizes them in order of probability as the basis for determining IRs for ISR assets. The S-2 is the responsible staff officer to put the IPB together although the IPB is a collaborative staff effort. Every staff officer possesses specific information the S-2 can use to piece together the IPB. Table 3-1 lists examples of staff input to enemy COA development, enemy situation template, and event template development and reconnaissance objectives.

Table 3-1. Staff input to threat COAs

Staff	*Responsibility*
Air and Missile Defense	• Evaluate likely air corridors. • Determine likely timing of air fires, air assault, or airborne operations. • Determine likely targets and objectives of enemy air operations. • Evaluate how the enemy Air Defense Artillery (ADA) is organized to protect its forces • Evaluate if the enemy will use air in reconnaissance or counterreconnaissance roles.
Fire Support	• Determine where the enemy will deploy mortars or artillery. • Recommend HVTs (further develop into HPTs during wargaming). • Anticipate how deep their indirect fires can range.
Engineer	• Determine where the enemy is most likely to emplace both conventional (for example, mines) and unconventional obstacles (for example, IEDs). • Determine time— ▪ To emplace each type of obstacle. ▪ To breach or neutralize obstacles. ▪ For an enemy force to establish a given level of defensive preparedness. • Determine ability to bridge different size rivers and streams and time required for each. • Make an initial assessment of effort required for stability assessments, such as building construction.
Chemical, biological, radiological, and nuclear (CBRN)	• Determine types of delivery systems, including minimum and maximum ranges. • Appraise threat CBRN protection capabilities. • Provide indicators of preparations to employ CBRN weapons. • Predict friendly assets the enemy is likely to consider HPTs for CBRN targeting. • Analyze existing contaminated areas that may indicate COAs adopted by enemy.
Signal	• Determine the threat's ability to locate or intercept friendly systems. • Predict the speed with which the enemy can collect, process, and target communication and C2 sites. • Evaluate the threat's ability to link collection systems to indirect or direct fires. • Estimate the deployment patterns of SIGINT collection systems.
CA	• Analyze the political and economic situation in the AO. • Determine what factions are friendly, neutral, or threat. • Determine who the key leaders are. Provide what are the cultural indicators that identify the populace is friendly, neutral, or anti-US. • Predict areas that civilians gather to protest or demonstrate. • Determine from whom or where information can be gained on particular AOs.

3-51. The S-2 produces threat models and effectively forecast the threats COAs, when the S-2—

- Understands the friendly mission throughout the operation.
- Identifies the physical limits of the AO and AOI.
- Identifies the operational environment characteristics that might affect the operation.

- Identifies the opportunities and constraints of the operational environments offer to threat and friendly forces.
- Thoroughly considers what the threat is capable of and what the threat prefers to do in like situations.

3-52. In short, the threat COA models which drive the MDMP are valid only if the S-2 establishes a good foundation during the first three steps of the IPB process.

Enemy Situation Template

3-53. The S-2 develops an enemy situation template for the ISR operations that includes a focus on the enemy's reconnaissance and counterreconnaissance efforts. Figure 3-7 depicts an example of an unconventional situation template and figure 3-8 depicts an example of a conventional situation template. The enemy situation template is designed to aid in planning friendly infiltration and survivability by identifying enemy actions that will impact on friendly reconnaissance efforts. It also includes enemy main body activities required to focus the reconnaissance unit on the reconnaissance objective that they are collecting against. The enemy situation template should include—

- Locations of known and suspected enemy locations.
- Suspected enemy boundaries.
- Likely enemy reconnaissance and infiltration routes with time phase lines (TPLs).
- Likely enemy operations and patrols.
- Enemy mortar and artillery locations and range fans.
- Enemy air defense locations and range fans.
- Known and templated obstacles.

CONDUCT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

3-54. Conduct ISR is an activity that synchronizes and integrates the planning and operation of collection and processing systems in DS of current and future operations. ISR is an integrated intelligence and operations function. In the BCT, this activity is a combined arms operation directed by the operations officer at the brigade and battalion level supported by their respective intelligence officers. Through ISR, the BCT continuously plans, tasks, and employs collection assets and forces to collect and disseminate timely and accurate combat information and intelligence to satisfy the CCIRs and other intelligence requirements. ISR operations are fundamental to information superiority and support friendly operations through four tasks:

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

3-55. The brigade S-2 and S-3, along with the entire staff, are responsible for ISR synchronization and ISR integration to ensure the plan meets the operational needs of the commander. ISR synchronization and ISR integration are discussed below. Reconnaissance and surveillance are discussed in chapter 4.

PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION

3-56. **ISR synchronization is the task that 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.**
- **Submits RFIs for adjacent and higher collection support** (FM 3-0).

3-57. The intelligence staff, supported by the MI Company (and SBCT Reconnaissance Squadron), with staff participation, synchronizes the entire collection effort. This includes all the assets the BCT commander controls, assets of lateral units, higher echelon units and organizations, and intelligence reach into a unified effort. This is done through centralized planning and decentralized execution, which optimizes the integration of ISR operations into the commander's scheme of maneuver and fire.

3-58. The S-2, or requirements manager, produces the ISR synchronization plan. The ISR synchronization plan is often produced in conjunction with the S-3's ISR plan. The collection strategies, which are designed not only to collect the intelligence but also to deliver it on time are entered onto the ISR synchronization plan.

3-59. The BCT S-2 is responsible for ISR synchronization, a process that includes the six continuous activities illustrated in figure 3-7.

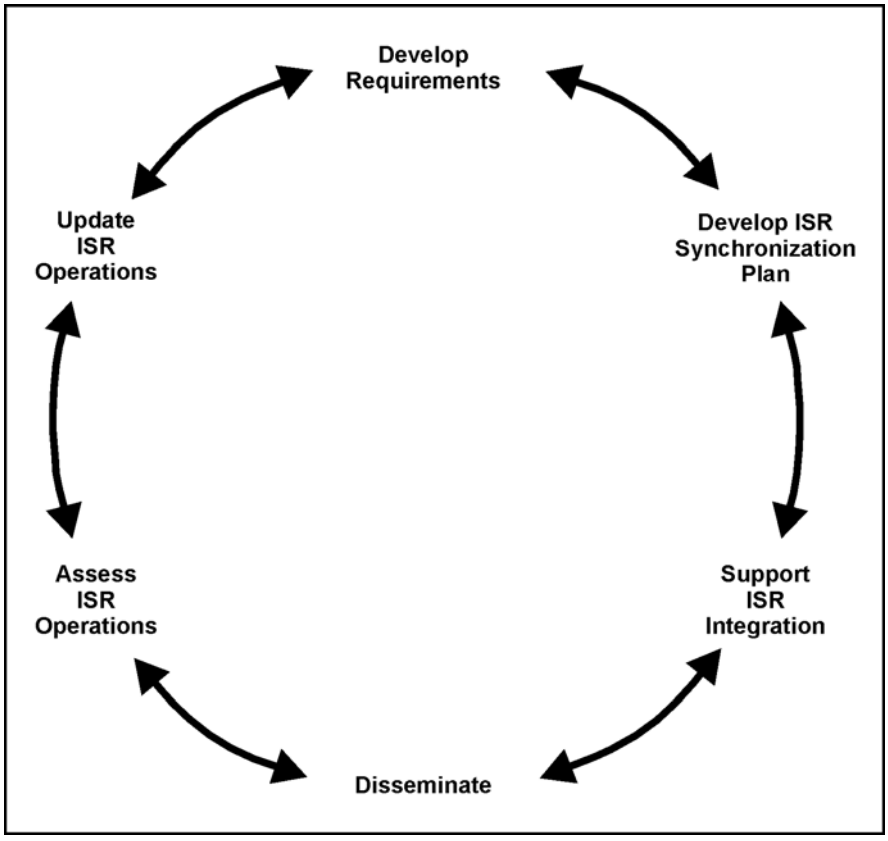


Figure 3-7. ISR synchronization activities

DEVELOP REQUIREMENTS

3-60. Developing requirements (requirements management) is the process of identifying, prioritizing, and refining gaps in data, relevant information, and knowledge concerning the AO and AOI that must be resolved in order for the commander to achieve situational understanding. Requirements are developed prior to conducting an operation and during ongoing operations. An important element in developing requirements is constant collaboration between all warfighting functions as well as the ISR Requirements Section of the MI Company's Analysis and Integration Platoon to redefine information requirements and

focus the ISR effort as the situation develops. While the rest of the staff contributes to this effort, the ISR Requirements Section is the primary element responsible for developing requirements during planning and steady-state operations. Using the commander's current stated requirements, the brigade mission statement, input from the brigade staff, and input from higher headquarters the ISR Requirements Section indentifies intelligence gaps and forwards them to the S-2 for consideration.

3-61. Because the ISR synchronization process is continuous and non-sequential, requirements are developed throughout the process and at all stages or phases of operational planning, preparation, and execution. The end state of requirements development is to produce new intelligence requirements that are developed from ongoing operations that will drive new operations, branches, and sequels. Effective requirements management depends on detailed IPB; this includes the maintenance of the intelligence running estimate, to include enemy situation templates and/or COA statements as well as the development of the event template or matrix. Timely development of the event template or matrix in accordance with the brigade battle rhythm is critical to the development of the decision support template, ISR synchronization plan, ISR overlay, and the execution of ISR operations.

DEVELOP INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION PLAN

3-62. The ISR synchronization plan (often depicted in matrix format) is a product the S-2 uses to ensure that collection tasks are tied to the brigade scheme of maneuver in time and space and to effectively link reconnaissance and surveillance to maneuver. Lessons learned from OIF and OEF show it is the easiest and most effective tool yet developed to synchronize ISR operations, proving to be very effective in identifying gaps in ISR coverage as well as communicating ongoing ISR operations to the commander and staff.

3-63. The ISR synchronization plan is typically constructed in matrix format. The S-2 uses the ISR synchronization plan to synchronize available assets to collect on CCIRs. The S-2 also uses the ISR plan, along with the ISR overlay, to brief ISR operations as required by the brigade battle rhythm. In support of the BCT S-2 the MI Company's Analysis and Integration Platoon develops and modifies the plan based on the current intelligence running estimate, enemy situation overlay, stated requirements, and event template or matrix. Figure 3-8 is an example ISR synchronization plan (in matrix format). Figure 3-8. Example ISR synchronization plan in matrix format.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1			ISR SYNCHRONIZATION MATRIX																								
2	DTG	LOCAL	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	*LOCAL*
3	ENEMY																										
4	FRIENDLY																										
5	**ISR FOCUS**																										
6		**RECON SQDRN**																									
7		FLT TRP 1																									
8		FLT TRP 2																									
9		SURV TRP																									
10		UAS PLT1																									
11		UAS PLT2																									
12		UAS PLT3																									
13		USA PLT4																									
14	**BCT ASSETS**	COLT PLT																									
15		**CAB 1**																									
16		**CAB 2**																									
17		**CAB 3**																									
18		**NLOS BN**																									
19		EQ-36 1																									
20		EQ-36 2																									
21		EQ-36 3																									
22		**BSB**																									
23		**MI CO**																									
24		HCT 1																									
25		HCT 2																									
26		HCT 3																									
27		**MTI**																									
28		**UAS**																									
29		**IMINT**																									
30		**COMINT**																									
31	**EAB ASSETS**	**ELINT**																									
32		**CI**																									
33		**HUMINT**																									
34		**SF/LRS**																									
35		*LOCAL*																									*LOCAL*

Figure 3-8. Example ISR synchronization plan in matrix format

3-64. As stated above, the ISR synchronization plan is a product the S-2 uses to synchronize the BCT's collection effort with the current threat assessment and friendly scheme of maneuver. This product and this process is a way to synchronize and communicate the ISR effort horizontally and vertically across commands. What it does not do, however, is provide the detail needed to perform technical control of the ISR effort. In OIF, S-2s typically use a working matrix to assist in managing this effort and assist analysts. Figure 3-9 is an example working matrix. As a tool for analysts, the working matrix—

- Provides additional detail and aids in developing the ISR synchronization plan.
- Links PIRs to the commander's lines of operation and/or decision points.
- Links collection requirements to NAIs and TAIs.
- Provides the task and purpose for the collection task.
- Provides detailed collection and reporting requirements.
- Is constructed in a spreadsheet format and is comprised of individual worksheets for the brigade and each of its subordinate battalions.
- Is posted to the brigade webpage and updated as needed by the S-2 at each echelon.
- Is not a tasking document and is not published as part of the base order.
- Is a working aid maintained on the brigade webpage that assists the intelligence staff in synchronizing internal operations across echelon.

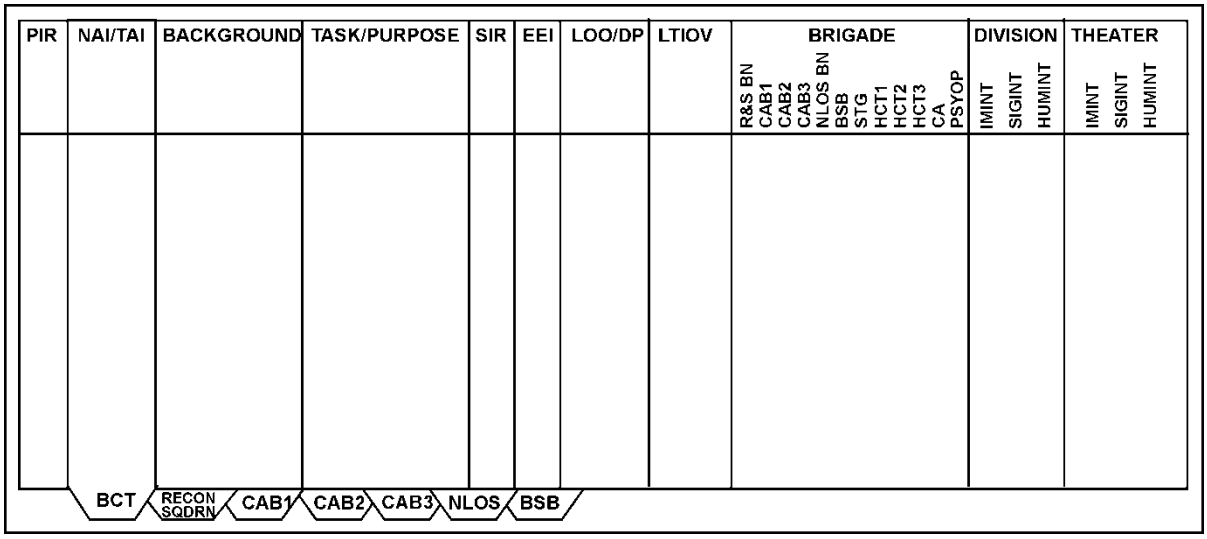


Figure 3-9. Example working matrix

SUPPORT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION

3-65. **ISR integration is the task of assigning and controlling a unit's ISR assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of OPLANs and operations orders (OPORDs)** (FM 3-0). During ISR integration, the entire staff participates as the lead for the ISR plan transitions from the intelligence officer to the operations officer. ISR integration is vital in controlling limited ISR assets. During ISR integration, the staff recommends redundancy and mix as appropriate. The result of ISR synchronization and ISR integration is an ISR effort focused on answering the commander's requirements through ISR tasks translated into orders.

3-66. ISR integration is accomplished with staff participation and in coordination with the intelligence officer; the operations officer is the staff proponent for ISR integration. Intelligence officers assist the operations officer in the development of the ISR plan by providing an ISR synchronization plan. The key to successful ISR operations is an ISR plan that—

- Is developed from well-reasoned enemy situation overlays, COA statements, and the event template or matrix.
- Is driven by the CCIRs and is focused on command-directed tasks.
- Is tied to the decisions the commander needs to make (decision points).
- Facilitates the commander's visualization and decision making.
- Is prepared jointly by the S-2/S-3 and rest of the staff.
- Remains synchronized with the scheme of maneuver.
- Is issued and updated as part of the orders process.
- Assigns appropriate collection tasks to subordinate units.

3-67. ISR integration is the task of assigning and controlling the ISR assets in terms of space, time, and purpose to collect and report information as a concerted and integrated portion of brigade operations. This task is the responsibility of the S-3, and it ensures assignment of the appropriate ISR assets to collection tasks through a deliberate effort supported by the entire staff across all warfighting functions.

3-68. During ISR integration, responsibility for ISR operations transitions from the S-2 to the S-3. ISR synchronization and integration results in a fused effort focused on answering the commander's

requirements through ISR tasks translated into orders. The S-3, with input from the S-2, develops tasks based on specific information requirements developed by the S-2 as part of ISR synchronization. These specific information requirements facilitate tasking by matching requirements to assets. The S-3 assigns tasks based on latest time information is of value (LTIOV), the latest event information is of value (LEIOV), and limitations of available ISR assets. The S-2 assists the S-3 in ensuring intelligence requirements are identified, prioritized, and validated. The S-2 also assists the S-3 in ensuring an ISR plan is developed and synchronized with the overall operation.

3-69. ISR integration is vital in controlling limited ISR assets. This task also includes integrating EAB ISR assets into collection operations. The S-2 assists the S-3 in conducting ISR integration by developing the required orders products, monitoring the current situation to predict changes to the enemy situation, and recommending changes to the ISR plan. All changes made to the ISR plan are issued in a FRAGO and are approved by the S-3. This includes dynamic retasking. During steady state operations the S-2 assists the S-3 in ISR integration by briefing the status of ISR operations in accordance with the daily battle rhythm. The S-2 normally uses the ISR synchronization plan, the ISR overlay, and the PIR to accomplish this

DISSEMINATE INTELLIGENCE

3-70. The timely and accurate dissemination of combat information and intelligence is critical to successful operations. Information and intelligence in the BCT is delivered as voice, text, graphic, or digital media. Voice data is disseminated over tactical radios on the command net or operations and intelligence net. Text, graphic, and other digital media are disseminated over ABCS systems including Force XXI Battle Command Brigade and Below (FBCB2) and deposited in the JCDB, email accounts, chat rooms, and on the brigade webpage. Information posted to the webpage is not considered disseminated until the S-2 ensures that subscriber-users have actually received the product. The timely and accurate dissemination of intelligence throughout the brigade is important to successful operations. See chapter 6 for more information on dissemination.

ASSESS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE OPERATIONS

3-71. The intelligence staff tracks reporting to determine how well the ISR assets and intelligence production efforts are satisfying the CCIRs. The desired effect is to deliver relevant information to the commander by the LTIOV. Assets are not wasted unnecessarily on outstanding tasks, as both the S-2 and the user ensure the other understands when an ISR tasking has been adequately fulfilled. The staff must—

- Monitor and maintain synchronization. Through coordination with the S-2, the staff knows when and what critical pieces of information are missing from the commander's estimate of the situation. The staff uses the ISR synchronization matrix and ISR plan to ensure synchronization with the overall operation and scheme of maneuver. The other critical tool for the staff is the decision support template. The staff must have a complete copy of the decision support template to ensure the ISR synchronization matrix does not miss collection requirements.
- Correlate reports to ISR tasks. The staff tracks which ISR task or group of ISR tasks originates from which PIR to ensure that the collected information was provided to the original requester. This tracking also allows the staff to rapidly determine which asset is available for retasking.
- Screen reports. The S-2 staff screens each report received for relevance, completeness, timeliness, and opportunities for cueing. If the staff determines that it completely fulfills the ISR task or requests for information (RFI), that ISR task or RFI is closed and the information is provided to the original requesting unit.
- Provide feedback to collectors and analysts. The staff provides feedback to all the ISR assets. This is normally provided through the C2 element of that unit. By doing so, the staff quickly reinforces if its collection or production is answering the original ISR task, or it can provide guidance if it does not. This feedback is essential to all ISR assets. The staff may provide additional information on its collection or analysis if the S-2 indicates what is needed.

UPDATE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLAN

3-72. Following reporting, the intelligence report or processed data is disseminated to the requester. The intelligence staff, in coordination with the requester, evaluates the reports and determines if the requirement has been satisfied. If the data is insufficient, the staff coordinates for additional coverage. Requester feedback establishes customer satisfaction, permits tasker deletion, and frees ISR assets and resources to be redirected to satisfy other active requirements (see FM 2-0).

3-73. As SIRs and, subsequently, PIRs are answered, the S-3, in coordination with the S-2 and staff, updates the ISR plan and refocuses assets to answer other or new ISR tasks within the constraints of METT-TC. Simultaneously, the higher headquarters is going through the same process and may answer subordinate unit PIRs or intelligence requirements. Thus, the requirements are tied to EAB headquarters requirements process, and the staff updates the ISR plan in a dynamic environment. To accomplish this, the staff—

- Maintains ISR synchronization.
- Cues assets to other collection opportunities.
- Eliminates satisfied requirements.
- Develops and adds new requirements.
- Recommends redirecting assets to unsatisfied requirements.
- Transitions to next operation.

DISSEMINATE INTELLIGENCE

3-74. The intelligence staff ensures that combat information and intelligence products are provided to commanders and other users at or before the LTIOV in a format supportive of situation development, IPB, targeting, or FP. The timely and accurate dissemination of intelligence throughout the brigade is important to successful operations. See chapter 6 for more information on dissemination.

EVALUATE REPORTING

3-75. The intelligence staff tracks reporting to determine how well the ISR assets and intelligence production efforts are satisfying the CCIRs. The desired effect is to deliver relevant information to the commander by the LTIOV. Assets are not wasted unnecessarily on outstanding tasks, as both the S-2 and the user ensure the other understands when an ISR tasking has been adequately fulfilled. The staff must—

- Monitor and maintain synchronization. Through coordination with the S-2, the staff knows when and what critical pieces of information are missing from the commander's estimate of the situation. The staff uses the ISR synchronization plan and ISR plan to ensure synchronization with the overall operation and scheme of maneuver. The other critical tool for the staff is the decision support template. The staff must have a complete copy of the decision support template to ensure the ISR synchronization plan does not miss collection requirements.
- Correlate reports to requirements. The staff tracks which ISR task or group of ISR tasks originates from which intelligence requirement to ensure that the collected information was provided to the original requester and to all who need the information. This tracking also allows the intelligence officers to determine which ISR tasks have been satisfied and which require more collection.
- Screen reports. The S-2 staff screens each report received for relevance, completeness, timeliness, and opportunities for cueing. If the staff determines that it completely fulfills the ISR task or RFI, that ISR task or RFI is closed and the information is provided to the original requesting unit.
- Provide feedback to collectors and analysts. The staff provides feedback to all the ISR assets on their mission effectiveness and to analytic sections on their production. This is normally

provided through the C2 element of that unit. By doing so, the staff quickly reinforces if its collection or production is answering the original ISR task, or it can provide guidance if it does not. This feedback is essential to all ISR assets. The staff may provide additional information on its collection or analysis if the S-2 indicates what is needed.

UPDATE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLAN

3-76. Following reporting, the intelligence report or processed data is disseminated to the requester and to all who need the information. The intelligence staff, in coordination with the requester, evaluates the reports for completeness and determines if the requirement has been satisfied. If the data is insufficient, the staff coordinates for additional coverage. Requester feedback establishes customer satisfaction, permits tasker deletion, and frees ISR assets and resources to be redirected to satisfy other active requirements (see FM 2-0).

3-77. As SIRs and, subsequently, PIRs are answered, the S-3, in coordination with the S-2 and staff, updates the ISR plan and refocuses assets to answer other or new ISR tasks within the constraints of METT-TC. Simultaneously, the higher headquarters is going through the same process and may answer subordinate unit PIRs or intelligence requirements. Thus, the requirements are tied to EAB headquarters requirements process, and the staff updates the ISR plan in a dynamic environment. To accomplish this, the staff—

- Maintains ISR synchronization.
- Cues assets to other collection opportunities.
- Eliminates satisfied requirements.
- Develops and adds new requirements.
- Recommends redirecting assets to unsatisfied requirements.
- Transitions to next operation.

This page intentionally left blank.

PART TWO

Intelligence Processing

ISR operations collect information and data about threat forces, activities, facilities, and resources as well as information concerning the physical environment of a particular aerospace, surface, or subsurface area, and other characteristics of the operational environment. Reconnaissance is distinguished by its limited or short-term objective. Surveillance is the long-term or sustained collection of information. Successful ISR results in the timely collection, processing, and reporting of relevant information. This relevant information forms the foundation of intelligence and situational understanding.

Chapter 4

Collect and Process Information

OVERVIEW

4-1. Intelligence operations generally include the steps and functions that constitute the intelligence process. At the tactical level, the collect and process steps of the intelligence process are interrelated and often indistinguishable. Normally, the ISR unit also controls the sensor-unique processing equipment. Collecting and processing begins with the receipt of an order and ends with the reporting of processed information to the commander, staff, and other appropriate users in a form suitable for action or production of intelligence.

4-2. Collecting includes the command, control, organization, and maneuver of organic or supporting assets into positions where they can satisfy objectives and report the information. The intelligence staff works with the operations staff to develop OPLANs and OPORDs that direct the execution of the ISR plan. Once the plan is in motion, the intelligence staff monitors the results, assesses whether the information met the objective, and recommends retasking as required. The foremost challenge of the ISR operations is to maximize the effectiveness of limited collection resources within the time constraints imposed by predeployment planning and combat operations.

4-3. Processing is the conversion of raw data into information that the intelligence staff can use to produce intelligence or, when critical or exceptional in nature, the commander and staff can readily act upon. Processing actions include initial imagery interpretation, data conversion and correlation, document translation, transcription, and decryption, as well as reporting the results of these actions to production elements. Processing may be performed by the same unit that collected the information or a separate, distinct unit. Normally, the ISR unit also controls sensor-unique processing and exploitation equipment. The BCT S-2 will have the capability to access required data from organic and non-organic ISR sensors through DCGS-A. Processing by the unit conducting the collection allows that unit to evaluate the accuracy and relevance of the information before reporting it.

4-4. Once collected and processed (as required), information is reported in accordance with the collected objective and instructions contained in the reconnaissance order. This processed information, however, remains distinct from the intelligence production task in that the data has not been subjected to the scrutiny of all-source analysis by the intelligence staff or supporting intelligence production organization.

4-5. See FM 3-20.96, FM 3-20.971, and FM 3-20.98for more information on ISR operations.

PREPARE AND EXECUTE

4-6. The brigade S-3 uses the WARNO, OPORD, or FRAGO to assign missions. Any brigade subordinate unit may be tasked to perform an ISR mission. Brigade subordinate units may be tasked to collect information through either implied or specified tasks.

4-7. The C2 element of each ISR asset plans, prepares, executes, and assesses its assigned ISR missions. Subordinate unit commanders manage their assigned ISR assets, conduct assigned ISR missions, and provide ISR capabilities to the brigade as required. Subordinate commanders seek to satisfy their own requirements by using organic assets. Based on the commander's objectives, subordinate commanders prioritize and submit to the S-2 any intelligence requirements that exceed organic ISR capabilities for collection by higher echelon assets. The S-2 reviews, validates, and prioritizes the outstanding intelligence requirements for the brigade and makes recommendations to the S-3 regarding the tasking of organic and attached brigade ISR assets to ensure maximum use of these resources.

4-8. Commanders have the responsibility to evaluate the risks (tactics, weather, safety, and sustainment) involved to complete the mission successfully. When the commander of an ISR asset under the direct OPCON of the brigade identifies a significant risk associated with its mission, the brigade commander is the final authority on whether or not mission needs outweigh the risks involved. The executing unit's commander normally provides input in the MDMP.

4-9. Since the purpose of ISR is to enhance the combat effectiveness of friendly forces by gaining an information advantage over threat forces, it is essential that ISR operations not compromise that advantage by providing indications of friendly force intentions. Operations security (OPSEC) measures are used during all phases of planning and execution of ISR operations. Essential secrecy is required about the specific characteristics of sensors and data links, deployment intentions, areas under surveillance, timing of surveillance, and operating patterns. ISR tasks are the actions of the intelligence collection effort.

RECONNAISSANCE

4-10. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (FM 1-02). It is designed to obtain information on the enemy or characteristics of a particular area. Reconnaissance is the precursor to all operations and may be accomplished through passive (overt or covert) surveillance, technical means, human interaction, or by fighting for information.

Reconnaissance Handover

4-11. Reconnaissance handover (RHO) is an operation between two units that transfers information and responsibility for reconnaissance of an assigned area or enemy contact from one unit to another. Many of the tasks involved in RHO are similar to battle handover and relief in place. The difference lies in the purpose for RHO is maintaining contact with the enemy or observation of a specific area, and that the reconnaissance units are not always within line of sight of each other. RHO is normally associated with a designated area or reconnaissance handover line or phase line; it may be of a sector or zone, NAI, TAI, and/or threat contact. RHO can be visual, electronic, digital, or analog. Coordinating RHO responsibility occurs from higher to lower unit.

Surveillance

4-12. Surveillance is the systematical observation of airspace, surface, or subsurface areas, places, persons, or things in the AO by visual, aural (audio), electronic, photographic, or other means. Other means may include space-based systems, using CBRN, artillery, engineer, special operations forces (SOF), and air defense equipment. A simple way to differentiate between the two is that reconnaissance elements tend to move, while surveillance elements tend to be static. Surveillance avoids detection and enemy ambushes.

4-13. See FM 3-20.96, FM 3-20.971, FM 3-20.98, and FM 3-21.94 for more information on reconnaissance and surveillance.

Process

4-14. Most ISR assets must collect and process their data prior to disseminating the data. MI systems each have their own reporting and processing systems that are detailed in the appropriate MI system manual and technical manuals. Processing involves converting raw data to a form that is usable by an analyst or for immediate action by a commander. Some ISR assets, particularly air and ground scouts, can report relevant information that is immediately usable by the tactical commander, for example, for targeting. However, in many cases, the output of an ISR asset is raw information of limited immediate utility to a commander.

4-15. Also, in small-scale contingencies (SSCs), the need for target confirmation by redundant sources, dictated by the ROE, prevents the immediate reaction by the tactical commander to raw information. The transformation of collected information into intelligence requires, in most cases, processing and analysis before the data is disseminated. The transmission of raw data to the processing system and then to the intelligence staff for analysis takes time and communications capabilities. These capabilities will vary widely with the deployment conditions and situation.

4-16. Collected information is provided via secure media to the appropriate processing elements. During processing, raw information is converted to forms that the intelligence analyst can use in the produce step of the intelligence process. Processing actions include initial imagery interpretation, data conversion and correlation, document translation, and decryption.

4-17. Processing may be performed by the same element that collected the information. Normally, the unit that has C2 over the collection asset also controls the sensor-unique processing equipment. Processing by the unit conducting the collection allows that unit to determine the appropriateness and quality of the reporting by the collection asset. An example of processing is in taking the technical parameters (frequency, pulse repetition frequency, and bandwidth) detected by an electronic warfare (EW) system and associating the parameters with a particular radar system. Rather than having to deal with raw technical data, the all-source analyst is provided with the relevant information about the radar's location, purpose, and identity.

4-18. Different types of information require different degrees of processing before the analysts can use the information. Some collected information, such as a reconnaissance report, may not require any processing although leaders in the reporting chain evaluate its appropriateness and accuracy. In the area of EW, due to improvements in hardware and software, processing is increasingly performed at the collection system. Captured enemy documents (CEDs) may only require translating before analysts can use them. Processing remains distinct from the produce step of the intelligence process because the data has not yet been subjected to analysis. Appendix C discusses CEDs and captured enemy equipment (CEE).

Fusion

4-19. DCGS-A provides automated level I and some level II fusion to assist the analyst in processing intelligence information. Level I fusion consumes uncorrelated single-source data and correlates data for use in targeting or further analysis. Level II fusion consumes correlated data and aggregates it into larger entities for situational awareness.

REPORTING

4-20. The following reporting techniques and procedures are generally present in most units. This information is intended to highlight the areas impacted by digital information systems. Staff and unit SOPs should address these items in greater detail as applicable for unit size, echelon of command, and degree of digitization.

Reports

4-21. The staff builds a large portion of the COP from information extracted from reports coming into the CP through the ABCS and its supporting systems. Advanced communications and automated data processing (ADP) systems provide digitized units with increased capacities to receive and store reported information from multiple sources. This high information tempo can degrade tactical efficiency without effective information management. At brigade and battalion levels, reports remain the centerpiece of the situational understanding. Reports take basically two forms: urgent or routine. While ABCS is the standard for both types of reports, voice messages remain an appropriate reporting mechanism for urgent reports. Units can also send urgent preformatted reports via FBCB2 and selected Army Tactical Command and Control Systems (ATCCS). Examples of these messages are the "Check Fire All" and "CBRN1" messages. DCGS-A will provide the S-2 access to reporting on the ABCS network. The primary value of digital reporting is that it assists with standardization and provides a wider span of access to potential users.

Reporting Guidelines

4-22. Reports exist to provide information in an organized manner. Central to effective information management is a good reporting system. Commanders and staff should consider the following when preparing, submitting, and using reports:

- Reports should contain only relevant information. This information should support decision making and the execution of operations. Limiting reports to essential information reduces the amount of time and effort subordinates must spend on collecting, organizing, and transmitting reports.
- Reports have prescribed formats to ensure completeness of information that is transmitted. The unit SOPs should outline the format for each report used by the unit. It should also explain how each report is used and under what conditions it is to be submitted.
- Commanders and staff must remember that timely reporting, especially of threat activity, is critical in fast-moving operations. They report accurate information as quickly as possible and do not delay reports for the sole purpose of assuring the correct format.
- Reporting units send only the parts or lines of a report that contain new information or changes. This will reduce transmission time and avoid overloading radio nets.
- Unit SOPs must clearly state what reports are sent by voice frequency modulated radios and what reports are sent by digital means. In general, reports for threat contact and actions, CCIR, exceptional information, and CBRN reports are sent by voice frequency modulated then followed-up with digital reports.

Report Formats

4-23. Report formats and uses are found in FM 6-99.2 and unit SOPs. Many of the standard reports and situation graphics exist as preformatted messages in the ABCS. These preformatted messages are intended to provide an interface between the ATCCS and the FBCB2. For example, the All-Source Analysis System-Light (ASAS-L) and DCGS-A can send a target intelligence data message to the fire support element's (FSE's) Advanced Field Artillery Tactical Data System (AFATDS). Reports can also automatically populate the display screens of all stations on the network. An FBCB2 contact report can, if set accordingly, transmit a threat unit icon to all clients on the net. Whether or not this unrestrained reporting style is desired will be a decision that the unit (typically battalion) information manager must make. This is a case of filtering or tailoring the process. See appendix B for examples of the most common reports used by the BCT.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ASSETS

4-24. The brigade conducts continuous ISR using its organic collection assets supplemented by additional maneuver, fire support (FS), MI, and FP assets from EAB. Some EAB assets may be attached to the

brigade based on METT-TC while other assets may be operating in the brigade's AO in general support (GS) of the EAB. The brigade can also forward requirements through the battalions for collection by the battalions' organic or attached collection assets. This procedure provides the brigade with a wide array of assets to draw upon, each with unique capabilities.

4-25. All elements of the brigade contribute to the ISR picture through direct or indirect reporting. Every Soldier is potentially an information collector. Soldiers conducting patrols, staffing, observation posts, staffing checkpoints, or even convoying supplies along a main supply route serve as the commander's "eyes and ears." The challenge for the intelligence professional is to understand what types of information Soldiers performing different tasks and missions can provide to overall situational awareness and how to leverage that information into situational understanding. It is essential to properly brief these assets so that they are aware of the intelligence requirements prior to their missions and to debrief them immediately upon completion of their missions while the information is still current in their minds and any timely intelligence they may provide is available for further action. This cycle (brief-mission-debrief-intelligence/situational awareness) is continuous throughout operations. The capabilities of any of these assets that are present in the brigade's AO must be considered when formulating the brigade ISR plan.

LOCAL NATIONAL AUTHORITIES

4-26. Local national authorities and former local national authorities know their populations and local infrastructure best. Key information can be gained from cooperative local national authorities or former authorities. Analysts must always consider that these sources may be biased for any number of reasons. Some examples of the types of information that local national authorities can provide are discussed below.

- Politicians usually know their populations very well or they would not be able to remain in office. They can provide detailed socio-cultural information on the populace within their region of control (for example, economic strengths and weaknesses or religious, ethnic, and tribal breakdowns). They are also usually aware of the infrastructure. Obviously, intelligence analysts must be aware that information provided by these personnel generally will be biased and almost certainly slanted in the long-term favor of that individual.
- Police can provide information on local criminal organizations, local ethnic breakdowns, and key terrain within their AOs. During stability operations, it would be useful to pay attention to the local police precinct boundaries when designating unit boundaries within an urban area. Dividing local national police boundaries between multiple US unit boundaries can cause liaison problems and confusion on both sides whenever US forces have to work with local national police forces. Additionally, local national police forces will have been conducting operations in their urban environment prior to US operations and will have adjusted precinct boundaries into manageable sections based on the number of police personnel available, areas requiring concentration based on high criminal activity or unrest, and, where applicable, religious, ethnic, or tribal breakdowns.
- Fire department personnel often have ready access to blueprints of the structures within their precincts, information on fire escapes, and other building safety-related information as well as detailed information on their structural composition (and the fire threat in individual buildings or whole blocks of a city).
- Public works personnel are uniquely familiar with the infrastructure of the city. They can provide information on the critical points in the city that must be secured in order for public services to be maintained; they can provide key information on AAs throughout the city (especially underground service passages and sewer and drainage systems).
- City halls in many parts of the world are also repositories of key records on the infrastructure of the city. They may contain detailed maps of the city, key city infrastructure information, and blueprints of the buildings in the city.

This page intentionally left blank.

Chapter 5

Intelligence

Using PIRs and commanders guidance the brigade commander drives the intelligence effort. These factors along with changing missions and operational environments impose numerous and varied requirements on the intelligence staff. The staff employs collaborative analysis techniques and procedures that leverage distributed intelligence production capability of higher and subordinate echelons to meet these requirements. Proficiency in these techniques and procedures enables the brigade intelligence staff to answer the commander and staff's requirements.

OVERVIEW

5-1. The production task involves evaluating, analyzing, and interpreting information from single or multiple sources into finished intelligence products. All-source analysis determines the accuracy and validity of combat information and single-discipline intelligence reports, thus reducing the potential for deception or erroneous information entering into all-source intelligence products and databases. Production is accomplished in response to expressed and anticipated intelligence requirements and within assigned AO and AOI.

5-2. The S-2 coordinates and directs intelligence production to provide non-duplicative all-source intelligence products to the unit commander, staff, and subordinate forces. Production occurs in the intelligence staff and separate production element at every echelon from national to battalion level. Effective production management ensures that the unit commander receives the intelligence products and services required to accomplish the assigned mission. Automated database systems provide current tailorable data appropriate to the mission.

5-3. The S-2 evaluates the success of the production task against the requirement stated in the PIR. Intelligence personnel at all levels evaluate the production process and the products in an effort to continuously improve support to the commander. Evaluation includes transiting from the collection and processing task, meeting production standards, improving processes, and providing feedback.

INTELLIGENCE

5-4. Intelligence is the product resulting from evaluating, analyzing, assessing, and interpreting available information concerning the threat, terrain, weather, and civil considerations. The brigade's intelligence staff provides the brigade commander and subordinates the intelligence they need to execute battles, engagements, and other missions in full spectrum operations. Tactical intelligence identifies and assesses the threat's capabilities, vulnerabilities, objectives, and potential COAs and is required for planning and conducting tactical operations (JP 1-02).

5-5. Assessing information is a continuous process that enables continuous analysis and depiction of activity and/or events in order to afford commanders time-sensitive situational understanding. ISR is one major element that must closely assess the mission's progress and rapidly adapt these finite collection resources in order to maintain situational awareness and contribute to the commander's situational understanding. It not only encompasses the operations process but also is evident throughout each warfighting function.

5-6. Timely, relevant, accurate, and predictive tactical intelligence supports the brigade commander in gaining tactical advantage and information superiority over threat forces. Tactical intelligence supports protection requirements by providing the commander with information on the imminent threats to the force including those from terrorists, saboteurs, insurgents, and foreign intelligence organizations. Tactical intelligence is distinguished from other levels of intelligence (strategic and operational) by its perishability and ability to immediately influence the outcome of the tactical commander's mission.

5-7. The enables the S-2 intelligence staff to produce intelligence and receive intelligence support from throughout the US intelligence community that falls into one of six categories. The categories of intelligence are distinguished from each other primarily by the purpose of the intelligence product. The categories can overlap and the same intelligence can be used in each of the categories. Intelligence organizations use specialized procedures to develop each category of intelligence. The following information describes each category and the responsible organization within the brigade. (See FM 2-0 for detailed information.)

- **I&W.** This is the analysis of time-sensitive information that could involve a threat to the US and multinational military forces, US political or economic interests, or to US citizens. While the S-2 produces I&W intelligence, each element, such as the MPs conducting PIO, contributes to the I&W through awareness of the CCIRs and reporting related information.
- **Current Intelligence.** The S-2 produces accurate reporting on the operational environment and current enemy situation, which becomes the threat situation portion of the COP, projects the enemy's anticipated situation and implication on friendly operations.
- **GMI.** Intelligence concerning military capabilities of foreign countries or organizations or topics relating to armed forces capabilities, including threat characteristics, organization, training, tactics, doctrine, strategy, military strength and effectiveness, and area or terrain intelligence. The S-2 develops initial IPB products from various GMI databases, and then develops and maintains the unit's GMI database tailored to their AO based on the commander's guidance. This database support the unit's plans, preparation, execution, and assessment of operations.
- **Target Intelligence.** This is the analysis of enemy units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities to attack, re-attack, or exploitation.
- **Scientific and Technical (S&T) Intelligence.** This is the collection, evaluation, and interpretation of foreign engineering science and technology with warfare potential. This includes military systems, weapons, weapon systems, material, research and development, and production methods. The S-2 establishes instructions within SOPs, orders, and plans for handling and evacuating captured enemy material for S&T intelligence exploitation.
- **CI.** This is the identification and recommended countermeasures against foreign intelligence security service threats and their ISR activities of non-state entities, such as organized crime, terrorist groups, and drug traffickers.

PRODUCTION

5-8. While performing the produce step of the intelligence process the S-2 analyzes information from single or multiple sources to develop all-source intelligence products. Like collection, the S-2 must ensure the brigade's intelligence production is focused, prioritized, and synchronized in accordance with the commander's PIRs as well as EEFIs. The BCT intelligence production architecture is based on the concept of DCGS-A enabled distributed collaboration. Each subordinate unit's intelligence element processes data and information into an intelligence product that is shared throughout the BCT.

5-9. This distributed analytic effort is complemented by collaboration between elements on unresolved issues or gaps in the threat "picture" to create and maintain a common master database. Distributed analysis means that each intelligence organization has a role in developing the current intelligence picture (as the intelligence portion of the COP) and conducting continuous situation development. DCGS-A allows intelligence analysts at all echelons to share their current annotated graphic representation of the intelligence situation in their operational environment. It then can be inserted into the higher command's situation graphic without the additional steps of querying databases or re-annotating the overlay with graphics. This process shares the results of analysis and not just data. The underlying data is linked to the overlay and is available on demand. It is pulled through the network as required since only changes to the graphic can be selected.

5-10. Subordinate, lateral, and higher echelon units all share a common picture of the operational environment without necessarily sending the underlying data. This process demands the use of collaboration. As each echelon's representation of the situation is compared, merged, and evaluated,

discrepancies are discussed to preclude duplicate reporting and to ensure that information from the higher command is available to supported commands without re-analyzing information at each echelon. DCGS-A collaboration tools assist analysts from different units and echelons in sharing and evaluating information.

5-11. Each warfighting function also provides a digital overlay of the current situation that facilitates producing the intelligence picture. For example, engineers will provide a continuous topographic situation overlay to show the affects of manmade and weather changes to the terrain (for example, minefields, roadblocks); the ADA element provides an analyzed air picture that shows the patterns of threat air, potential airfields, and forward arming and refueling points (FARPs). The result is that the S-2, supported by the MI Company, uses combat information, targeting data, and intelligence from the BCT's ISR resources to develop an accurate and timely intelligence assessment. It has the organic processing and communications systems to collaborate with external analytic elements, subordinate battalion S-2s, and the Analysis and Integration Platoon to continuously update and refine portions of the BCT's COP depicting the threat and other conditions of the operational environment.

5-12. The Analysis and Integration Platoon develops and maintains the brigade's GMI on potential threat forces and environments based on unit CONPLANs and commander guidance. As an essential component of unit readiness, this database supports the brigade's planning, preparing, and executing of exercises and operations. The S-2 staff, along with the Analysis and Integration Platoon, performs the following production tasks:

- IPB.
- Situation development.
- Target development.
- Combat assessment.

5-13. The brigade S-2 is part of a DCGS-A enabled distributed intelligence production system. Each intelligence staff within the system is responsible for developing the threat situation within its operational environment. These threat assessments within a given AO, AOI, or threat functional area support the COP within their unit and the commands of higher, lower, and adjacent units. Distributed production allows the S-2 to focus S-2 personnel on answering the commander's PIRs while supporting the development of the higher echelon's COP. This type of production technique requires analyst-to-analyst collaboration, standardized formats and procedures, and trust in the analytic conclusions of each echelon.

5-14. The S-2 relies on the Analysis and Integration Platoon of the MI Company to process information collected by the brigade's ISR assets, to support distributed intelligence production, to access databased information, and to pull intelligence products from the higher echelons via DCGS-A. The MI Company conducts -source analysis. The MI Company's intelligence analysts develop situation graphics that support the S-2 section's intelligence production and RM.

SITUATION DEVELOPMENT

5-15. Situation development is a process for analyzing information and producing current intelligence about the threat situation in a particular area. The process depends upon products developed during IPB and the continuous monitoring of events and specific activities in the brigade's operational environment. The process helps the S-2 confirm threat COAs, explain the threat activity's relationship to the friendly operation and area, and identify intelligence gaps. The current intelligence products developed through the situation development process help the brigade commander to understand the current threat situation and make decisions on current and future operations. The S-2, with the support of the MI Company's Analysis and Integration Platoon, conducts situation development during the preparation for and execution of the brigade's operations.

5-16. The intelligence staff uses the situation development process to understand current threat activities and produce intelligence that answers the commander's PIRs. The sequence of steps may vary with the nature and urgency of the collected information. Time-sensitive relevant information or partially developed intelligence that affects the current operation may be disseminated immediately upon recognition. Once

disseminated, the staff completes the tasks of the process by analyzing the information and updating the current intelligence.

5-17. The digital (or analog) situation map (SITMAP) with supporting overlays is the S-2 section's primary analytic tool in the situation development process. The SITMAP provides the S-2 with a graphic representation of threat activity within the operational environment. It serves as a common vehicle for analyzing information and disseminating the current intelligence picture. By incorporating automated intelligence tools, the S-2, supported by the MI Company's Analysis and Integration Platoon, can quickly post, correlate, and update information on the situation graphic and, following analysis, update the intelligence database. Some of the specific uses of the SITMAP are to—

- Evaluate and integrate information and intelligence from multiple sources.
- Track the disposition, strength, and movement of threat forces.
- Isolate indicators of threat COAs, intentions, and objectives.
- Track other operational environment considerations (terrain, weather, and civil considerations) that may affect friendly operations.
- Identify new information that may affect friendly operations.
- Present the current threat assessment to the commander and staff.

RECORD INFORMATION

5-18. The situation development process requires that relevant information is converted into text or graphic format and arranged into groups of related items. The S-2 receives information from organizations internal to the brigade and from organizations outside the brigade. This information consists of message traffic on military and political events of interest to the brigade; real-time reporting of operational situations by subordinate battalions and companies; and graphic products, summaries, and briefings from higher echelon organizations. The MI Company's Analysis and Integration Platoon records this information in the brigade's intelligence database to facilitate retrieval, correlation, and presentation of data for evaluation, analysis, and dissemination. Information recording mechanisms (analog and digital) include—

- Intelligence journals.
- Intelligence files.
- SITMAPs.
- Intelligence workbooks.
- Threat characteristics records.

EVALUATE INFORMATION

5-19. When evaluating information the S-2 determines the relevance of the information to the operation, reliability of the source, and accuracy of the information. Evaluation of information at the tactical level is a simple step compared to the procedures employed at the strategic level. From the viewpoint of the brigade or battalion, information that relates to the unit's AO and AOI is relevant; information about areas outside the AOI may or may not be relevant. Analysts supporting the S-2 and the MI Company may not be able to judge the reliability of a source because it may not have repetitive contact with the source.

Relevance

5-20. Relevant intelligence answers the CCIRs about the threat and other conditions of the operational environment. The S-2 must produce and present products that focus on the unit's mission and help the commander to visualize and understand the operational environment.

5-21. The analyst evaluates the relevance of information by filtering the information based on the following criteria:

- Relates to the unit's operational environment.

- Applies to the unit's mission.
- Responds to a PIR or intelligence requirement.

Reliable

5-22. In evaluating the reliability of information, the analyst looks at both the information and the source of the information. The evaluation of reliability is built in throughout the collection and analysis system. The principal basis for judging the reliability of a source or an agency is previous experience with the source or agency. The criteria for evaluating information from brigade units and supporting ISR assets come from knowledge of the units' training, experience, and past performance. The following ratings are typically applied to the source:

- Reliable
- Usually Reliable
- Fairly Reliable
- Not Usually Reliable
- Unreliable
- Cannot be judged

Accuracy

5-23. As illustrated in Table 5-1, accuracy addresses the probable truth of the information. Normally, the analyst judges the accuracy of a piece of information by comparing it with similar information available in the database. When possible, the analyst obtains confirming or refuting information through higher headquarters, different agencies, or other sources. In general, the analyst evaluates the accuracy of reported information based on the answers to the following basic questions:

- Is it plausible for the fact or event to occur?
- Is the report consistent within itself?
- Is the report confirmed or corroborated by information from another source?
- Does the report agree or disagree with other available intelligence?

5-24. For more information regarding reliability and accuracy see FM 2-22.3, Appendix B.

Table 5-1. Information evaluation rating scale

ACCURACY	
1	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability; usually demonstrates adherence to known professional standards and verification processes
2	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time; may not have a history of adherence to professionally accepted standards but generally identifies what is known about source feeding any broadcast
3	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
4	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
5	Lacking in authenticity, trustworthiness, and competency; history of invalid information
6	No basis exists for evaluating the reliability of the source; new information source

ANALYZE INFORMATION

5-25. To analyze information, the S-2 with the MI Company's Analysis and Integration Platoon draws conclusions about the probable meaning of the evaluated information and determines its significance relative to forecasted threat COAs and the commander's PIRs. The S-2 also attempts to identify activity or trends that provide the I&W of the initiation, change, or escalation of threat actions that represent opportunities or risks to a friendly force. The S-2 uses the indicators developed for each threat COA and PIR during the MDMP as the basis for analysis and conclusions. Analysts supporting the S-2 apply the following substeps (assessing and testing) to analyze information.

5-26. Assessing entails the sifting and sorting of evaluated information to update the current situation with respect to the threat activity and unit's mission and operations. It begins with a clear understanding of the unit's mission and commander's intent. All information gathered is viewed in relationship to the commander's mission, intent, and stated requirements. Assessment requires judgment and a thorough knowledge of—

- The command's organization, operations, and capabilities.
- Characteristics of the AO and AOI.
- How the threat organizes, equips, trains, employs, and controls its forces.
- All of the IPB products.

5-27. Compare and contrast the assessment against the forecasted threat COAs. The comparison includes verifying the existence or nonexistence of indicators. The lack of information relating to specific indicators may signify that the COA is incorrect. The lack of information or reporting may also point to either an information gap regarding one or more indicators, or to a threat deception effort. If the S-2 identifies either of these situations, the S-2 must then consider adjusting the ISR effort. Ultimately, the brigade S-2 must determine the significance of the threat information as it relates to the following basic questions:

- Does the information confirm or deny forecasted threat COAs?
- Does the information confirm or deny predicted threat objectives?
- Does the information identify new threat COAs and objectives?
- Does the information answer the commander's requirements?

UPDATE CURRENT INTELLIGENCE

5-28. In order to support the commander's situational understanding intelligence products and databases must be updated continuously. The S-2's primary method of updating the commander is through personal interaction, briefings, and updates to the threat portion of the COP. Concurrently, the S-2 section—

- Updates the threat situation graphic.
- Updates the intelligence database.

- Develops intelligence reports or summaries.
- Recommends adjustments or redirection of ISR operations to the S-2.

TARGETING METHODOLOGY

5-29. The methodology used to facilitate the attack of the right target with the right asset at the right time is **DECIDE**, **DETECT**, **DELIVER**, and **ASSESS** (**D3A**). The D3A methodology is designed to assist the commander in the decision-making process and facilitates synchronizing maneuver, intelligence, and fire support. In current operations forces have used modified targeting methodologies. See JP 3-60 and FM 6-20-10 for information on targeting and targeting TTP.

TARGET DEVELOPMENT

5-30. The target development process is the systematic evaluation and analysis of target systems, components, and elements to determine HVTs for potential attack through maneuver, fires, or information. An HVT is an asset or capability that the threat commander requires for the successful completion of a specific action. The target development process results in a list of these HVTs that the FS staff uses to identify HPTs and to create an FS plan. The analytic products developed during the process also serve as the basis for battle damage assessment (BDA) of selected HPTs linked to DPs. The target development process consists of the following interactive tasks.

- Identify target system.
- Identify target system components.
- Conduct modeling andwargaming.
- Identify target component elements.
- Perform target validation.
- Prepare preliminary documentation.
- Establish collection requirements.

IDENTIFY TARGET SYSTEM

5-31. In the first task in the target development process, the Analysis and Integration Platoon identifies the target systems that support specified threat activities. The platoon first groups target systems according to geographic and functional areas. The geographic area includes the brigade's AO, AOI, or a specific part of these areas. The functional areas include the warfighting functions of movement and maneuver, intelligence, fires, sustainment, C2, and protection. Using the threat templates from IPB and access from databases, the platoon identifies the geographic or functional target systems that the threat commander would consider a strength or weakness in his or her ability to execute operations and achieve his or her objective.

5-32. For example, to achieve the objective of delaying a threat offensive operation, the platoon might recommend that the brigade attack the threat's logistics system to reduce the threat's capability to sustain its offensive action. However, while an attack against the logistic system may render that system inoperable, this does not guarantee the slowing of the threat offensive. The threat may have sufficient supplies in the basic load of its forward units to achieve its tactical objective. Table 5-2 provides an example of FS as a target system.

IDENTIFY TARGET SYSTEM COMPONENTS

5-33. Once the Analysis and Integration Platoon has identified the target systems, the second task is to examine the various system components. A system component is a set of targets within a target system performing a similar function. For example, the FS system components might include target acquisition (TA), attack system, C2, and service support. Network nodal analysis of the components of an insurgent

system might include the political infrastructure, main line combat forces, people's (local) militia, logistical support structure, and intelligence systems.

5-34. Using IPB situation templates, the platoon analyzes criticality and vulnerability of the target system components. This refined HVT list helps the operations, intelligence, FS, and other staff members during COA development and wargaming.

Table 5-2. Example of a conventional target system's components and elements

SYSTEM	*COMPONENTS*	*ELEMENTS*
Fire Support	Target Acquisition and Battlefield Surveillance	• Observers and Scouts • Radars • MI Units • Army Aviation • Frontline Troops
	Attack Systems and Munitions	• Field Artillery • Mortars • Tactical Air Support • Naval Gunfire • Army Aviation • Electronic Warfare
	Command and Control	• Facilities • Systems
	Sustainment	• Munitions Storage • Transportation

Criticality

5-35. Criticality is a measure of the relative importance of components within a target system as they relate to specific objectives. If the objective is to eliminate the threat FS system, the staff might determine that their target acquisition (due to numbers, capabilities, and doctrine) is the critical component of the FS system. Targets are evaluated based on the extent that the loss of them undermines the threat's ability to execute its plan and contributes to accomplishing the brigade commander's objectives. For this reason, target development focuses on identifying critical nodes within key target systems to satisfy targeting objectives and to conform to the commander's guidance.

Vulnerability

5-36. Vulnerability is a measure of the brigade's ability to detect (identify, locate, and track) and deliver (lethal or nonlethal attack) the desired effect (destroy, degrade, or neutralize). The end product of the identifying target system components is an unconstrained prioritized list of HVTs reflecting relative importance of the targets. A target may not be physically vulnerable to brigade assets. If, however, it is critical to brigade operations, it should be retained on the HVT list to provide impetus for requesting support from higher echelons. A key point in assessing the vulnerability of a target or target system is the ability of the brigade to effect a favorable change in the target's activity and not necessarily the brigade's ability to physically destroy the target or target system.

5-37. The platoon should include all potential targets in the analysis. Analysis should be as thorough as circumstances, time, and resources allow. After the individual targets have been identified for analysis, the S-2 should gather intelligence describing the characteristics of these targets.

CONDUCT MODELING AND WARGAMING

5-38. The third task in target development is for the Analysis and Integration Platoon to analyze the relationship between target components. The platoon must estimate and weigh the contribution of each target component to overall threat activity. For example, the destruction of service support rather than target acquisition might be deemed critical to the threat's ability to conduct FS.

5-39. After the analysis, the brigade FS staff can then determine the potential means of disrupting a related target set. The outcome of the modeling or COA development is a prioritized list of HPTs and associated targeting PIRs and represents targets that will best achieve or contribute to the commander's objectives. At this point the list is still unconstrained, as some of the targets may not be vulnerable to the effects that friendly forces can bring to bear upon them. The target list contains specifically designated and militarily significant components, elements, and activities against which future attack operations may be directed. At this point in the targeting process, the HPT list has not been finalized, and constitutes only a working list requiring further evaluation before specific execution planning.

IDENTIFY TARGET COMPONENT ELEMENTS

5-40. In the fourth task, the Analysis and Integration Platoon takes the list of HPTs developed during wargaming and identifies the target component elements. A target component element is the smallest identifiable activity or function of a target component. Just as components are essential parts of a target system, target elements are the essential parts of a target component. As illustrated in table 6-2, the component elements of an FS attack system might include field artillery (FA) pieces, mortars, and electronic attack (EA).

5-41. The one additional factor the platoon considers when selecting a target component element is the level of damage desired or the length of time the damage effect will last. To achieve the commander's objectives, it may not be necessary to destroy the threat artillery pieces because destroying their targeting systems will render them ineffective. With the advent of more precise fire and attack systems, it is now possible to effectively engage a whole series of smaller, more intricate target elements with precision-guided munitions (PGMs).

PERFORM TARGET VALIDATION

5-42. The fifth task in target development is for the Analysis and Integration Platoon to assist the FS staff in validating the target by considering legal restrictions, ROE, or other limitations. Based on this evaluation, the platoon confirms or nominates new targets to the FS staff for the HPT list. As a general rule, the brigade staff should validate targets as early as possible in the targeting process. The brigade staff must consider the following when validating targets.

- **Current Situation.** Changes in the situation may require a change in the targeting effort. Assessing the current situation ensures the targets remain consistent with the commander's objectives and intent.
- **Law of Armed Conflict.** The law of armed conflict should be considered throughout the target selection process to ensure efficient use of planning assets. Support from the BOLT is essential during all phases of the process to ensure the appropriate and necessary intelligence is available to the appropriate decision maker.
- **Emerging Targets**. New or better targets may prove to be invalid because they are no longer operational or important.

PREPARE PRELIMINARY DOCUMENTATION

5-43. The sixth task in the target development process is for the S-2 to prepare target graphics and target folders on each HPT. Documentation includes messages produced during the earlier tasks of target development, particularly ROE and clearance messages generated during validation.

ESTABLISH COLLECTION REQUIREMENTS

5-44. In the last task, the Analysis and Integration Platoon integrates TA and assessment requirements for each HPT into the intelligence running estimate and ISR plan. The FS staff must articulate its intelligence requirements early in the targeting process to support RM, target development, and eventual combat assessment. In general, each HPT equates to a PIR that the brigade commander must prioritize against other PIRs. The target elements associated with that HPT form the basis of the requirement that the platoon uses to develop the ISR tasks or RFIs to support the “detect” and “assess” functions of the targeting process.

5-45. In conducting target development, there will normally be collection requirements because the S-2 cannot identify all target elements. For example, when attempting to identify the target elements, the Analysis and Integration Platoon may find that for the command, control, and communications system to function there is a missing communications node in the database. This is the time when the platoon attempts to pull or access information from EAB; or through the RM process, requests the intelligence from EAB; or directs subordinates to collect the missing information.

5-46. The principles of the targeting process apply in major combat operations (MCO), SSCs, and peacetime military engagements (PMEs). The platoon must consider the increased use of nonlethal fires and need for precision. The platoon may interact and coordinate with nontraditional elements and agencies like private organizations, other federal and civil agencies, multinational forces, and HN forces to collect targeting data. The brigade commander and the FS staff need to clearly articulate the desired goal of the “fires.”

5-47. See FM 34-3, FM 6-20-10, and JP 2-03 for more information on the "decide" function and target development aspects of the targeting process.

COMBAT ASSESSMENT

5-48. Combat assessment is the determination of the overall effectiveness of force employment in military operations. It is composed of three major components: BDA, munitions effects assessment (MEA), and reattack recommendation (JP 1-02). Intelligence normally provides BDA. Fires support provides MEAs. However, combat assessment, especially reattack recommendations involves not only targeting but also the current operations.

BATTLE DAMAGE ASSESSMENT

5-49. BDA is the estimate of damage resulting from the application of lethal or nonlethal military force. BDA is composed of physical damage assessments (PDAs), functional damage assessments (FDAs), and target system assessments (TSAs). Although BDA is primarily an intelligence responsibility, it is integrated into the targeting process and requires input from and coordination with operations and fire support staffs. Figure 5-1 shows combat assessment coordination.

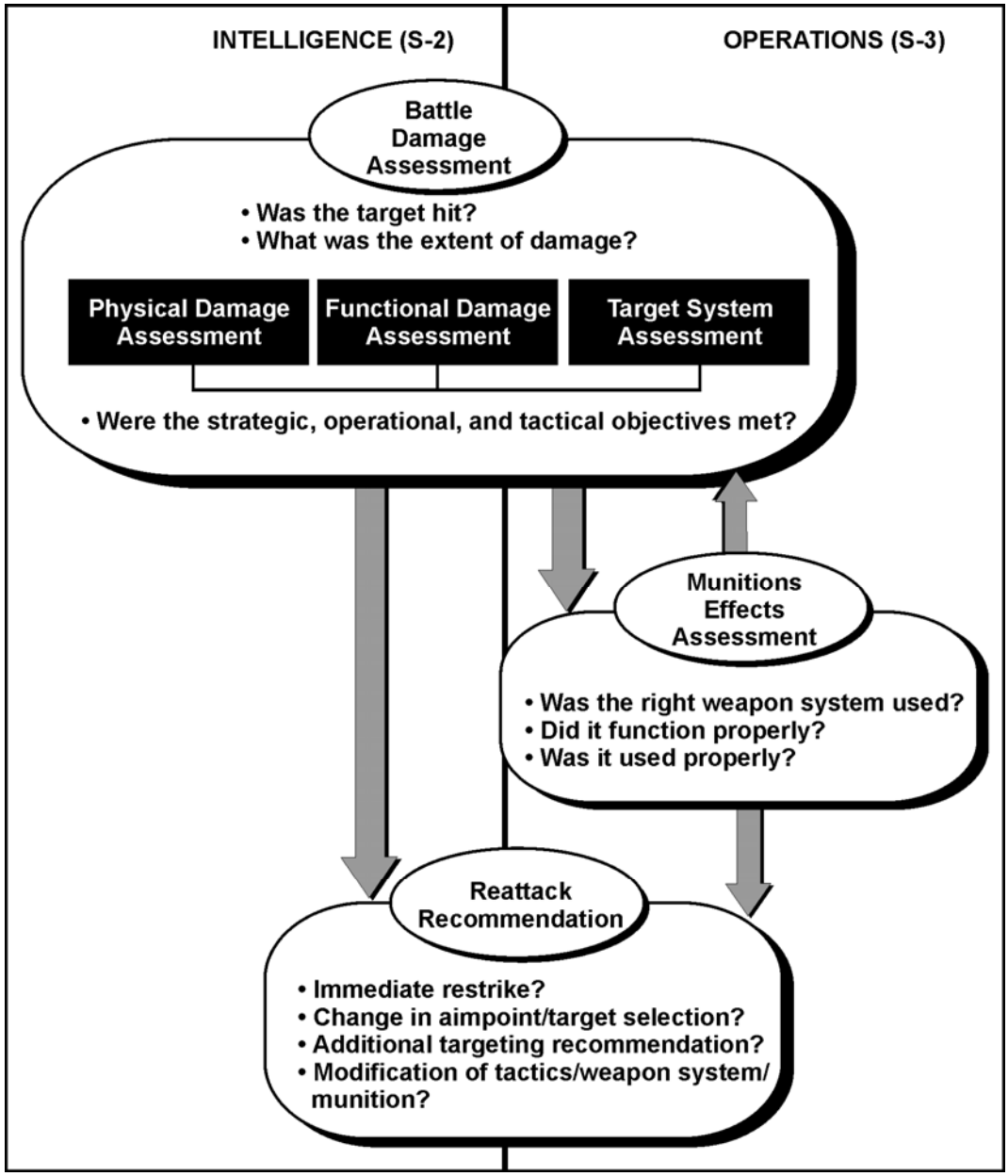


Figure 5-1. Combat assessment coordination

5-50. The most critical ingredient for an effective assessment is a comprehensive understanding of the commander's objectives and how they relate to a specific target. The brigade uses maneuver, fires, and IO against an HPT to effect a change in that target's actions or capabilities. The Analysis and Integration Platoon assesses the success of the targeting in relation to the desired effect. This task is significant when applying the assessment to IO.

5-51. Often the only indicator of the effects of the IO is through long-term surveillance of target activity to see if it has been modified. For example, in a stability operation, friendly forces are frequently met with anti-US demonstrations that block roads and, in general, prevent friendly forces from moving through the AO. The commander's objective is to reduce the anti-US demonstrations through offensive IO. The brigade targets local population with PSYOP through US engineer and medical support projects in the AO. The

demonstrations will probably not stop over night, but the platoon can assess the success of the IO "fires" over time by a decrease in anti-US demonstrations and by a change in local public opinion toward the US forces. The three components of combat assessment are—

- PDA (sometimes called the target damage assessment).
- FDA.
- TSA.

Physical Damage Assessment

5-52. The PDA is an estimate of the extent of physical damage to a target based upon observed or interpreted damage. This post-attack target analysis should be a coordinated effort among all units. The following are representative sources for data needed to make a PDA.

- Mission reports.
- Imagery.
- Weapon system video.
- Geospatial intelligence (GEOINT), HUMINT, imagery intelligence (IMINT), measurement and signature intelligence (MASINT), SIGINT, and OSINT.
- Visual reports from ground spotters or combat troops, controllers, and observers.
- Artillery target surveillance reports.
- Combat information reports.

5-53. When the target is under observation by visual or technical means, the observing unit can provide the initial PDA and may recommend an immediate reattack before sending the report to the Analysis and Integration Platoon for further analysis. Certain FS systems such as artillery and attack helicopters may be able to provide their own initial report on target physical damage. The desired effect is compared to the reported PDA to identify force employment problems or requirements for reattack. In nonlethal attacks, there may not be any physical damage.

Functional Damage Assessment

5-54. The FDA is an analytical task that the Analysis and Integration Platoon conducts in cooperation with the FS staff. The FDA estimates the remaining functional or operational capability of a targeted unit, facility, or object. Functional assessments are inferred from the assessed physical damage and the perceived modification of target activity. The FDA also includes estimates of the threat's ability to recuperate to include the time required to resume normal operations. The FDA integrates the initial target analysis with other related sources, including GEOINT, HUMINT, IMINT, MASINT, SIGINT, and OSINT; and then compares the original objective with the current status of the target to determine if the objective has been met.

Target System Assessment

5-55. The TSA is the Analysis and Integration Platoon's estimate of the overall impact of force employment against an adversary target system. The platoon fuses all component PDAs and FDAs on targets within a target system and assesses the overall impact on that system's capabilities. For example, the platoon may combine the FDAs of the threat's tanks, infantry fighting vehicles, and reconnaissance vehicles to determine the overall damage to the maneuver system. This process lays the groundwork for future attack recommendations.

MUNITIONS EFFECTS ASSESSMENT

5-56. The MEA is conducted concurrently and interactively with BDA, since the same visual signatures used to determine the level of physical damage also give clues to munitions effectiveness. MEA is primarily the responsibility of operations and FS personnel, with inputs from the intelligence staff. MEA analysts seek to identify through systematic trend analysis, any deficiencies in weapon system and

munitions performance or combat tactics by answering the question, "Did the forces employed perform as expected?" Using a variety of inputs (targeting analysts, imagery analysts, structural engineers, weaponeers, and mission planners), operations and FS personnel prepare a report assessing munitions performance. Reports should detail weapon performance against specified target types. This information could have a crucial impact on future operations and the quality of future BDA.

REATTACK RECOMMENDATION

5-57. Reattack recommendations follow directly from both BDA and MEA efforts. Basically reattack recommendations answer the question, "What can be done to fix problems identified by BDA and MEA?" Evolving objectives, target selection, timing, tactics, weapons, vulnerabilities, and munitions are all factors in the new recommendations, combining both operations and intelligence functions.

5-58. See FM 6-20-10, FMI 5-0.1, and JP 2-03 for more information on the assessment function of the targeting process.

This page intentionally left blank.

Chapter 6

Analyze, Disseminate, and Assess Intelligence

Intelligence is of no value unless it reaches those who need it in a timely manner. Analysis is key in converting combat information and single-source intelligence into all-source intelligence products and targeting information. Information received from multiple sources is analyzed and critical information is identified; the timeliness, relevancy, and accuracy of the information is determined; and conclusions are reached. These conclusions are immediately disseminated, used to form recommendations to the commander, or used to form the basis of intelligence analysis products.

Disseminating intelligence entails using information management techniques and procedures in conjunction with the tools of the ABCS. DCGS-A assists the intelligence staff in delivering timely, relevant, accurate, and predictive intelligence to the commander, staff, and subordinates. DCGS-A also provides the BCT with secure, redundant, dedicated broad-bandwidth communications with multi-security levels that enable the timely exchange of analytic findings and metadata.

OVERVIEW

6-1. Intelligence operations generally include the six steps that constitute the intelligence process: generate knowledge, plan, prepare, collect, process, and produce. Additionally, there are five functions that occur throughout the six steps of the intelligence process: commander's input, reach, analyze, assess, and disseminate. For more information on the six steps of the intelligence process and the five functions see the revised FM 2-0 when published.

6-2. Analysis occurs throughout the intelligence process. The intelligence staff analyzes intelligence, information, and problems to produce intelligence, solve problems and, most importantly, answer the PIRs. The intelligence staff—

- Analyzes each requirement to determine its feasibility, whether or not it supports the commander’s intent, and to determine the best method of satisfying the IRs.
- Analyzes collected information to determine if it satisfies requirements. They analyze information from multiple sources to develop all-source intelligence products.
- Analyzes information and intelligence to ensure the focus, prioritization, and synchronization of the unit’s intelligence production is in accordance with the PIRs.
- Analyzes information to determine its significance relative to predicted enemy COAs and the CCIRs (PIRs and FFIRs).
- Through predictive analysis, attempts to identify enemy activity or trends that represent opportunities or risks to the friendly force.
- Uses the indicators developed for each enemy COA and CCIRs (PIRs and FFIRs) during the MDMP as the basis for their analysis and conclusions.

6-3. The intelligence staff disseminates intelligence within the staff to higher, adjacent, and subordinate headquarters. Through the intelligence staff, the S-2 integrates IPB and threat situation products into decision-making and planning processes. The S-2 ensures the timely delivery and presentation of intelligence in a form that is readily understood and directly usable by the unit commander, staff, and subordinates. These products should not overload the commander, staff, or the unit’s information system capabilities. During multinational operations, the S-2 must work with approving authorities to ensure classification and releasability instructions support the timely dissemination of intelligence and CI products to multinational forces.

6-4. Dissemination consists of both "push" and "pull" dissemination techniques:

- The push technique allows the unit to send tailored intelligence products down to its subordinate units and across to adjacent units. Subordinate units can also push products up to the next higher command. Examples of these products include—
  - Early warning and previously unanticipated threat activity or information on other conditions of the operational environment affecting operations.
  - Responses to the PIRs of subordinate units.
  - Tailored products that the unit or staff requested in advance.
  - Current threat situation graphics and reports.
- The pull technique allows units to retrieve products considered relevant to their operations and consumes less communications and processing resources. The pull technique involves the unit intelligence staff having direct electronic access to databases, intelligence files, web-based homepages, or other repositories of higher and lower echelon intelligence organizations. Pulling intelligence is preferable to submitting RFIs, provided the desired information already exists in a usable form in an accessible database or website.

6-5. The S-2 needs to continuously evaluate the intelligence dissemination process and systems. Intelligence personnel at all levels assess the success of the dissemination task and make changes as needed to improve the flow and presentation of intelligence. The evaluation looks at—

- The transition from dissemination to the next iteration of the intelligence process.
- Adherence to dissemination standards.
- Performance improvements to the organization and the process.
- Commander and staff feedback.

6-6. See FM 2-01, FM 6-02.2, JP 2-01, and the ABCS Staff Leader's Guide for additional information.

ANALYZE

6-7. All-source and intelligence discipline analysts of the Analysis and Integration Platoon use a number of methods to analyze threat forces. FM 34-3 and FM 2-22.3 provide details on the analysis methods that intelligence analysts commonly use. Each intelligence discipline may use variations of these methods to analyze information unique to their specialty. The following paragraphs describe pattern analysis, indicator analysis, and analysis of threat characteristics.

6-8. There are three basic analytical products (time event charts, matrices, and link analysis diagrams) and various automated tools that are particularly useful to intelligence analysis. Each of these analytical products incorporates fragmented bits of information and organizes them into a chart, diagram, or matrix that can easily be read. Analysts typically use automated software programs (such as Analyst Notebook) on DCGS-A to create these products. However, the examples of the analytical products provided here are basic manual depictions. There are several advantages to using computer programs: products can be shared over networks and portals and it is a more efficient means of managing large quantities of individual bits of information.

PATTERN ANALYSIS

6-9. Pattern analysis is the process of deducing the doctrine and TTP that threat forces prefer to employ by carefully observing and evaluating patterns in their activities. This technique is based on the premise that threat COAs reflect certain characteristic patterns that can be identified and interpreted. Pattern analysis can be critical when facing a threat whose doctrine is adaptable, undeveloped, or unknown; thus, it is necessary to create your own threat model and threat templates. The following three tools can help intelligence analysts to determine operational patterns and create and update their threat model.

- Incident Overlay.

- Pattern Analysis Plot Sheet.
- Link Diagram.

Incident Overlay

6-10. Figure 6-1 is an example of an incident overlay. It illustrates cumulative events that have occurred within the AO and focuses on the "where" of an event. The intelligence analyst may use multiple incident overlays that focus on a different subject or blend subjects. Normally, the incident overlay includes additional information such as notes or graphics. The intelligence analyst should use the incident overlay in conjunction with the pattern analysis plot sheet.

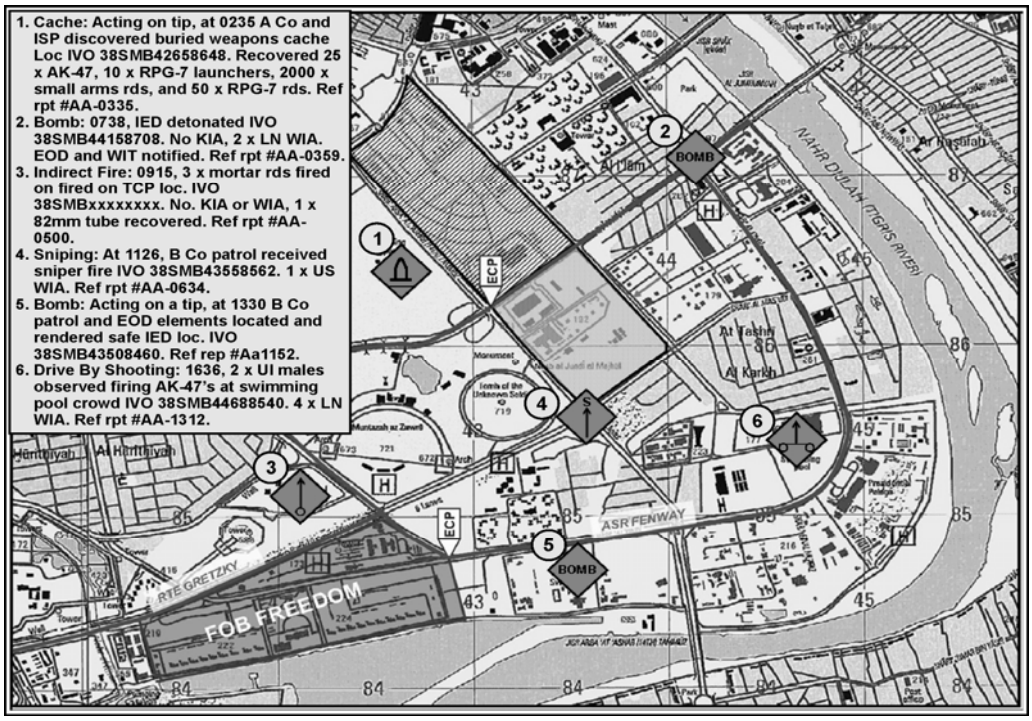


Figure 6-1. Incident overlay

Pattern Analysis Plot Sheet

6-11. The analyst uses the pattern analysis plot sheet to focus on the "time" and "date" of each serious incident that takes place within the AO. The pattern analysis plot sheet helps distinguish patterns in activity that are tied to particular days, dates, or times. When used in conjunction with the incident overlay and any threat templates, a pattern analysis plot sheet supplies the bulk of the data needed to complete an event template. Figure 6-2 is an example of a pattern analysis plot sheet.

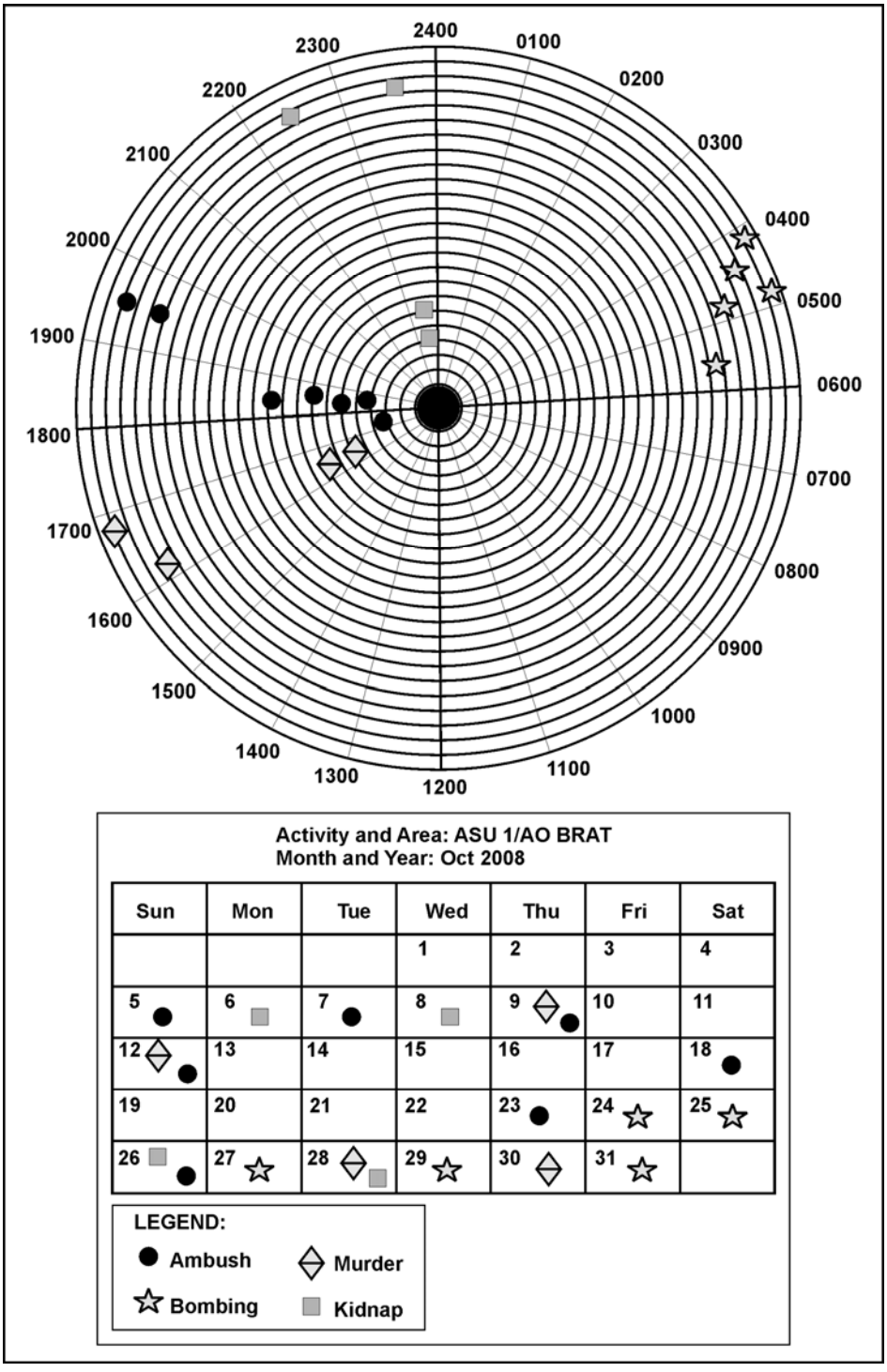


Figure 6-2. Pattern analysis plot sheet

LINK DIAGRAM

6-12. A link diagram combines the association, relationship, and activities matrices into a single graphic. It shows how individuals and functional groups of individuals are related. By analyzing it, you can determine intelligence gaps.

ASSOCIATION MATRICES

6-13. The association matrix is used to establish the existence of an association, known or suspected, between individuals. "Direct connections" include, for example, face-to-face meetings or confirmed telephonic conversations. Figure 6-3 provides a one-dimensional view of the relationships and tends to focus on the immediate AO. Analysts can use association matrices to identify those personalities and associations needing a more in-depth analysis in order to determine the degree of relationship, contacts, or knowledge between the individuals. The structure of the threat organization is formed as connections between personalities are made.

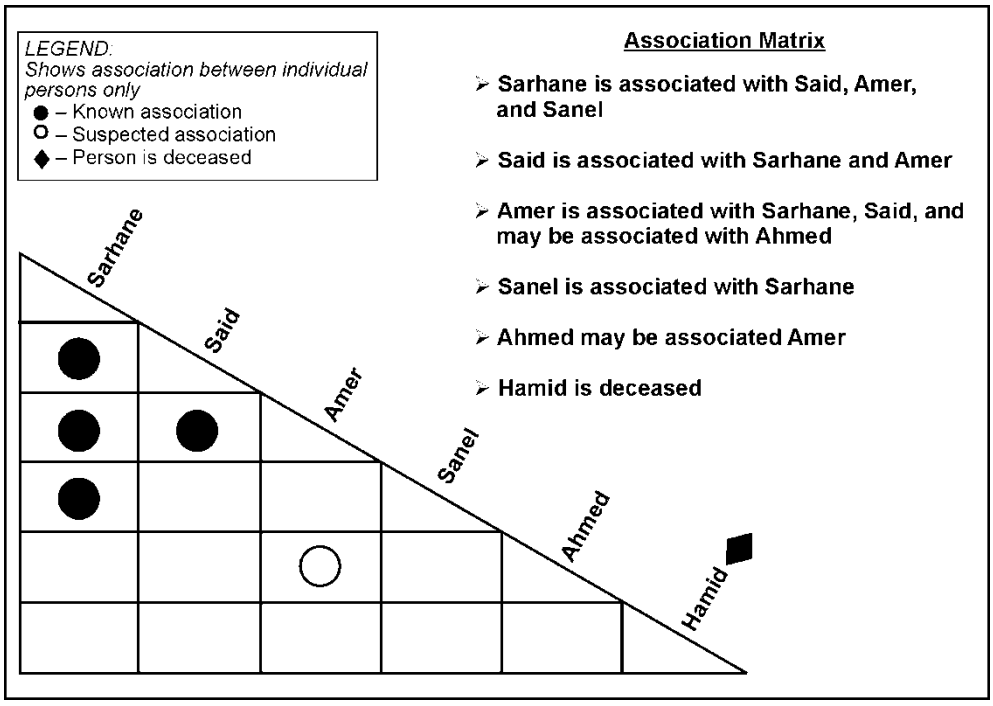


Figure 6-3. Association matrix

RELATIONSHIP MATRIX

6-14. Relationship matrices are intended to depict the nature of relationships between elements of the AO. The elements can include members from the noncombatant population, the friendly force, international organizations, and an adversarial group. Utility infrastructure, significant buildings, media, and activities might also be included. The nature of the relationship between two or more components includes measures of contention, collusion, or dependency. The purpose of this tool is to demonstrate graphically how each component of the city interacts with the others and whether these interactions promote or degrade the likelihood of mission success. The relationships represented in the matrix can also begin to help the analysts in deciphering how to best use the relationship to help shape the operational environment.

6-15. The example relationship matrix shown in figure 6-4, while not complete, is intended to show how the relationships among a representative compilation of population groups can be depicted. This example is an extremely simple version of what might be used during an operation in which many actors and other

population elements are present. For instance, the section marked "Population" might include considerably more population subgroups than the two included in this sample. When used during a deployment, it is important for the analysts to realize what groups, subgroups, and other elements should be represented in the matrix. In addition, it should be noted that the matrix could be used to depict the perceived differences in relationships. For example, in figure 6-4, Political Group 3 is shown to have a dependent relationship with Economic Group 1. The complementary relationship (a similar mark in the corresponding box linking Political Group 3 and Economic Group 1) is not indicated because it might not exist.

6-16. To illustrate the usefulness of the matrix, consider the relationship of the government with the infrastructure. In this case, the relationship is "friendly," perhaps because the government is in control of the infrastructure without contest from the owners or suppliers of the infrastructure. For example, this could be considered the case when Slobodan Milosevic controlled the electricity supply for Kosovo. Milosevic apparently used the infrastructure at his disposal to supply electricity to the population, but intermittently threatened to deny the service in order to maintain control over a possibly hostile population. How can this information be used by the commander and the staff? Perhaps by understanding the nature of two elements of the AO, the link between the two elements can either be eliminated or leveraged in order to suit the needs of the friendly unit.

6-17. Using figure 6-4, there is a relationship of possible collusion that exists between the government and Political Group 3, and a friendly relationship between the government and the media. Some questions the intelligence analyst might ask when reviewing this information include—

- How can the government use the media to its advantage?
- Will the government seek to discredit Political Group 3 using the media?
- Will the population view the media's reporting as credible?
- Does the population see the government as willfully using the media to suit its own ends?

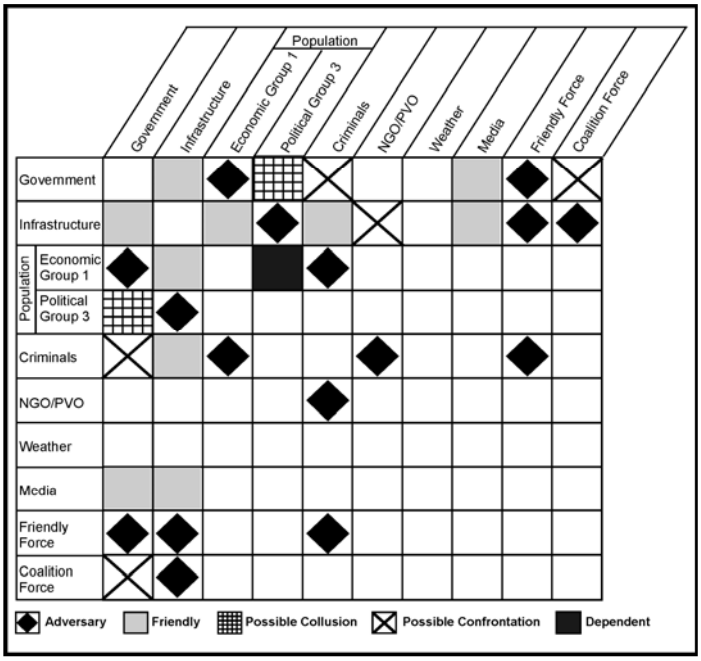


Figure 6-4. Relationship matrix

ACTIVITIES MATRIX

6-18. Activities matrices help analysts connect individuals (such as those in association matrices) to organizations, events, entities, addresses, and activities—anything other than people. Information from this matrix, combined with information from association matrices, assists analysts in linking personalities as

well. The activities matrix, as shown in figure 6-5, is constructed in the shape of a rectangle, with rows and columns tailored to the needs of the analyst in depicting the problem at hand.

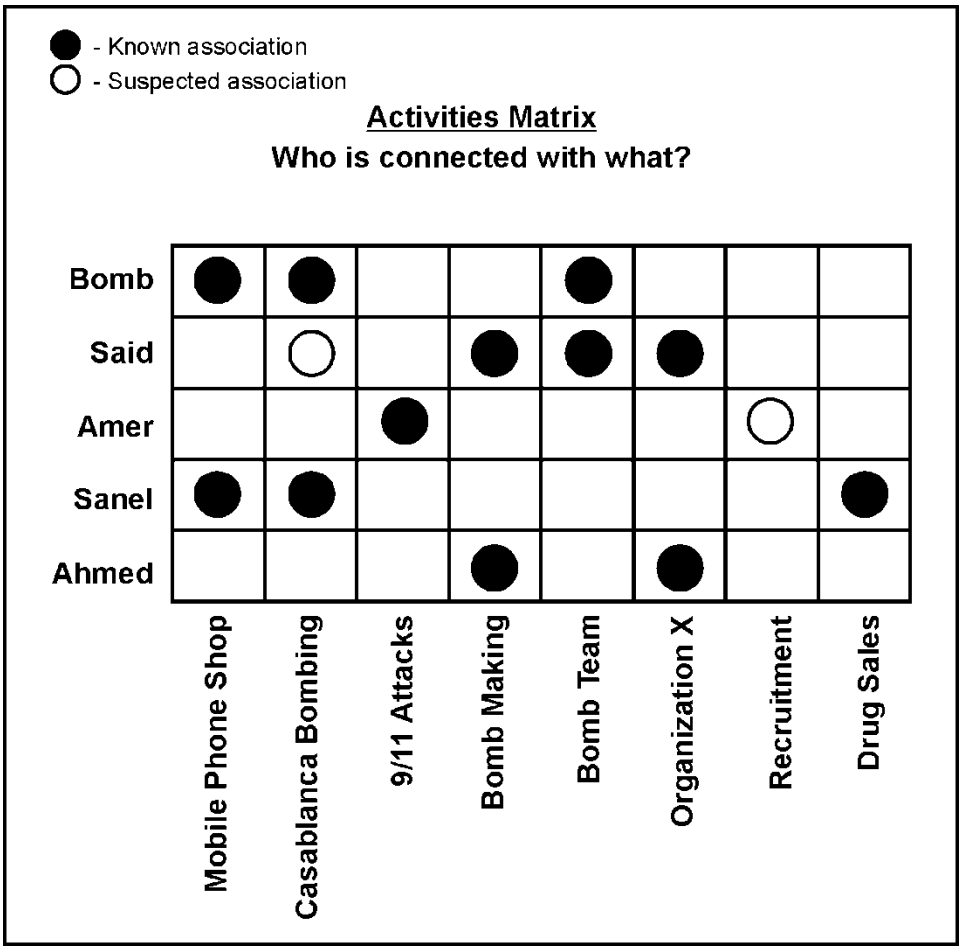


Figure 6-5. Activities matrix

TIME EVENT CHART

6-19. Time event charts, as shown in figure 6-6, are chronological records of individual or group activities designed to store and display large amounts of information in a small space. Analysts can use time event charts to help analyze larger-scale patterns of activity and relationships. There is great latitude in preparing a time event chart; some of the common characteristics are that the beginning and end of the chart are shown with triangles; other events with squares; particularly noteworthy events have "X's" drawn across the square; the date is always on the symbol; a description is below the symbol; and the flow is from the left to the right, for each row employed.

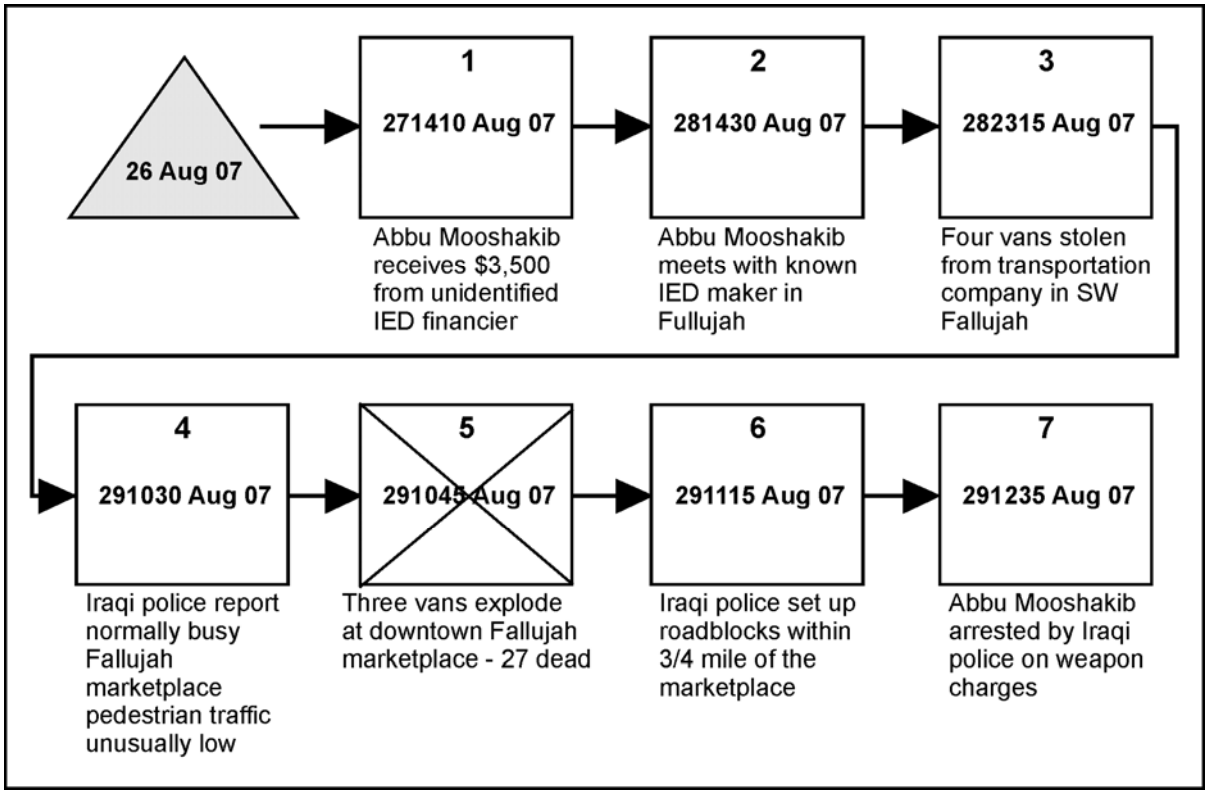


Figure 6-6. Time event chart

LISTS AND TIMELINES OF KEY DATES

6-20. In many operations, including most stability operations, key local national holidays, historic events, and significant cultural and political events can be extremely important. Soldiers are often provided with a list of these key dates in order to identify potential dates of increased or unusual activity. These lists, however, rarely include a description of why these dates are significant and what can be expected to happen on the holiday. In some cases, days of the week themselves are significant. For example, in Bosnia weddings were often held on Fridays and celebratory fire was a common occurrence on Friday afternoons and late into the night. Timelines—a list of significant dates along with relevant information and analysis—seek to provide a context to operational conditions. These timelines could include descriptions of population movements or political shifts that are relevant to the AO. They could also include a brief historical record of the population or area, highlighting the activities of a certain population sector. As analytic tools, timelines might help the intelligence analyst predict how key sectors of the population might react to given circumstances.

CULTURE DESCRIPTION OR CULTURAL COMPARISON CHART OR MATRIX

6-21. In order for the intelligence analyst to avoid the common mistake of assuming that only one perspective exists, it may be helpful to clearly point out the differences between local ideology, politics, predominant religion, acceptable standards of living, norms, regional populace interests, and US norms. A culture comparison chart can be a stand-alone tool, listing just the different characteristics of the culture in question, or it can be comparative—assessing the host country population relative to known and familiar conditions. See figure 6-6 for a cultural comparison chart.

VALUE	*WESTERN*	*MIDDLE EASTERN*
Individualist and Collectivist Societies: **Individualists** hold that the individual is the primary unit of reality and the ultimate standard of value. **Collectivists** believe everyone belongs to a certain group; the group protects its "members" and expects their loyalty in return.	***Individualist*** *Self-sufficient* *Independent* *Personal achievement*	***Collectivist*** *Team work (Family)* *Reliance/Patronage* *Family honor*
Universalism and Particularism: **Universalists** are more likely to apply absolutes regardless of circumstances or situation; the same rules apply to everyone in like situations. **Particularists** believe one's behavior in any given situation depends on specific circumstances.	***Universalist*** *Right is right/wrong is wrong* *Treat everyone alike* *Everyone has the same rights*	***Particularist*** *Right and wrong is situation dependent* *Life is not fair* *Exceptions made for certain people*
Achieved and Ascribed Status: How different cultures deal with different levels of status.	***Achieved Status*** *Earn status through work*	***Ascribed Status*** *Status through birth, age, or seniority*
Uncertainty Avoidance: The ability of people in a specific culture to adapt to changes or the unknown. Those with high uncertainty avoidance do not like change and, to some extent, fear the unknown. People with low uncertainty avoidance do not feel so threatened or anxious about uncertainty and are curious rather than frightened of the unknown.	***High Uncertainty Avoidance*** *Unknown is frustrating*	***Low Uncertainty Avoidance*** *Curious of unknown*

Figure 6-7. Cultural comparison chart

PERCEPTION ASSESSMENT MATRIX

6-22. Perception assessment matrices are often used by PSYOP personnel and can be a valuable tool for intelligence analysts once completed by trained PSYOP personnel. Friendly force activities intended to be benign or benevolent might have negative results if a population's perceptions are not considered, then assessed or measured. This is true because perceptions—more than reality—drive decision making and in turn could influence the reactions of entire populations. The perception assessment matrix seeks to provide some measure of effectiveness for the unit's ability to reach an effect (for example, maintain legitimacy) during an operation. In this sense, the matrix can also be used to directly measure the effectiveness of the unit's CA, Public Affairs, and PSYOP efforts.

6-23. One proposed PSYOP program developed for Operation RESTORE DEMOCRACY in Haiti illustrates why perception assessment is necessary. Prior to deployment, leaflets were published informing the Haitian populace of US intentions. The original leaflet was published in Dutch, the language of the Haitian elite. The one actually used for the PSYOP program was published in Creole, the official language of Haiti, because an astute PSYOP team member realized the need to publish to the wider audience.

6-24. If the Dutch flier had been dropped on Port-au-Prince, it could have undermined the American mission to the country in several ways. The majority of the population would have been unable to read the flier. The subsequent deployment of US forces into the country, therefore, could have been perceived to be hostile. The mission itself, which was intended in part to restore equity within the nation's social structure,

could have backfired if the Haitians viewed the Dutch flier as an indication of US favoritism to the Haitian elite.

6-25. Perception can work counter to operational objectives. Perceptions should therefore be assessed both before and throughout an operation. Although it is not possible to read the minds of the local national population, there are several means to measure its perceptions:

- Demographic analysis and cultural intelligence are key components of perception analysis.
- Understanding a population's history can help predict expectations and reactions.
- HUMINT can provide information on population perceptions.
- Reactions and key activities can be observed in order to decipher whether people act based on real conditions or perceived conditions.
- Editorial and opinion pieces of relevant newspapers can be monitored for changes in tone or opinion shifts that can steer or may be reacting to the opinions of a population group.

6-26. Perception assessment matrices aim to measure the disparities between friendly force actions and what population groups perceive. A sample matrix is shown in figure 6-7. In addition to trying to assess the perceptions of each population group within an AO, it might serve the interests of the unit to assess its own perceptions of its activities. All of the following questions can begin to be addressed by the unit's scrutinizing its view of an operation:

- Are members of the unit exhibiting decidedly Western or American values that are not appreciated by the host country population?
- Are embedded American beliefs preventing the unit from understanding the host country population or its coalition partners?
- Is what the intelligence and command staff perceiving really what is going on in the AO?
- Does the population believe what the unit believes?
- Is there something that is part of the population's (or a subgroup's) perception that can be detrimental to the unit?

Condition	Cultural norm	Alternative proposed by friendly force	Population's perception	Acceptable difference in perception?	Root of difference	Possible to change perception?	Proposed solution	Possible consequences of unchanged perception?
Food	Rice	Meat and potatoes	Inadequate/ Inconsiderate	No	Culturally accepted norms/ standards, no known physically detrimental effects	No; logistically restricted	Just offer potatoes, seek exchange for rice	Starvation, rioting
Use of guns	All men carry weapons	All weapons confiscated	Unfair	No	Culture	No; Soldier safety	PSYOP campaign; weapons turn-in program	Armed backlash
Government structure	Tribal	Hierachical	Tolerable as long as needs are fulfilled by group in charge	Yes	History	No	Bargain	Unknown

Figure 6-8. Perception assessment matrix

INDICATOR ANALYSIS

6-27. Indicators are any positive or negative clue that points toward threat activities, capabilities, vulnerabilities, or intentions. Analysis of indicators requires a number of actions. First, the analyst—

- Examines input (collected information and intelligence).
- Ensures any information pertaining to the indicators is footnoted with details of the event and looks for the development of patterns. If the analyst notices that one group of indicators is being satisfied but another is not, the analyst then looks closely to ensure that an attempt is not being made to deceive.
- Ensures the indicators are valid or that they have not already occurred but were missed. If the analyst is satisfied that the indicators are valid, the analyst reports the findings.

Prioritizing Indicators

6-28. The all-source analysts of the Situation and Target Development Section normally establish a list of indicators and place a priority on each. The section can develop a list of standing indicators or develop indicators specifically to answer the commander's PIR. The analysts use these indicators to cross-reference specific events and activities with probable threat trends and COAs.

Weighing Indicators

6-29. The prioritization of indicators is important in that it establishes the relative weight of one indicator compared to another. Indicators may lead the analyst to develop a hypothesis that may or may not be true. If the indicator was part of a deception plan, then the hypothesis may be incorrect. It is always dangerous to draw conclusions from a single indicator. Each indicator is integrated with other indicators and factors before analysts can detect patterns and establish threat intentions.

THREAT CHARACTERISTICS

6-30. Threat characteristics analysis does not predict threat intentions or probable COAs but is a means of cataloging intelligence data that qualifies and quantifies certain aspects of threats. The analyst considers the characteristics shown in table 6-1 to focus the analysis. The situation may dictate that one or more of the factors receive a higher priority than another. For asymmetrical operations, additional analysis of threat characteristic categories of personalities, culture, and internal organizational processes are added.

DISSEMINATE

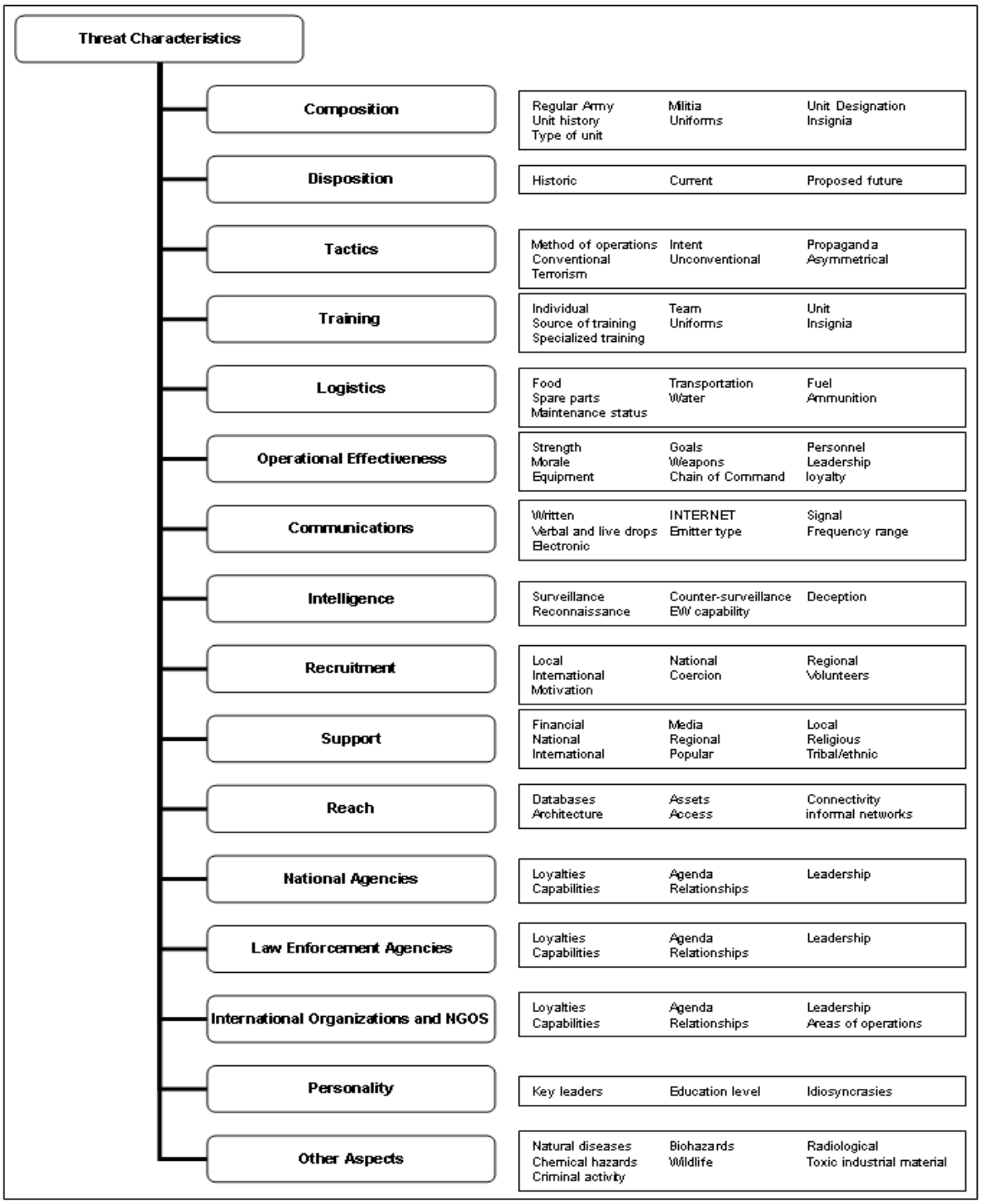
6-31. The intelligence staff ensures that combat information and intelligence products are provided to commanders and other users as soon as possible and prior to LTIOV when identified. Intelligence and information must be in a format supportive of situation development, IPB, targeting, or protection requirements. The intelligence staff is responsible for ensuring that any dissemination is done in accordance with AR 381-10, Procedure 4, and other applicable security regulations. During operation planning, the intelligence staff coordinates with the brigade staff, subordinate commands, and EAB J-2/G-2 to ensure that specific assets, personnel, equipment (especially communications), and procedures are available for disseminating intelligence and intelligence products within the AO.

6-32. The S-2's involvement during operation planning ensures the S-2 understands which intelligence products are needed, required timeliness, consumer locations, and logistics and infrastructure assets available to support intelligence dissemination. This can be extremely important during stability operations when air, ground, and sea assets may be limited and LOCs extended.

6-33. The timely and accurate dissemination of intelligence throughout the brigade is key to successful operations. DCGS-A provides the BCT S-2 with access to theater and national databases reducing the latency in the dissemination of information throughout the brigade and to subordinate units. The intelligence staff works with subordinate S-2s and EAB RM teams, or joint-level dissemination program

managers (DPMs) to get the intelligence products to the user. The staff ensures that appropriate mailing addresses, message addresses and routing indicators, and special security office (SSO) security accreditation are requested and established for those units. This administrative information must be communicated to and validated by the joint-level DPM, who will provide the information to the Defense Intelligence Agency (DIA) and other supporting national agencies.

Table 6-1. Threat characteristics



6-34. DCGS-A supports distributed operations by providing access to data and products across the Intelligence Enterprise and collaboration capabilities across echelons to enhance situational awareness.

However, particularly when dealing with time-sensitive information, the intelligence staff ensures that the user receives the required information before the LTIOV. Relevant information is passed by the most expeditious means to any affected units as well as to the unit initially requesting the information. Information is passed to the appropriate intelligence organization for analysis and incorporation into intelligence products. The staff will perform the following steps:

- **Arrange for Direct Dissemination**. Have ISR assets report directly to the unit needing the information for decisions. This dissemination method is written into the ISR task or RFI if the S-2, with the commander's approval, wants the unit to execute it. If the S-2 allows the asset to report directly to the requesting unit, the intelligence staff provides the S-2 with a copy of the information to update the ISR synchronization plan. Direct dissemination is most commonly used for FA and ADA units and the target nomination process.
- **Determine Perishability.** The intelligence staff, with the approval of the S-2, determines what information will bypass the normal intelligence processing functions and be sent directly to the commander needing it to make decisions based on the criticality of the information and its LTIOV. Within the complement of automated intelligence tools, the S-2 can set DCGS-A information alarms for critical pieces of intelligence. These alarms alert the analyst that the information has arrived prior to its being passed on to the brigade staff. These few seconds or minutes, saved by the alarm capability, are critical in the decision-making cycle of the combat commander.
- **Determine How Much to Disseminate.** The intelligence staff determines the amount of information to disseminate to the higher and subordinate commanders. It may not be important to provide the entire text of a message to the user if the unit location and identification answer the ISR requirement.
- **Identify Media for Dissemination**. This step is unique to each unit. The media for dissemination includes every means of moving information around the battlefield. The unit's intelligence architecture provides this type of information to the S-2. If it does not, the intelligence staff must work with the supporting signal unit to determine communications links and methods between the brigade and the subordinate CPs. The staff provides a list of dissemination systems to all users of the intelligence products.
- **Disseminate.** The final phase involves the actual movement of intelligence around the battlefield. The intelligence staff uses those systems available to provide intelligence products to commanders on time. The staff maintains a tracking system for all outgoing intelligence. To say that one has disseminated the product without verifying that the user received it will not suffice. The staff ensures that the mail arrived. The analyst uses United States Message Text Format formatted messages.

INFORMATION CHANNELS

6-35. Reports and other information move throughout the ABCS along specific channels. These channels help streamline information distribution by ensuring the right information is passed in a timely manner to the right person or element. There are three channels through which commanders and their staffs communicate: command, staff, and technical.

Command Channel

6-36. The command channel is the direct chain-of-command link that commanders, or authorized staff officers, use for command-related activities. Command channels include Internet/Intranet, command radio nets, video teleconferences (VTC), and the Maneuver Control System (MCS).

Staff Channel

6-37. The staff channel is the staff-to-staff link within and between headquarters. The staff uses the staff channel for control-related activities. Through the staff channel, the staff coordinates and transmits planning information, controlling instructions, and other information to support C2. Examples of staff

channels include the operations and intelligence radio net, the staff meeting, and the primary ABCS warfighting function control systems.

Technical Channel

6-38. The technical channel is normally the link between two similar commands within a larger command. Staffs typically use technical channels to control activities. These activities include fire direction and the technical support and sensitive compartmented information (SCI) reporting channels of ISR operations. The EW tasking and reporting radio net, broadcast intelligence communications, and the wide area networks supporting single-discipline collection, processing, and production are examples of technical channels.

6-39. The J/G/S-2X is the doctrinal term used to refer to the CI and HUMINT operations manager that works directly for the J/G/S-2. The terms also refer to the staff section that the 2X leads. The 2X section is organized to provide focus, technical support and control for all CI and HUMINT activities. See chapter 9 figure 9-1 for more information.

INFORMATION MANAGEMENT

6-40. Guided by the XO, the brigade staff uses the information categories, channels, and management process to facilitate information collaboration and exchanges between staff elements, disseminate relevant information, and answer the CCIR. The information management process entails three distinct tasks—filtering, fusing, and focusing information—so that commanders and primary staff officers are not overburdened or distracted by unnecessary details. Even when requirements are well defined, collection normally generates masses of information. Some of that information will be extraneous, irrelevant, or untimely when it arrives; some can become useless or of limited value if it is misdirected or delayed in distribution. Information management is therefore highly time-sensitive and subject-sensitive. Finally, information collection goes on continually and, to be effective, staff leaders must review its results and the CCIR periodically. If information management is not dynamic and self-renewing, the CCIR, which are the process' foundation, will become dated and less supportive of the operation.

6-41. The staff executes each task of the process using the digitally enabled routines and information system tools of the ABCS. During tactical operations, the three tasks are not always distinctively progressive or sequential. The actions of the staff over the period of the operation blend the tasks as success, or the mission changes and variations drive adjustments to the flow. Often, the process is compressed as the mission or operation progresses toward DPs. The process remains intact, however, as information is collected, processed, distributed, reported, and tailored for display.

ARMY BATTLE COMMAND SYSTEM

6-42. ABCS enables commanders to rapidly gain reliable information. ABCS satisfies two critical battle C2 requirements: interoperability and situational awareness. ABCS employs networks that are interoperable with theater, joint, and combined C2 systems. ABCS is a combination of all Army C2 systems, including the following systems:

- Global Command and Control System-Army (GCCS-A).
- Command and Control Personal Computer (C2PC).
- Maneuver Control System (MCS).
- Advanced Field Artillery Tactical Data System (AFATDS).
- Air and Missile Defense Workstation (AMDWS).
- Distributed Common Ground Station-Army (DCGS-A).
- Brigade Command Sustainment Support System.
- FBCB2.
- Integrated Meteorological System (IMETS).

- Digital Topographic Support System (DTSS).
- Tactical Airspace Integration System.

6-43. The brigade ISR architecture is a subset of the brigade's overall C2 system architecture, which is designed to support the ABCS. The ABCS is a multiple-level C2 system that ties together the brigade's C2 efforts from the individual weapons platform to the joint level. ABCS consists of control systems and support systems.

PRESENTATION TECHNIQUES AND PROCEDURES

6-44. The staff's objective in presenting information is to provide the commander with relevant information. Table 6-2 lists the three general methods that the staff uses. Digital systems within the ABCS contain standard report formats, maps, and mapping tools that assist the staff in presenting information in written, verbal, and graphic form. Audio and video systems like large format display and teleconferencing systems found in the digital CP enable the staff to use a combination of the methods in multimedia presentations.

Table 6-2. Presentation methods and products

METHOD	*PRODUCTS*	*REFERENCE*
Written Narrative Report	Reports, Estimates, and Studies	FM 5-0 and FM 1-02
Verbal Narrative Report	Briefings (information, decision, mission, and staff)	FM 5-0
Graphic Display	Charts, Overlays, and SITMAPs	FM 1-02

SITUATION MAPS

6-45. The SITMAP is the primary graphic display within the CP. There are more SITMAPs in the digital CP than there are ABCS monitors. Effective management of SITMAPs is at the core of maintaining an accurate COP. Management ensures the staff does not get overwhelmed or confused, improves decision-maker confidence, and improves presentation of information. Areas of control include SITMAP production, storage, and distribution. The operations and intelligence staffs are the elements most concerned with SITMAP management.

6-46. SITMAPs are constructed initially using existing databases, the orders and supporting graphics from higher headquarters, and current disposition of subordinate units. The staff and subordinate units can forward or update digital overlays by either "push" or "pull" techniques. Generally, SITMAPs are categorized as plans (future operations), current operations, and outdated or completed operations. The plans SITMAPs are produced and distributed by the S-3/S-2 plans team. The current operations SITMAPs can be further typed as either "essential" or "as required." (See table 6-3.) Essential SITMAPs are considered to be those required for normal operations. They must be kept current and open. Other SITMAPs may be required for operations, but are not needed at all times. They will be kept by the responsible staff element and sent to the S-3 operations team as needed.

Table 6-3. Essential and "As Required" SITMAPs

ESSENTIAL	*AS REQUIRED*
• Current friendly situation • Current threat situation • Higher headquarters operations • Unit current operations • Subordinate unit current operations • Fire support • ISR • Army Airspace Command and Control • Engineer	• Air Defense • Signal • Movement • CBRN • Logistics • Sustainment Area

COMMON OPERATIONAL PICTURE

6-47. The COP is the current set of command and staff running estimates, situation graphics, and other relevant data that is understood by and digitally accessible to all parts of a force. As a consolidation of the best available information, the COP reduces the need for queries; forms the basis for discussions, plans, estimates and orders; and accelerates decision cycles. The staff uses this shared mission-focused information to present a tailored graphic display to the decision maker. The COP is derived from a common database created from multi-information sources from within the military information environment and the large global information environment. As a shared reference within a force, the COP provides the structure necessary to support visualization and, as the commander's concept and plan mature, shared situational understanding within the command.

6-48. The brigade represents a critical link in creating and maintaining the digital COP. Staff leaders at brigade face a unique challenge in training and developing procedures that integrate the digitized friendly situation of the FBCB2, with the semi-digital threat situation, and the semi-digitized situations and reporting channels. The brigade battle captains are presented with multiple information feeds from the wide variety of forces in front of, in, adjacent to, and to the rear of the brigade zone. Simultaneously, reporting requirements necessitate an analysis of the FBCB2 information and development of the applicable MCS, or DCGS-A reports to brigade.

6-49. Brigade staff leaders have fewer control systems than a division and a smaller but rapidly changing information load. At this level, particularly when in contact with the threat forces, the volume of internally generated information does not exceed that of analog units. In either kind of unit, when scouts have eyes on the lead threat reconnaissance force, the most likely means of informing the brigade S-2 will be voice. A major challenge in data management at brigade level is to receive, evaluate, analyze, and report multiple pieces of information at a high tempo.

Building the Common Operational Picture

6-50. The COP begins with the staff populating MCS, or DCGS-A enterprise databases from the OPORD of the higher headquarters and existing intelligence database. The staff may not initially set up all the control systems. Normally, the operations and intelligence staffs set up first, followed by other staff elements as required to support planning and developing the COP. The COP matures as the staff executes the MDMP, receives additional guidance, and updates supporting databases and graphics. The staff updates and disseminates the COP at key junctures when planning, preparing, and executing operations.

6-51. Predeployment tempo may require databases and products developed in the garrison. Limited time for planning and preparing prior to deployment may limit the full activation and integration of the brigade's ABCS components until arrival in the AO. Once in the AO, the staff brings up the control systems individually then integrates them into the area networks as the information and communications infrastructure becomes operational.

Design and Focus

6-52. Each commander may need information presented in different formats based on the mission, CCIR, and command philosophy. Similarly, staff leaders need specialized displays that support their own needs and functional area. The COP provides a mechanism for all of these individualized products to be integrated and presented in a common forum. As the standardized base of information, it offers a quick check on the latest information on threat, friendly forces and other conditions of the operational environment, and facilitates discussions between commanders and staff leaders.

6-53. The CCIR and presentation guidance determine the content and focus of the COP at every stage of operations. In determining what the COP should contain, the commander considers the factors of METT-TC and/or the PMESII-PT variables and provides the staff with specific guidance on major elements of information. The commander refines or modifies the COP requirements as the plan matures or operation progresses. To do this, the commander may focus the staff's attention on particular areas, call for greater detail during a critical time, eliminate some subjects that no longer affect success from the COP, or add elements that have assumed greater importance during the operation. For example, as an attacking battalion closes on its objective and success depends on seizing it, the commander may want to concentrate all elements of the COP on close-in and near-term IRs.

Production and Control

6-54. Information products that result from building the COP are manipulated or focused depending on the need to support the commander's accurate visualization as the battle flows toward designated DPs. The COP for units in a JTF, for example, will share all the JTF's operational graphics and refer to the same set of JTF staff running estimates. But two brigade commanders in adjacent sectors in an area defense will shape their COP differently because of differences in terrain, levels of support, and concepts of operation. A third brigade held in reserve will form a broader COP than either of the committed brigades and will lay greater emphasis on factors such as routes, the air defense situation, location and condition of threat forces in depth, and mobility considerations throughout the sector.

6-55. SOPs establish the routine external and internal distribution of products. The digital CP also requires a focal point to control what is displayed, when, to what level of detail, and how often. This control can be as simple as the brigade XO monitoring the TOC information setup to having specially trained and dedicated personnel at the JTF CPs. A separate production center may be an option for control of the multitude of products available to a combat information center (CIC). Production functions also apply for setup and conduct of VTC white board sessions.

Internal and External Awareness

6-56. Each staff element must maintain its portion of the COP as well as awareness of other staffs' products and their information sources. As discussed earlier, the level of the unit and the type of CP drive the mechanics involved in overall operational awareness. The following are some of the mechanisms for maintaining internal and external CP awareness. See FMI 5-0.1 for CP and staff operations.

- **Staff Meetings.** Staff leader interaction remains the key to coordinated update of the COP. Staff leaders conduct frequent staff meetings to cross-check situational information before acting on or forwarding the information. This interaction is more informal within staff elements and at the battalion and brigade levels.
- **Shift-change Briefings.** During continuous operations, CPs normally operate in shifts. To ensure uninterrupted operations, staffs execute a briefing when shifts change (normally ever 12 hours). Depending on the situation, it may be formal or informal and include the entire staff or selected members. To facilitate a quick but effective shift-change briefing, unit SOPs should contain its format and sequence. Normally the meeting is face-to-face among key CP leaders. The XO oversees the briefing, with participants briefing their areas of expertise. The briefing's purpose is to inform the incoming shift of –
  - Current unit status

- Significant activities that occurred during the previous shift.
- Significant decisions and events anticipated during the next shift.

- **Operation Update and Assessment Briefing.**
  - The XO, S-3, and S-2 are key players in specifying which displays are briefed at operation update and assessment briefings. The operation update and assessment briefing provides an established set of information items to the commander, XO, or S-3.
  - The large amounts of data and level of granularity of the digitally produced information can make it tempting to over inform and hence waste time. The technical enablers in the digital CP provide some dividends in saving time. Each briefing slide in the operation update and assessment briefing has a staff element that maintains the original file on its workstation or server. Using file transfer protocol, the staff can merge updated slides into one file at one control station for the operation update and assessment briefing Large memory-consuming graphics slow-down transfer and tie-up transmission means during exchanges between CPs.
  - The staff can redeem the time lost in transferring files between CPs by sharing operation update and assessment briefing via VTC. This capability is valuable for verifying the accuracy of unit information that another CP, unit, or headquarters maintains
  - The BCT will precede the division or JTF in time blocks that allow the brigade and its subordinate battalions to monitor and interact via VTC. The brigade must economize viewing time so those staff leaders are not tied-up in meetings. The physical CP arrangement and the distribution of monitors should allow primary staff officers the latitude to continue work while concurrently monitoring operation update and assessment briefings and other VTC sessions.

Combat Information Center (CIC)

6-57. The digital CP normally sets aside an area for a CIC. The CIC tracks and displays for the commander those staff products that form the COP. A CIC varies in complexity depending upon the unit level and type. Displays in the CIC can be a combination of control system overlays, video feeds projected on large screen displays, and analog maps or charts. Size and mobility of the CP and the preferences of the commander drive types, format, and quantity of information presented in the CIC. In the CIC at division and above, the CP normally has sufficient video and display assets to support production of "rolling" update information, much like timed news segments.

- The VTC facilitates decision making by reducing the time commanders and staffs spend moving physically between CPs to attend planning and orders sessions or time spent waiting to receive, review, and respond to textual OPORDs. Through the VTC, the brigade can present information, discuss COAs, make decisions, and coordinate action.
- Factors that impact VTC operations include types of equipment, timing of conferences, and management procedures used between the conferee stations. VTC sites need rigid step-by-step checklists that detail actions from system initialization to shutdown. Control stations must maintain prescribed conference group settings (type conference, and applicable conferees). For example, the brigade tactical CP controls a VTC for the command group that includes all major subordinate commands and separate battalions. Higher headquarters normally control VTCs. Channels and screens are pre-set to accommodate the video feed and graphics. The staff must establish audio protocol to mute selected stations until required.
- VTC follow-up actions are part of information management, as well as normal staff procedures. During whiteboard sessions, commanders interact with subordinate or higher commanders. This situation accelerates the plan-and-prepare portion of the MDMP. Often, commanders draw their schemes on the whiteboard and refine them as discussion ensues. Staff leaders must watch and note all interactions with attention to detail. Commanders may establish new or update IRs. They may also frame FRAGOs and require follow-up graphics and other ABCS products.

Division of Labor

6-58. At every level of command, there will be an explicit division of labor between the CPs. This is normally a function of the tactical responsibility assigned to the various CPs. The sustainment areas of digitized units are normally complex to control. CPs and TOCs have to make concerted efforts to follow the sustainment area situation as the battle progresses. The presence of analog friendly forces, the threat of threat special operations, and the challenges of the civil or military situation, HN support, and other diverse information variables demand that staff leaders in sustainment areas are well-trained and have full access to the COP.

Disseminating the Common Operational Picture

6-59. Staff leaders disseminate the COP and supporting products over the tactical communication system almost continuously. The staff promptly posts formal changes to running estimates on a regular schedule and amends the databases, strength accounts, inventories, terrain overlays, and tactical control (TACON) measures, as necessary. Initial estimates and updates go to organic, adjacent, attached, and supporting units and to the next higher level of command. Methods of dissemination range from analog to near-real time (NRT) digital and direct video link. Besides those already discussed, the capabilities and limitations of the communications architecture of the ABCS drive the specific mediums that support the dissemination of the COP.

Standardizing the Common Operational Picture

6-60. The tempo of tactical operations can quickly overwhelm any staff to include the staff of a digitally enabled brigade. Information is the key to digital operations, and the COP is the brigade's primary focus and visualization mechanism. Without an accurate, up-to-date COP, the BCT could lose information superiority at a critical point in the operation. Therefore, in addition to established staff procedures, the digital staff must have standardized techniques and procedures to manage digital information and maintain the COP. It is essential that the staff establishes and practices these SOPs before being thrust into crisis planning. Failure to set standards for digital information and products will result in the failure of the brigade's information management process. The following are two examples of digital standards.

- **File Management.** The brigade staff is directly involved in how digital files and directories are created and named. The ABCS labels messages by Internet Protocol (IP) address that has little meaning to the operators. For example, a simple threat situation overlay might have an IP address of "iew3i02, 148.33.44.1". The control system manager in the unit or staff element must convert this indiscernible IP address into a user-friendly file name. Normally, the file names contain the unit, C2 node, and staff element. For example, the convention might be "4INFDIV USTAC1 G-2 OPS 1" meaning the overlay is the product of the G-2 Operations Section of the 4th Infantry Division and is located at the division's tactical CP 1. The manager can also standardize staff and product directory names.

Note. /C2PRODUCTS/SITMAPS is the directory for the current SITMAPs of G-3 Operations while /C2PRODUCTS/SITMAPS/FUTURE is the directory for planning graphics of G-3 Plans.

- **Graphics and Overlay Colors.** Screen displays can become extremely cluttered with icons and control or intent graphics. The staff must designate color codes for unit graphics to provide uniformity between staffs and units as well as enhance on-screen readability. The staff should use the color codes prescribed in Military Standard 2525B and FM 1-02 when formally distributing plans and overlays. Attention to higher color conventions is required when operating in a joint environment.

ASSESS

6-61. Assessment occurs during each step of the intelligence process. If the intelligence provided to the commander and staff answers the intelligence requirement and is provided by the time required and in the format requested, then the PIR is satisfied and subsequently closed. A requirement is not satisfied when resulting intelligence does not meet the above criteria. If time permits, the requirement should be retasked. When a satisfied requirement results in a new request, a new requirement is generated and the process is repeated. The commander and S-2 measure the effectiveness of the intelligence process against the following standards:

- Timely. Intelligence is useful only if the S-2 gets it to the commander and staff soon enough to support planning, influence decisions, and prevent surprise.
- Relevant. Intelligence must answer the CCIRs about the threat and other conditions of the operational environment. The S-2 must produce and present products that focus on the unit's mission and help the commander to visualize and understand the AO.
- Accurate. Intelligence must provide a balanced, complete, and objective picture of the threat and other conditions of the operational environment. When doubt exists, the S-2 must capture and present that uncertainty in measurable terms to the commander. The commander must make the decision as to whether the risk fostered by uncertainty of the threat situation is acceptable or unacceptable to the mission.
- Predictive. Intelligence should advise the commander of present and future threat intentions, objectives, capabilities, and COAs.

This page intentionally left blank.

PART THREE

Intelligence Organizations

The MI Company provides analysis and ISR synchronization support to the brigade S-2. It coordinates and executes tactical HUMINT operations as directed by the brigade S-3, S-2, and S-2X. The MI Company's primary purpose in the BCT is to assist the S-2 in maintaining a timely and accurate picture of the enemy situation. This picture aids in predicting future enemy COAs and in answering the brigade commander's intelligence requirements.

Chapter 7

Military Intelligence Company

MISSION

7-1. The MI 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 MI 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.

ORGANIZATION

7-2. MI Company contains a headquarters element, an Analysis and Integration Platoon, a TUAS Platoon, and a Ground Collection Platoon. They conduct ISR integration and intelligence production in support of the brigade's planning, preparation, and execution of multiple, simultaneous decisive actions across the distributed AO.

7-3. 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 CP 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. Chapter 8 discusses the Analysis and Integration Platoon in detail.

7-4. The TUAS Platoon provides the commander real-time visual imagery in support of reconnaissance and targeting operations.

7-5. The Ground Collection Platoon contains a tactical HUMINT Section and a Prophet Control Section. The tactical HUMINT Section collects HUMINT through screening interrogations, debriefing contact operations, and support to 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 SIGINT operations as directed by the brigade S-3 in coordination with the brigade S-2. Chapter 9 discusses the Ground Collection Platoon in detail.

7-6. The BWT, when attached, provides the BCT with a weather prediction and weather effects analysis capability. The BWT—

- Evaluates and applies OWS forecasts to specific brigade missions, weapons systems, strategies, tactics, and applications; deploys with the brigade; and in general provides both direct and indirect tailored customer support.

- Provides accurate, timely, reliable meteorological support to all facets of brigade force planning, training, deployment, employment, and evaluation.

7-7. In addition to support to the S-2, the BWT is the main source of weather support for all brigade warfighting functions. As a member of the commander's special staff, the SWO is responsible for coordinating OWS 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 TACON of the SWO.

FUNDAMENTAL CONSIDERATIONS

7-8. During the brigade's planning, the MI 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 OPORD input, annex B, and annex L. The MI Company commander advises the brigade S-3 on the employment of what EAB 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 MI Company commander produces the company OPORD, and prepares to support the brigade's ISR plan. In addition to the task organization considerations in FM 5-0, the MI Company commander attempts to—

- Provide seamless analytical support to the brigade S-2.
- Assist with the synchronization of intelligence and electronic warfare (IEW) assets in the brigade's AO.
- Retain the flexibility to reallocate and reposition company assets in response to changes in the brigade's mission, concept of operations, scheme of support, and threat.
- Receive a TROJAN SPIRIT team and other attachments as directed in the brigade order.
- Establish logistics and security relationships with the brigade HHC to sustain and protect the MI Company personnel and equipment.

COMMAND AND SUPPORT RELATIONSHIPS

7-9. 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 TUAS 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 MI Company commander to conduct logistical and security coordination and planning with other brigade C2 elements. Table 7-1 shows the command and support relationships.

7-10. Command relationships establish the degree of control and responsibility a commander has for the forces operating under his or her control. Command relationships can be attached, under OPCON or TACON. HUMINT collection teams (HCTs) from the Ground Collection Platoon may operate in DS of subordinate brigade elements, particularly during entry operations or to support combat operations.

Table 7-1. Command and support relationships

IF RELATIONSHIP IS:		INHERENT RESPONSIBILITIES ARE:							
		Has Command Relationship with:	May Be Task Organized by:	Receives Sustain-ment from:	Assigned Position or AO by:	Provides Liaison to:	Establishes/ Maintains Communication with:	Has Priorities Established by:	Gaining Unit Can Impose Further Command or Support Relationship of:
COMMAND	Attached	Gaining unit	Gaining unit	Gaining unit	Gaining unit	As required by gaining unit	Unit to which attached	Gaining unit	Attached; OPCON; TACON; GS; GSR; R; DS
	OPCON	Gaining unit	Parent unit and gaining unit; gaining unit may pass OPCON to lower HQ (Note 1)	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	OPCON; TACON; GS; GSR; R; DS
	TACON	Gaining unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by gaining unit and parent unit	Gaining unit	GS; GSR; R; DS
	Assigned	Parent unit	Parent unit	Parent unit	Gaining unit	As required by gaining unit	As required by parent unit	Parent unit	Not Applicable
SUPPORT	Direct Support (DS)	Parent unit	Parent unit	Parent unit	Supported unit	Supported unit	Parent unit; Supported unit	Supported unit	(Note 2)
	Reinforcing (R)	Parent unit	Parent unit	Parent unit	Parent unit	Reinforced unit	Parent unit; Reinforced unit	Reinforced unit; then parent unit	Not Applicable
	General Support Reinforcing (GSR)	Parent unit	Parent unit	Parent unit	Parent unit	Reinforced unit and as required by parent unit	Reinforced unit and as required by parent unit	Parent unit; then reinforced unit	Not Applicable
	General Support (GS)	Parent unit	Parent unit	Parent unit	Parent unit	As required by parent unit	As required by parent unit	Parent unit	Not Applicable

NOTE 1. In NATO, the gaining unit may not task organize a multinational unit (see TACON).
NOTE 2. Commanders of units in DS may further assign support relationships between their subordinate units and elements of the supported unit after coordination with the supported commander.

7-11. Support relationships are specific relationships established between supporting and supported units. The MI Company may place HCTs in DS to brigade elements. In this support relationship, the MI Company retains C2 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 GS, the teams operate in the AO of brigade elements but are under the OPCON of the brigade, as exercised through the MI Company commander and the Ground Collection

Platoon Leader for positioning the assets and for assigning collection priorities. Additionally, the MI Company commander may physically collocate the OMT of the Ground Collection Platoon with the brigade's S-2X section (see chapter 9 for more information).

CAPABILITIES AND LIMITATIONS

7-12. Enabled by the DCGS-A enterprise the MI Company —

- Conducts intelligence "reach" to Army Forces (theater, joint, and national agencies) to access, retrieve, and manipulate intelligence databases and products.
- Tracks the current battle and advise the brigade S-2 and S-3 on the repositioning and retasking of ISR assets.
- Stores and analyzes multi-discipline and multi-source products.
- Conducts all-source analysis to support situational understanding.
- Fuses distributed analytic products to provide input into overall COP.
- Supports the planning of ISR operations.
- Conducts HUMINT collection and HUMINT analysis.

7-13. General limitations of the MI Company include—

- Limited HUMINT analysis capability.
- Lack of XO, organic CBRN, and armorer personnel, which limits the ability to conduct company administrative activities.
- Insufficient transportation capability to optimally employ the HUMINT collection assets.
- No organic capability to repair and replace intelligence systems damaged or destroyed due to accident or battle damage.

COMMAND AND CONTROL ORGANIZATION

7-14. The company commander is responsible for the C2 of the MI Company. Leaders at all levels within the company aid the commander in executing these responsibilities. The commander discharges the responsibilities through an established chain of command. The commander holds each subordinate leader responsible for the actions of the unit. When the commander assigns a mission to a subordinate, the commander also delegates the necessary authority and provides the resources, guidance, and support needed to accomplish the mission. The commander must allow the subordinate commander freedom of action. ISR operations do not provide the luxury of supervising subordinates in detail. The commander remains free to address the unit as a whole and to anticipate future actions. Subordinate leaders adhere to this philosophy.

7-15. The company commander is ultimately responsible to ensure that the unit is properly trained to comply with the Law of War (LOW) and Intelligence Oversight, which operations are conducted in compliance with the LOW and Intelligence Oversight, and that illegal or questionable activity is properly reported and investigated. Appendix D provides more information on intelligence oversight.

COMPANY HEADQUARTERS

7-16. **Company Commander.** The MI Company commander—

- Advises the brigade commander on the capabilities, limitations, and most effective employment of the company.
- Coordinates with the S-2 to ensure that the intelligence staff functions are supported to the best of the ability of the company.
- Responds to the tasking of the brigade commander as directed by the brigade S-2 and S-3.
- Organizes for combat based on the mission, scheme of support, task organization, and specified and implied tasks contained in the brigade's OPORDs.

- Uses the brigade's order to plan, prepare, execute, and assess the MI Company's operations.
- Oversees the collective and individual training of the company. While the tendency may be to place emphasis on intelligence training, the commander must ensure that all intelligence and non-intelligence tasks are incorporated into the mission-essential tasks list (METL) and trained to standard.
- Continually assesses the company's ability to sustain its internal operations and its ability to support assigned missions.
- Establishes clear and consistent standards and guidance for current and future operations. This guidance allows the MI Company leaders and Soldiers to adhere to the commander's intent without constant personal supervision.
- Is responsible for the discipline, combat readiness, and training of the commanded unit.
- Must be proficient in C2 of the unit, employment of organic and attached assets, and interpreting the ISR tasks of the company and supported commands.
- Ensures that all personnel are trained and prepared for deployment.
- Must know the capabilities and limitations of assigned and attached personnel and equipment.
- Analyzes and restates the mission, designs the concept of operations, organizes the company, and provides analysis and integration support to the S-2 section and HUMINT collection support to the brigade and its subordinate units.
- Issues mission orders with sufficient details for subordinate leaders to plan and lead their units.
- Trains subordinates to work within his or her intent to achieve the mission objectives during his or her absence, the failure of communications, or changes in the situation.
- Must know the threat, its organization, its ISR systems, and how it operates.
- Must know the terrain over which the commanded unit will operate and how that terrain enhances or limits ISR operations.
- Must be aware of the operational limitations of the commanded unit and ensure all company assets are properly positioned and fully synchronized to accomplish the mission.

7-17. Once the operation starts, FRAGOs and quick responses are the norm. The orders received from brigade and those that the company issues must be simple and clear to enable swift execution upon receipt. The commander prepares to accept mission orders, and without further detailed instructions, takes action to execute the order within the intent of the brigade commander. During the operations, the MI Company commander "fights" platoons and tracks teams.

7-18. The commander normally operates from the company TOC, collocated with the brigade TOC. At the TOC, the commander supervises planning, monitors operations, interfaces with the staff, and rests. The commander frequently departs the TOC to receive orders, conduct staff reconnaissance, inspect, brief subordinates, and visit Soldiers.

7-19. **Company Executive Officer.** The MI Company has an authorized XO position while the Stryker Brigade Combat Team does not. Senior leaders within the company must assume these duties and responsibilities.

7-20. **First Sergeant (1SG).** The 1SG is primarily responsible for sustaining the company's ability to fight. The 1SG supervises the procurement and distribution of fuel, ammunition, food, water, clothing, equipment, replacements, and repair parts. The 1SG ensures Soldiers injured, wounded, or killed in action are treated and evacuated. The 1SG coordinates the evacuation and recovery of damaged equipment. The 1SG usually operates independently but complementary to the commander, usually at a critical location where the commander needs additional supervision, oversight, or observation. The 1SG works closely with the platoon leaders and platoon sergeants. The 1SG's focus changes frequently based on the needs of the unit and the direction of the commander. The 1SG's specific responsibilities include—

- Executing and supervising routine operations. This may include enforcing tactical SOPs; planning and coordinating training; coordinating and reporting personnel and administrative actions; and supervising supply, maintenance, communications, and field hygiene operations.

- Supervising, inspecting, and observing all matters designated by the commander.
- Planning, rehearsing, and supervising key logistical actions in support of the tactical mission. These activities include resupply of Classes I, III, and V products and materials; maintenance and recovery; medical treatment and evacuation; and replacement and return-to-duty processing.
- Conducting training and ensuring proficiency in individual skills and small-unit collective skills that support the company's METL.
- Receiving and assigning personnel replacements to subordinate platoons.
- Establishing and maintaining the foundation for company discipline, in conjunction with the commander.

7-21. **Supply Sergeant.** The supply sergeant requests, receives, issues, stores, maintains, and turns in supplies and equipment for the company. The supply sergeant coordinates all supply requirements and actions with the 1SG and the brigade S-4. Normally, the supply sergeants position themselves in the brigade support area either with the brigade HHC supply or with the brigade support battalion (BSB). The supply sergeant will—

- Control the company's cargo vehicles.
- Monitor company activities and the tactical situation.
- Anticipate and report logistical requirements.
- Coordinate and monitor the status of the company's logistics requests.
- Coordinate and supervise the company's logistics support from brigade HHC or the BSB.

7-22. **CBRN NCO.** The MI Company does not have a CBRN noncommissioned officer (NCO) but the company is required to provide a Soldier from within the company to support this function. That Soldier is required to serve as the CBRN NCO as a full-time duty. To achieve this, a Soldier must be removed from another modified table of organization and equipment (MTOE) authorized job to fill the duties listed.

7-23. The CBRN NCO assists and advises the company commander in planning for and conducting operations in a CBRN environment. The CBRN NCO plans, conducts, and supervises CBRN defense training, covering such areas as decontamination procedures and the use and maintenance of CBRN-related equipment. The CBRN NCO will—

- Assist the commander in developing company operational exposure guidance in accordance with guidance from higher headquarters.
- Make recommendations to the commander on CBRN survey and monitoring and decontamination support requirements.
- Requisition CBRN-specific equipment and supply items.
- Assist the commander in developing and implementing the company CBRN training program.
- Inspect company elements to ensure CBRN preparedness.
- Process and disseminate information on threat and friendly CBRN capabilities and activities.
- Advise the commander on contamination avoidance measures.
- Coordinate, monitor, and supervise decontamination operations.

7-24. **Armorer.** The BCT and SBCT MI Companies are responsible for organizational maintenance on the company's small arms and evacuation of weapons, as necessary, to the DS maintenance unit.

PLATOON LEADER, PLATOON SERGEANT, AND TEAM LEADER

7-25. **Platoon Leader.** The platoon leader's responsibilities parallel those of the company commander. The platoon leader—

- Is responsible to the commander for the platoon's combat readiness and employment.
- Must have a thorough knowledge of platoon TTP.
- Must know platoon equipment and personnel capabilities and limitations.

- Must be capable of advising the MI Company commander and supported unit commander on the platoon's capabilities and the most effective platoon employment.

7-26. **Platoon Sergeant (PSG).** The PSG leads the platoon elements as directed by the platoon leader and assumes command of the platoon in the absence of the platoon leader. The PSG assists the platoon leader in maintaining discipline, conducting training, and controlling the platoon in combat. Specifically, the PSG—

- Supervises the maintenance of equipment, supply, and other support matters.
- Ensures subordinate teams collect, evaluate, and report information in accordance with the standards of their military occupational specialty (MOS), skill level, technical capability of their equipment, and unit standards.
- Supervises resupply, field hygiene, maintenance and recovery, medical treatment and evacuation, and local area security.
- As necessary, leads the platoon quartering party.
- Conducts training and ensures proficiency in individual and collective skills that support the platoon's METL.
- Trains the platoon leader and NCOs in the small-unit leadership, technical, tactical, and logistical skills needed to succeed and survive on the battlefield.
- In conjunction with the platoon leader, establishes and maintains the foundation for platoon discipline.

7-27. **Team Leader.** The team leader is responsible to the platoon leader for the combat readiness and team employment. The team leader must be tactically and technically proficient in the TTP of the team's primary collection, processing, production, or dissemination mission. The team leader must know equipment and personnel capabilities and limitations. The team leader must be capable of advising the platoon leader and supported unit commander on the most effective platoon employment. The team leader must be capable of exercising sound judgment and operating without the platoon leader's direct supervision.

COMMAND POSTS AND OPERATIONS CENTERS

7-28. The C2 facilities and the DCGS-A enterprise provides the commander with the means necessary to manage information, coordinate action, make decisions, and disseminate orders for effective C2. These facilities sustain the operation through continuity, planning, and coordination of operations and support. Table 7-2 describes the six basic CP functions.

MI COMPANY COMMAND POST

7-29. The MI Company CP normally is collocated with the brigade TOC to facilitate C2 of the company assets and to maximize BCT S-2 support. The MI Company CP includes the company headquarters element, the Analysis and Integration Platoon, the TUAS 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 HCTs of the Ground Collection Platoon operate under DS of maneuver battalions and the reconnaissance squadron or even their subordinate companies and troops.

Table 7-2. Basic command post functions

Function	*Task*
Receive Information	• Receive messages, reports, and orders from subordinate units and higher. • Monitor tactical situation. • Maintain a journal of significant activities and reports. • Maintain and update unit locations and activities. • Monitor threat situation. • Maintain status of critical classes of supplies.
Distribute Information	• Submit reports to higher headquarters. • Serve as a communication relay between units (serve as net control station for operations and intelligence and command nets). • Publish orders and instructions. • Process and distribute information to appropriate units or staff sections. • Coordinate with adjacent unit liaison officers or teams. • Coordinate with supported and supporting units.
Evaluate Information	• Evaluate and consolidate reports. • Evaluate asset use and ISR mission success; recommend retasking assets as required. • Anticipate events and activities, taking appropriate actions as required. • Move assets based on the tactical situation. • Identify information that relates to CCIR. • Orchestrate the MDMP.
Make Recommendations	• Submit recommendations to the commander based upon available information and staff analysis.
Integrate Resources	• Integrate attached elements into the company concept of operation.
Synchronize Resources	• Synchronize company resources available by ensuring all attached and assigned elements are used properly and, if not, recommend corrections.

HEADQUARTERS ELEMENT

7-30. The company headquarters element consists of the commander, 1SG, and supply sergeant. The headquarters personnel control all the company's operational, logistical, administrative, and training activities.

PLATOON HEADQUARTERS

7-31. The Platoon headquarters is normally located where they can best C2 their platoon elements. All three platoons—Analysis and Integration Platoon, TUAS Platoon, and Ground Collection Platoon—normally will be collocated with the BCT S-2. Elements of the TUAS Platoon and Ground Collection Platoon could be deployed anywhere in the AO.

COMMAND AND CONTROL COMMUNICATIONS

7-32. The MI Company operates on several communications and processing nets. These nets provide the framework needed to coordinate the tasking, reporting, C2, and sustainment support of company subordinate units spread across the width and depth of the brigade's AO. Communications redundancy ensures that support to brigade operations will not be severely disrupted by the loss of any one system or CP.

7-33. The MI Company's OMT Section in the Ground Collection Platoon normally operates at the collateral security level to ensure the timely dissemination of combat information and targeting data to organizations operating outside MI channels. The collateral level operating environment also limits the damage to the brigade's intelligence operations should threat forces capture the CP or its personnel.

7-34. The MI Company's assets use three basic communications nets: the operations and intelligence (O/I) 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 FSE, aviation, or ADA communications nets.

- **O/I nets** or DCGS-A links the intelligence collectors and producers to the consumers of the intelligence information. It is used to pass information of immediate value to the affected unit and to analytical elements at the supported unit.
- **Command nets** exist at every echelon of command. They 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 all of their subordinate collection teams and to the centers or organizations that provide the databases and technical guidance necessary for single-discipline collection and analysis. For example, the technical net would connect HCTs through their control teams to the S-2X and higher echelon HUMINT analysis organizations.

7-35. The mechanism for reporting will be covered for each specific operation in the OPORD for that mission based off METT-TC considerations and organization and is dependent on the specific command or support relationship delineated in the OPORD or FRAGO. General principles based on command or support relationships are as follows:

- When a unit is attached, it will operate on the communications nets of the unit to which they are attached.
- When in GS, the unit will maintain all communications links to its parent unit with other communications nets as specified in its orders.
- When in DS, units will normally operate on the O/I and command nets of the unit they are supporting in addition to the communications links to the parent unit.

7-36. TROJAN SPIRIT communication systems are organic to the MI Company. Through the DCGS-A network centric enterprise the intelligence analysts assigned to the TROJAN SPIRIT access the dedicated multi-level 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).

This page intentionally left blank.

Chapter 8

Analysis and Integration Platoon

ISR operations generate an enormous amount of raw data, information, and intelligence that are processed via the DCGS-A enabled enterprise. Intelligence organizations from the BCT through national levels assist the decision makers and their intelligence staff in managing this information. Specifically, the MI Company's ISR Analysis Platoon and ISR Integration Platoon support the S-2 Section. They manage requirements and intelligence production and maintain visibility of ISR assets while distilling the volume of information resulting from both activities into intelligence databases and tailored products.

ORGANIZATION

8-1. The Analysis and Integration Platoon consists of a headquarters section, a Situation and Target Development Section, an ISR Requirements Section, a CGS Section, and a Satellite Communication (SATCOM) Team.

MISSION

8-2. The Analysis and Integration Platoon is the brigade S-2's principal support organizations for GMI, target intelligence, and ISR management. They are all-source, multidiscipline intelligence organizations with the organic analysis, management, and information technology capabilities needed to perform these tasks across full spectrum operations. Analysis and Integration Platoon's intelligence products and databases support the S-2 in advising the brigade commander and staff, in analyzing and presenting the current threat situation, and in analyzing and wargaming future threat COAs.

8-3. The Analysis and Integration Platoon uses its DCGS-A to database threat information, track threat movement, assess threat combat effectiveness, and create graphic and textual products that depict the results of its analysis. The Analysis and Integration Platoon shares its information and conclusions through collaboration with brigade and its subordinate element's S-2 personnel, and higher and lateral echelon intelligence organizations. Through use of the DCGS-A enterprise the analysis and management personnel pull intelligence and other relevant information from external intelligence organizations to enhance its analysis, understanding, and reporting of threat forces. These communications mechanisms allow the Analysis and Integration Platoon to respond to the PIRs of the S-2 Section and RFIs from intelligence staffs throughout the brigade.

8-4. The Analysis and Integration Platoon develops, manages, and communicates all-source and multidiscipline intelligence. As with all military operations, the Analysis and Integration Platoon leader must review platoon organization based on METT-TC factors to ensure the proper personnel, equipment, and support are in place to execute each mission.

8-5. The Analysis and Integration Platoon provides intelligence planners to support the S-2 planner in threat COA development and wargaming. The planners work with the BCT S-2 operations team, S-3 plans team, and other staff elements to prepare for future operations. They use the IPB products from EAB and refine them to develop and present the threat's COAs during staff planning. They work with FS planners to select and prioritize HVTs for targeting as HPTs. The S-2 planner, with support from the Analysis and Integration Platoon, writes the intelligence running estimate and the intelligence portions of the BCT OPORD. The planners refine and update their planning products throughout the planning, preparation, and execution of the BCT's operations. They work closely with the S-2 operations team to ensure continuity between the S-2 Section's assessment of current and future threat operations. The intelligence planning focus is METT-TC dependent but generally extends beyond the immediate AO to the BCT's AOI and includes asymmetric aspects of the enemy's capabilities. The intelligence planning effort must—

- Develop and present the threat's COAs and assessment of the friendly force from the threat's perspective.
- Monitor current situation to continually assess the operational environment (and the impact) on future COAs.
- Wargame threat COAs against friendly COAs during staff planning and decision making.
- Assist the BCT's FS planner in identifying threat HVTs and potential HPTs for both lethal and nonlethal attack.
- Produce and disseminate the intelligence running estimate to the BCT staff at a predetermined time according to the commander's guidance and METT-TC.
- Conduct detailed horizontal planning and collaboration with the other BCT staff members.
- Develop the threat situation paragraph of the OPORD.
- Continuously collaborate with the S-2 operations team on the impacts of current operations on future threat COAs.

8-6. The Situation and Target Development Section and ISR Requirements Section perform analysis to support understanding of the operational environment. Both sections—

- Integrate information from organic and external collection activities to include direct downlinks from external ISR resources, processed through the common ground sensor (CGS), ASAS, and the TROJAN SPIRIT or DCGS-A to produce current intelligence in support of providing an understanding of the current situation.
- Provide tip-off or cueing for specific targeting assets including those that support information operations, indirect fires, and lethal and nonlethal effects.

8-7. The Situation and Target Development Section performs analysis to support the operational environment. They conduct traditional analysis of spot reports as well as pattern and term analysis to assist in predicting possible threat COAs and tipping off potential future activities within the AO by individuals or groups.

8-8. The ISR Requirements Section provides RM, ISR synchronization, and single-source management in support of the brigade's ISR process. It maintains visibility on organic and attached ISR assets. These functions allow the brigade commander to more efficiently manage the ISR effort between echelons and support the dynamic tasking of the BCT's ISR assets. It conducts ISR RM, SIGINT technical support and analysis, and multi-sensor visualization for the BCT commander and staff in support of the BCT S-2 Section.

8-9. The Intelligence Processing Team operates the CGS or CGS component of DCGS-A. The team receives and processes radar data from the US Air Force's E-8C and U-2 aircraft. The Intelligence Processing Team—

- Uses the data to detect, locate, classify, and track a variety of moving and fixed targets within the BCT's AOI.
- Uses the CGS to receive, store, process, correlate, disseminate and display NRT information from other collection assets with its radar data to refine its interpretation of the threat activity.
- Works closely with the imagery analysis team to ensure timely support to situation development and targeting.
- Provides the BCT with a rapidly deployable, mobile, and responsive intelligence processing capability.

SECTION RESPONSIBILITIES

HEADQUARTERS SECTION

8-10. The Analysis and Integration Platoon headquarters consists of a platoon leader and a platoon sergeant who act as the shift officer in charge (OIC) and noncommissioned officer in charge (NCOIC) during tactical operations.

8-11. The shift OIC focuses and prioritizes work, synchronizes interaction between teams, and task organizes the combined analysis and integration resources in response to the MI Company commander's orders and S-2 guidance. The shift OIC evaluates and tracks tasks, focuses the analysis effort, and reviews intelligence products for quality and timeliness. The shift OIC interacts with the S-2 sections, other brigade staff elements, the G-2 section and EAB ACEs to ensure intelligence products answer the commander's PIRs and other IRs. The shift OIC must therefore have a thorough knowledge of the intelligence operations, capabilities, and limitations.

SITUATION AND TARGET DEVELOPMENT SECTION

8-12. The Situation and Target Development Section conducts situation development, database management, threat disposition, target development, combat assessment, and imagery analysis in support of the BCT S-2 section. The section conducts distributed and collaborative analysis by gathering, analyzing, and fusing information from multiple echelons and sources to produce intelligence products that meet the BCT commander's decision making and planning requirements. The result is that the section uses combat information and intelligence from all the BCT's ISR resources to develop an accurate and timely intelligence assessment of the threat and other conditions of the operational environment. It has the organic processing and communications systems to collaborate with external analytic elements, the BCT S-2 section, reconnaissance squadron S-2, subordinate battalion S-2s, and the ISR Requirements Section to continuously update and refine the threat portion of the BCT's COP.

Senior All-Source Analysts

8-13. The senior all-source analysts oversee the analysis of information and the production of intelligence from multiple echelons and sources on threat capabilities, organizations, dispositions, and readiness. They oversee the operations of the teams within the analysis section and coordinate their activities.

Situation Development

8-14. Enabled by the DCGS-A enterprise Situation and Target Development Section develops the current threat picture for the COP of the BCT AO and AOI through the distributed collaborative analysis and the fusion of combat information and multidiscipline intelligence identified by the threat disposition development team. It accesses the current situation from higher, lower, and adjacent units as well as warfighting functions specific products from experts within brigade. It fuses this information into an annotated graphic assessment of the current situation. The S-2 operations team uses the current situation picture, coupled with the S-2 planner's planning products, to verify predicted threat COAs and intentions.

Database Management

8-15. The database manager maintains the technical health of the platoon's all-source analysis system or DCGS-A correlated database. The database manager receives and processes incoming data, correcting format and input errors to ensure that messages can be parsed into the all-source correlated database. On the direction of the senior all-source analyst, the database manager updates database files. As required, the database manager publishes portions of the database to the ABCS shared joint common database and to subordinate S-2s and other intelligence activities.

Threat Disposition

8-16. The Situation and Target Development Section supports the development of a common understanding of the current and future situation by directing threat personnel and equipment queries to the brigade level collectors. The queries are approved by the "intelligence battle captain" or the S-2 and forwarded as IRs through the tasking system. The section then analyzes the information reported by these units in conjunction with external collection and analysis products. It fuses this information with other warfighting function's analytic products to provide a current disposition overlay using collaborative tools.

8-17. This section exchanges the results of analysis and discusses issues with external regional experts to enhance its products and provide them to the S-2 planner. The section conducts IPB and NRT all-source analysis of threat information wherever it resides to eliminate latency and loss of context to support situational understanding, targeting, and FP. This function also includes conducting trend and pattern analysis as a means of providing predictive intelligence support to future operations.

Target Development

8-18. The Situation and Target Development Section conducts combat assessment in support of the BCT S-2 section and the FSCOORD. For target development, the section uses the intelligence and staff planning products it develops in conjunction with the S-2 planner to identify HVTs. Target development requires the section to receive, process, database, and present in graphic format information on threat forces, facilities, and capabilities. The section continuously shares this information with other elements within the MI Company, the S-2 section, reconnaissance squadron, the FSCOORD, and BCT CP to facilitate development and execution of the BCT's FS plan. The section supports combat assessment by leveraging multiple sources and the results of all source analysis.

8-19. Supporting combat assessment requires extensive coordination with the S-2 section, FSCOORD, information operations staff officer, and other teams within the Analysis and Integration Platoon. This collaboration ensures the analysis addresses both the physical and functional aspects of each target during target development and assessment. It also requires that common procedures and methodology be established which synchronize and integrate Army combat assessment and BDA with those at joint and national levels.

8-20. Success in the BDA process and the combat assessment function of the targeting process are achieved when the commander has the information necessary to quickly make decisions about COAs and FS; as such, it demands a continuous update to the current assessment of threat BDA. The Situation and Target Development Section serves as the intelligence focal point for target development during the execution of operations by working directly with the FSCOORD to execute targeting missions and to coordinate changes.

Imagery Analysis Support

8-21. The imagery analysts in the Situation and Target Development Section develop tailored imagery products to support analysis, maintain secondary imagery databases to support plans and operations, and support targeting development and combat assessment. The imagery analysts primarily maintain the imagery product library and retrieve imagery products from multiple sources to satisfy the BCT's imagery requirements. These analysts have the ability to conduct initial exploitation of the imagery that is generated from internal sources such as digital and video cameras and the TUAS. They access and request imagery through DCGS-A from external sources such as JSTARS SAR imagery and tactical exploitation of national capabilities imagery product libraries, exploit imagery from internal sources, and assist in correlating it.

Joint Deployable Intelligence Support System (JDISS)

8-22. The JDISS on board the TROJAN SPIRIT allows the Situation and Target Development Section to access, focus, and tailor the broader technical and analytic products from national and theater analytic centers to meet the BCT's intelligence needs. Using organic communications and processing systems, they access existing databases, products, and analytic expertise resident in service and joint and national ISR

resources at both the collateral and SCI levels. These split-based operations and intelligence "reach" capabilities facilitate collaboration, task sharing, and access to EAB databases (virtual databases in the future), as well as IPB products and focused analysis. TROJAN SPIRIT is a component of DCGS-A (Version 4).

ISR REQUIREMENTS SECTION

8-23. The ISR Requirements Section assists the S-2 and S-3 in developing, coordinating, monitoring, and making adjustments to the brigade's ISR plan. The section works with the S-2 planner to identify information requirements and collection strategies. The ISR Requirements Section —

- Works with the situation and target development section to develop ISR tasks to answer the commander's PIRs.
- Works closely with the S-2 and the S-3 to recommend specific tasking of ISR assets and to identify shortcomings in the current and near-term ISR support.
- Monitors the ISR plan to ensure subordinate ISR assets and external production resources deliver relevant information, targeting data, and intelligence to the commander.
- Develops collection requirements, monitors asset status, recommends tasking of brigade organic collection assets to the S-3.
- Requests information from higher and lateral intelligence production centers.
- Participates in the BCT staff wargaming and targeting sessions to extract information that answers the commander's decision-making and targeting needs.
- Coordinates with the S-2 to identify shortcomings in the current and near-term ISR support.

8-24. By simultaneously monitoring the current situation and future planning, the section can rapidly recognize and recommend redirection of ISR assets to respond to situations that are significantly divergent from the assumed threat COAs which led to the current concept of maneuver, fire, or information operations. Collaboration, both virtual and analyst-to-analyst between the ISR Requirements Section and the S-2, is essential to the synchronization of the ISR effort and presentation of the most current intelligence possible to the BCT commander and staff. Some specific ISR Requirements Section tasks are to—

- Develop intelligence requirements that support friendly COAs.
- Develop ISR tasks to support each SIR.
- Develop multidiscipline, multi-echelon, and warfighting function ISR tasks and RFIs.
- Assist the S-2 with the development and inclusion of ISR tasks into paragraph 3a(3) (ISR) and 3a(4) (Intelligence) of the OPORD.
- Develop and maintain the ISR matrix and IEW synchronization matrix in annex B (Intelligence) of the OPORD.
- Manage RFIs to EAB intelligence organizations.
- Perform SIGINT technical support and analysis.

8-25. The SIGINT analysts in the ISR Requirements Section maintain an overall SIGINT overlay for the BCT's AO. The SIGINT analysts serve as the conduit for SIGINT data and information within the BCT. They provide SIGINT focus and technical guidance to the MI Company/SBCT's reconnaissance squadron Prophet teams through the analysis of current information and data received from higher headquarters. Specific SIGINT analysis tasks include—

- Receiving technical support, planning, RM, and database access from national-, joint- and theater-level SIGINT through intelligence "reach."
- Providing technical support to the Prophet Control Section.
- Providing collateral level technical information to the reconnaissance squadron/reconnaissance squadron.
- Correlating CGS or DCGS-A communications intelligence (COMINT) and electronic intelligence (ELINT) reporting.

COMMON GROUND STATION SECTION

8-26. The CGS receives, stores, processes, correlates, disseminates, and displays in NRT radar imagery from the USAF JSTARS E-8C providing the deep and wide ground picture. E-8C radar data provides moving target indicators (MTIs), fixed target indicators (FTIs), and SAR imagery. The CGS—

- Simultaneously processes ISP overlays and collateral level SIGINT reports received from the Intelligence Broadcast Service via its joint tactical terminal (JTT), imagery products from U2 and airborne reconnaissance low (ARL) platforms, and the fire control radar freeze-frame picture from Apache Longbow, video imagery, and telemetry from Army and US Air Force (USAF) UASs, when collocated with the UAS GCS.
- Can also receive and store secondary imagery.
- Is designed to provide imagery, message, and analytical interface with the ASAS or CGS component of the DCGS-A.

8-27. The CGS processing system allows its operators to maintain and manipulate related intelligence and EW broadcast intelligence as well as to display threat situation, sensor data, and database information in a graphic format. The ability to interface with AFATDS allows the FSCOORD to access information to support target development and combat assessment. Sensor links and connectivity available through the CGS include—

- JSTARS moving target indicator (MTI) and SAR imagery.
- USAF U2 electronic MTI.
- ARL MTI information.
- USAF RC-135 Rivet Joint SIGINT reporting via the C/JTT.
- Guardrail Common Sensor (GRCS) SIGINT reporting via the combined or JTT.
- Army and USAF UAS video and telemetry.
- Other broadcast intelligence downlinks.

SATELLITE COMMUNICATIONS (SATCOM) TEAM

8-28. The SATCOM Team is responsible for integrating SCI communications into the existing network architecture using the TROJAN SPIRIT system. The TROJAN SPIRIT organic to the Analysis and Integration Platoon will normally collocate with the BCT S-2 and the Analysis and Integration Platoon during operations. The intelligence analysts assigned to the TROJAN SPIRIT access the dedicated multi-level security, high-capacity communication link between BCT CPs, theater, joint, 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 system also provides the opportunity for secure, analytic collaboration externally to the BCT. The TROJAN SPIRIT also provides access to the Joint Worldwide Communications System (JWICS) through its JDISS.

CONSIDERATIONS

8-29. The Situation and Target Development Section and the ISR Requirements Section reflects an organization built principally to support the brigade operating independently for a short time. Organizing the scant resources in the platoon to accomplish all of the functions required to provide support to the BCT will challenge the platoon leadership. The Analysis and Integration Platoon lacks a well-defined, single-source analysis capability and rely on intelligence products through intelligence "reach." Staffing and training issues continue to challenge the MI leadership. The platoon must prepare to receive and integrate augmentees to fill personnel shortages and expand its operations for stability operations. These augmentees may include foreign personnel in addition to individuals and teams from other services and national agencies.

Chapter 9
Ground Collection Platoon

ORGANIZATION

9-1. The Ground Collection Platoon consists of a Prophet Control Section with a Prophet Control Team and two Prophet Collection Teams and a SATCOM Team, as well as a HUMINT Collection Section with an OMT and three HCTs.

MISSION

9-2. The Ground Collection Platoon contains the BCT's SIGINT and HUMINT collection assets. During operations, it is extremely likely that these assets will be tasked out across the brigade's AO and may be tasked to support subordinate brigade elements. The Prophet Control Section provides mission management, correlates direction finding (DF) data and reports combat information on threat emitter activity and ISP position. The OMT and HCTs provide the BCT with an organic capability to conduct HUMINT collection (interrogation, debriefing, tactical questioning, and limited DOMEX). The HUMINT capability is directed toward assessing the enemy and civil considerations to answer the BCT commander's PIR.

SECTION RESPONSIBILITIES

PLATOON HEADQUARTERS

9-3. The Ground Collection Platoon headquarters consists of a platoon leader and a PSG.

- The platoon leader is responsible to the commander for the combat readiness and employment of the platoon. The platoon leader ensures that the platoon's administrative, logistic, and training requirements are met. The platoon leader must know the capabilities and limitations of the platoon's personnel and equipment. The platoon leader must advise the MI Company commander and, if platoon assets are DS, advise the supported unit commander on the platoon's capabilities and the most effective employment of the platoon.
- The PSG leads elements of the platoon as directed by the platoon leader and assumes command of the platoon in the absence of the platoon leader. The PSG assists the platoon leader in maintaining discipline, training, and controlling the platoon in combat. The PSG supervises the maintenance of equipment, supplies, and other sustainment requirements. As an expert on the platoon's equipment and operations, the PSG ensures subordinate teams collect, evaluate, and report information in accordance with the standards of their MOS, skill level, technical capability of their equipment, and unit standards.

PROPHET SECTION

9-4. The MI Company's EW capability dwells in the Prophet section of the Ground Collection Platoon. The Prophet section conducts EW operations. The Prophet collection teams detect, locate, and track threat communications emitters. This information becomes part of the COP. If EA capable, the teams deliver nonlethal effects against selected HPTs that deny, disrupt, and delay the threat's ability to exercise C2. If tasked, the Prophet system can support electronic protection by monitoring and identifying potential shortcomings in friendly forces communications security (COMSEC). Whether operating independently or as part of a DF baseline, the teams position themselves where they can detect threat emitters and communicate with the multi-sensor control team.

9-5. The BCT Prophet section consists of a Prophet control team and two Prophet collection teams (Stryker BCT possesses three Prophet collection teams) and a SATCOM team. It is the BCT's primary collector of SIGINT in support of the BCT commander's PIR.

Prophet Control Team

9-6. The Prophet control section provides technical control and guidance to the Prophet collection teams. DCGS-A will incorporate Prophet control functions as well as provide access to Theater and National SIGINT databases. DCGS-A receives reports from the Prophet collection teams, conducts initial SIGINT analysis, and forwards those reports and any analysis to the BCT S-2. It provides immediate reporting of time-sensitive combat information, protection requirements information, or intelligence to the Analysis and Integration Platoon in the Brigade S-2 and directly to the subordinate headquarters in whose AO the Prophet Collection Team is operating. Prophet control continually monitors and evaluates the SIGINT collection and retasks based on METT-TC to ensure the best collection possible to support the commander's PIR. Prophet control receives technical support from the Analysis and Integration Platoon in the BCT S-2.

Prophet Collection Teams

9-7. The Prophet collection teams conduct SIGINT collection activities and report combat information back to the BCT through the Prophet control section. Prophet collection teams work independently or in tandem to establish fixed site location (DF) for signal emitters and serve as a SIGINT intercept station. They receive technical control and guidance from the Prophet Control section.

9-8. Modern SIGINT operations are challenged to keep pace with information technology and its related digital communications explosion. Today a requirement exists to collect and process signal information in support of the BCT CCIRs. SIGINT collection, as part of the total ISR effort, will be essential in locating, identifying, and tracking emitters. A fully integrated SIGINT collection capability can contribute significantly to developing the COP.

9-9. The Prophet collection teams provide signals intercept and DF data on threat emitters in the BCT's AO. Voice intercept exploitation will depend on the language capabilities of the 35Ps manning the Prophet system. A local language-specific 35P may augment each team when deployed. This augmentee and any of the Prophet collection team 35P that speak the local language can enhance the platoon's intercept capabilities since knowing what is being said in voice communication can provide combat information and help to determine the significance of the DF information that the platoon gathers.

9-10. The Prophet control team correlates line of bearing (LOB) data from the Prophet collection teams to locate threat emitters and evaluates the effectiveness of SIGINT collection operations. In the absence of a Prophet control team, the responsibility of data correlation, OPCON, and reporting falls upon the senior SIGINT collection operator. These additional responsibilities will have an impact on that team's ability to provide effective coverage of their assigned target area.

9-11. The collection teams, whether conducting operations in support of the brigade or the subordinate maneuver elements, must be placed in proximity to the signal source while maintaining communication with the control team. Due to the limited height of collection antennas, the low power output of threat emitters, and the line of sight constraints imposed by terrain, the collector must be deployed forward into the close combat area. The coordination of logistical support and security for the collection and control teams remains the responsibility of the squadron regardless of a team's support relationship.

Fundamentals of Employment

9-12. The key to the successful execution of the SIGINT collection mission is a division of labor into distinct areas by organizations of different echelons.

Technical Support

9-13. The MI Company's Prophet teams' ability to perform their mission depends on a number of factors. The primary factor is the BCT's ability to rapidly develop or access specific electronic order of battle (EOB) information about the threat. EOB and technical information on threat communications and noncommunications systems are essential to conducting signals intercept and DF. Regional and national

SIGINT activities are the BCT's primary sources for this information during the planning and initial execution of brigade operations.

9-14. The brigade S-2, in conjunction with the Analysis and Integration Platoon from the MI Company, will access EOB at EAB and provide that data to the Prophet control section. The Prophet teams, however, should not depend exclusively on these outside organizations to have comprehensive EOB and technical data for every operation. Sometimes, the technical data from EAB may also prove to be of little or no value in tactical operations, particularly during the initial hours and days of actual operations. Thus, Prophet teams deployed with an entry force or combined arms battalions in brigade operations must be prepared to collect and produce their own EOB SIGINT technical data to accomplish the mission.

9-15. The BCT staff, represented by the brigade S-2 and the MI Company, must rapidly access and develop technical information about threat communications systems and methods. SIGINT elements of the US Army Intelligence and Security Command (INSCOM) are the primary sources for information on the communications infrastructure within the AO and threat ground forces communications. The BCT staff feeds this information to the Prophet Control Section which provides the information to the Prophet collection teams. Once in the AO, the Prophet teams conduct surveillance of threat communications and develop technical data for electronic warfare support (ES) and EA.

Site Security

9-16. Due to the small size of the Prophet collection teams, the continuous (24-hour operations) nature of their mission and mission-specific site locations that the teams must employ to accomplish their mission, security augmentation will probably be necessary. The Ground Collection Platoon leader, in conjunction with the MI Company commander, may have to request this additional security augmentation from the BTB S-3 who may forward the request to the BCT S-3. Operating alone should be the last choice when employing Prophet teams, as it seriously degrades their collection capability and survivability.

Prophet Team Effectiveness

9-17. Prophet teams are most effective when—

- Employed in a stationary mode. DF accuracy is increased.
- Operated in a multi-station formation.
- Positioned to minimize system receiver interference. This increases the potential capability of the team to acquire threat emitters of significant interest in a timely manner.
- Positioned to optimize overlapping areas of intercept coverage.

Site Selection

9-18. Prophet collection team sites must meet certain requirements to accomplish its mission. These sites must—

- Be located within range of targeted transmitters.
- Ensure that the receiving antenna is positioned to intercept the arriving signal.
- Be located near its supporting elements.

9-19. Positioning the intercept antenna is the most important factor to consider when selecting sites. The Prophet collection team cannot intercept a threat signal or find a threat emitter unless it acquires the target. Numerous conditions can interfere with a team's ability to acquire threat signals. At a minimum, the following conditions need to be considered:

- Metallic Conductors. Avoid wire lines, such as telephone, telegraph, and high-tension power lines. Wire lines absorb an incoming signal and introduce distortion, hum, and noise into the receiving antenna. Some distortion of the arriving waveform may be acceptable if the site is for intercept operations only. But DF operations must be free from outside influences.
- Military Objects. Friendly emitters interfere with signal intercept. The team's communications on tasking, DF flash, and reporting nets are potential sources of interference. Other sources

include TA radars, FBCB2 mobile subscriber equipment, and SATCOM. If collocated among highly active communications systems, the Prophet collection team will not be able to use terrain-masking techniques to isolate their antennas from friendly interference. If the team is collocated with C2 assets, operators should use field telephones or runners to coordinate collection and reporting. The team should also place their equipment away from generators to reduce noise and electronic interference. If not collocated, the team may position its communications antennas so a hill mass screens them from intercept antennas and from the threat. This will cause a minimum of interference to intercept antennas and will mask observation.

- Terrain. Hills and mountains between the intercept antenna and the threat emitter will limit the quality of intercept. In mountainous terrain, selected antenna positions should be relatively high on the slopes or, if possible, on forward slopes. Locations at the base of a cliff or in a deep ravine or valley must be avoided. For operations above the high-frequency range, the team should select a location that will afford line of sight reception. In mountainous terrain, the objective is to get the antenna as high as possible. Soil content (such as high iron) is also a consideration for signals intercept and system grounding. Bodies of water can also be a problem between the collector, and the target emitter can also influence reception.
- Urban Objects. Some buildings near an intercept site can reduce the quality of the target signal. Every attempt should be made to position the intercept antenna as far from manmade objects as possible. Positions adjacent to roads and highways should be avoided. In addition to the noise and confusion caused by vehicles, their ignition systems may cause electrical interference. Copying weak signals requires a great deal of concentration by the intercept operator. The operator's attention should not be diverted by extraneous noises. Heavy traffic areas also are prime targets for air and artillery attacks.
- Vegetation. Trees near the antenna system offer advantages and disadvantages. Foliage can be used to camouflage the antenna system. It also can be used to mask the antenna system from unwanted signals. However, trees with heavy foliage absorb radio waves. Leafy trees have more of an adverse effect than evergreens. Foliage should not be positioned between the antenna elements and the target signals, and it should never touch the elements of the antenna. Intercept antennas should extend above the surface of the vegetation level when "looking" at the target transmitter. The antenna can be "masked" from unwanted signals if the foliage behind and to each side of it extends higher than the antenna.

Signals Intercept

9-20. Signals intercept includes actions to search for, intercept, and identify what the enemy is saying, doing, or what they are intending to do by means of intercepting their electronic communication. Signals intercept can provide information of immediate tactical value that will affect decisions and operations such as the identification of imminent hostile actions, threat avoidance, targeting, or EA. Signals intercept precedes all other Prophet collection team operations.

Signal Externals

9-21. Tactical-level Prophet collection teams exploit the external properties of signals. Externals are defined as the attributes or characteristics of the carrier wave such as the frequency, modulation, and method of transmission. The exploitation of signal externals provides support to the BCT's situational understanding and targeting. An LOB can be obtained from a single Prophet vehicle or dismounted collection system, and it provides a specific azimuth along which an enemy emitter dwells. However, pinpointing an emitter (obtaining a cross-fix) requires the application of two collection systems.

Signal Internals

9-22. Operational and strategic-level SIGINT organizations exploit the internal properties of signals. Internals are defined as the information transmitted on the carrier wave. The exploitation of signal internals

provides COMINT, technical data, and long-term target continuity. Tactical-level SIGINT teams can also exploit the internals provided the team has personnel assigned or attached who are experienced in Morse code or the target language.

9-23. Acquiring the intelligence gleaned from the exploitation of the signal internals in NRT remains critical at the tactical level. INSCOM units, in conjunction with other US cryptologic system organizations, provide this exploitation support either from a support base outside the BCT's AO via DCGS-A or by attaching forward support teams with special personnel and equipment for onsite operations.

Direction Finding

9-24. Friendly and threat forces utilize communications extensively. Even when radio operators are extremely conscientious about COMSEC procedures, Prophet collection teams can intercept and approximate the location of the signal emitter. Specifically, Prophet collection teams can use DF to determine—

- Movement of threat personnel or equipment.
- Locations of emitters associated with weapon systems and units.
- New emitter locations and confirmed known emitter locations.
- Possible targets for lethal and nonlethal attacks.

9-25. In addition to finding threat forces, DF operations can assist the friendly force. Prophet collection teams can support the BCT by—

- Locating and redirecting scouts, patrols, and, if attached, long-range reconnaissance units from reconnaissance objectives to friendly positions during limited visibility.
- Vectoring reconnaissance and combat forces to threat positions.
- Vectoring search and rescue personnel to downed aircraft and personnel beacons.
- Supporting CI assets conducting signal security assessments.
- Locating sources of communication interference and jamming.

9-26. DF involves determining the direction of arrival of a radio wave. DF systems indicate the approximate direction along an imaginary line upon which an emitter lies. This is commonly referred to as an LOB. A stationary Prophet collection team can determine only the approximate direction of an emitter. Also, the greater the distance from the Prophet Collection team site to the emitter, the greater the possibility for error. On the average, for every degree of error, there will be a 17-meter variation over each kilometer of range to the emitter.

9-27. Two stationary Prophet collection teams are able to approximate the general vicinity of an emitter. This approximation is determined by the intersection of two LOBs and is referred to as a "cut." Two teams working together or one team moving between two sites can produce a cut (provided the emitter remains stationary). A cut indicates the approximate location of an emitter. This data is adequate for nonlethal (electronic) attack but inadequate for targeting by lethal attack delivery systems.

9-28. Three or more stationary Prophet collection team sites can "fix" the location of a specific emitter. A fix indicates the most probable location of an emitter. LOBs from three different Prophet collection teams normally form a triangle when plotted on the map. This conclusion can also be reached with the LOB data of less than three Prophet collection teams which are moving among multiple sites or by an airborne platform. Through terrain analysis of the area within the triangle, the SIGINT collector or analyst can determine the most probable location of the emitter. Some systems are designed to automatically determine the emitter's location without collector or analyst intercession. A fix will generally result in an area target.

9-29. A factor that influences the accuracy of the fix is the geographical relationship of the Prophet collection teams with respect to the threat emitter. Multiple LOBs on the same threat emitter offer the most effective application of the SIGINT collection assets. Thus, Prophet collection teams are most effectively deployed, based on METT-TC into multi-station formations.

- Standalone is a single station formation where each Prophet collection team operates independently. This is the least desirable method of DF operations; however, a standalone system can perform signals intercept and DF while on the move. This mobile intercept and DF capability allows the flexibility to provide collection support to units during a variety of missions.
- When operating in a multi-station baseline, Prophet collection teams work together to locate and, if directed, track the movement of the threat emitter. A multi-sensor control team, when available, tasks each collection team to locate the same emitter. This entails the control team providing the collection teams with the frequency, and any technical data that would help the teams find the same emitter.

9-30. As Prophet collection teams are moved closer to threat emitters, DF accuracy improves and the collection teams develop the potential to hear and find deeper threat targets. Positions along the maneuver brigades' rear boundary limit collection to the close combat area. More forward positions allow for collection beyond the close battle area but may stretch the C2 links between the Prophet teams, the Prophet control sections, and the BCT TOC as well as degrade their survivability and mission capability if not augmented with security elements.

Transcription

9-31. Prophet collection teams, when augmented by a linguist in the proper language (optimally with voice intercept training) have the capability of collecting signal internals, such as messages in the threat language. These teams may be capable of recording and transcribing this information. Recording capabilities do not exist with all systems. Most reports require only the gist of message traffic. Transcription can be time consuming and requires thorough knowledge of the target and its language. However, when necessary, Prophet collection teams may develop extracts or complete translations of intercepted messages. These transcriptions should be forwarded to the control team for use in analysis of the ongoing threat situation and to aid in developing the threat database. These language functions, in most cases, cannot be accomplished by a Soldier with another language-dependent MOS, an Army Civilian, or a contracted civilian because they lack the required EW-related skills (voice intercept) or target knowledge.

9-32. Although the ES collection missions are of a passive nature (receive only), the BCT's SIGINT collection assets can provide effective support to the force, especially if supported by EAB airborne platforms. Prophet teams can be actively employed in ISR missions during the conduct of decisive full spectrum operations. Prophet teams are rapidly deployable and responsive to the commander's needs throughout all Army operations.

SATCOM Team

9-33. The SATCOM team is responsible for integrating SCI communications into the existing network architecture using the TROJAN SPIRIT system. TROJAN SPIRIT will be a component of DCGS-A (Version 4). The TROJAN SPIRIT organic to the Analysis and Integration Platoon will normally collocate with the BCT S-2 and the Analysis and Integration Platoon during operations. The intelligence analysts assigned to the TROJAN SPIRIT access the dedicated multi-level security, high-capacity communication link between BCT CPs, theater, joint, 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 system also provides the opportunity for secure, analytic collaboration externally to the BCT. The TROJAN SPIRIT also provides access to the JWICS through its JDISS.

HUMINT Collection Section

9-34. The BCT's HUMINT assets will be most effective in an SSC environment. Operations in an SSC rely heavily on extensive and continuous interpersonal contact throughout the AO. The HUMINT

Collection Section has one OMT and three HCTs. The HCTs are task organized and placed based on METT-TC to best meet the CCIRs.

9-35. When focused and synchronized properly, HUMINT can provide the BCT commander and staffs with an enhanced understanding of the threat. While most effective in the HUMINT-rich SSC environment, the HCTs must be prepared to conduct operations at all levels of conflict. The HUMINT collectors contribute to developing an understanding of the current situation by questioning local inhabitants and refugees, debriefing friendly forces, and tactical questioning and interrogation of detained persons to include enemy prisoners of war (EPWs) and DOMEX.

9-36. HUMINT supports the protection plan and answers the commander's intelligence requirements by employing HCTs to conduct focused collection, limited analysis, and production on the adversary's composition, strength, dispositions, tactics, equipment, personnel, personalities, capabilities, and intentions.

Operational Management Team

9-37. The OMT assists the Ground Collection Platoon leader and the MI Company commander in the C2 of assigned or attached tactical HCTs. The OMT also provides the teams with technical guidance and converts ISR taskings into specific team missions. Each OMT can control two to four collection teams. The OMT is normally collocated with the BCT S-2X at the BCT TOC and operates under C2 of the Ground Collection Platoon leader with guidance from brigade.

9-38. The S-2X works in conjunction with the OMT and provides technical guidance, intelligence oversight, source deconfliction, and specific tasking information to the OMT. The OMT supports the dissemination of taskings, reports, and technical data between the S-2X, BCT S-2, the Analysis and Integration Platoon and the deployed collection assets. When the BCT is augmented with HCTs from higher organizations, the brigade should also receive a proportional OMT augmentation. When two or more HCTs from the HUMINT section are attached, under OPCON or placed in DS of a subordinate element of the brigade, they should be accompanied by an OMT. When a single collection team is attached in DS of a subordinate element of the brigade, the senior team member exerts the control over the team normally provided by the OMT. OMTs—

- Provide technical guidance and control to the HCTs operating within the BCT.
- Coordinate HUMINT collection and CI collection requirements and operations of supported units with the S-2X team.
- Provide quality control over reporting by the collection teams.

HUMINT Collection Teams

9-39. HCTs are composed of four HUMINT collectors (MOS 35M (97E)). Additional personnel may augment the team as required. Interpreters from the outside organizations or civilian contractors with appropriate security clearance may be added when the language capability of the organic HUMINT collectors is inadequate to meet mission requirements. Technical intelligence personnel or other specific subject matter experts may augment the team to meet technical collection requirements.

9-40. The HCT mission includes—

- Screening operations.
- Conducting contact operations.
- Eliciting information from local sources.
- Debriefing operations.
- Conducting limited exploitation of foreign documents.
- Interrogating detained persons to include EPWs.
- Conducting liaison with local LEAs and foreign military security and intelligence services.
- Conducting limited HUMINT analysis.
- Conducting preliminary CI inquiries.

9-41. The HCT's command and support relationship will be determined by the BCT commander based on METT-TC and on recommendations from the BCT S-2, the S-2X, and MI Company commander. These relationships will be specified in the task organization portion of the BCTOPORD. Teams may be in a GS role directly supporting the BCT headquarters or under OPCON, attached, or in a DS role supporting subordinate elements of the BCT. In GS, the teams respond directly to tasking and mission guidance from the OMTs. The teams report all information to include administrative, technical (for example, contact reports, source registry information, ICF information), and intelligence information reports (IIRs) and size, activity, location, unit, time, and equipment (SALUTE) reports to the OMT. Information copies of SALUTE reports are also forwarded to units that would be immediately affected by the SALUTE information. The OMT forwards the administrative reports to the platoon leader and the technical and information reports to the S-2X.

9-42. In the DS role, the S-2 of the supported unit establishes the team's collection priorities. If two or more teams are in DS, they should be accompanied by an OMT and will respond to the supported unit's S-2 priorities through that OMT. DS teams, supported by an OMT, report all administrative, intelligence, and technical information to the OMT. The OMT forwards administrative information to the HCT leader, intelligence information to the supported unit S-2 with an information copy to the S-2X to expedite higher echelon reporting, and technical data to the S-2X. A separate DS team (not OMT) reports administrative information to the Ground Collection Platoon leader, intelligence information to the supported unit S-2 with a copy to the S-2X, and all technical data to the S-2X.

Task Organization

9-43. As described above, there are three organic HCTs of four personnel in the BCT. Once the BCT is alerted for deployment to a specific geographical region, the brigade may receive augmentation of additional four-person HCTs with the same MOSs and grades as the organic teams but with language capabilities in the target language. The augmentation teams must have organic transportation and automation equipment. Augmentee teams can consist of individuals drawn from different units or, if possible, as intact teams from a single unit.

9-44. These teams or individual augmentees should be integrated into the BCT to ensure the appropriate language is distributed among the organic and augmentation teams. If language qualified 35M are not available, the existing teams and the augmentation teams can have civilian contract linguists or other military linguists added to provide the language capability.

9-45. The structure of the section is modular to facilitate its augmentation by teams from higher echelons and the detachment of teams to provide DS to subordinate units of the brigade. All the brigade's HUMINT assets should usually support the brigade's initial entry force. During entry operations, the OMT can be deployed with the brigade tactical CP or alternately can be deployed with the S-2 of the entry battalion or squadron. In combat operations involving the entire brigade, HCTs should be attached, under OPCON, or in DS of maneuver battalions and the reconnaissance squadron or even their subordinate companies and troops. This requirement is based on—

- The relative importance of that subordinate element's operations to the overall brigade's scheme of maneuver.
- The potential for that subordinate element to capture EPWs, documents, and materiel or encounter civilians in the operational environment.
- The criticality of information obtained from those sources to the success of the brigade's overall OPLANs.

9-46. Although organized into four-person teams, the most expedient deployment of HCTs in any environment is in two-person elements in a vehicle. This maximizes battlefield coverage particularly when operating in an urban environment or a large AO. This configuration allows room in the vehicle for interpreters, technical experts, and security. Dividing the team into two-person elements in separate vehicles allows the elements to provide overwatch when moving through hostile terrain. These procedures, while advantageous, require the procurement of additional vehicles and may not be operationally possible.

9-47. HUMINT collectors are deployed to areas of maximum anticipated source potential to rapidly collect and exploit immediate tactical information. Centrally locating the assets at brigade EPW collection points or refugee camps, if any are established, results in unacceptable delays in critical time-sensitive intelligence reporting; this is due to the time involved in moving the sources of information to central locations and should only be done in highly static situations. The closer the collector is to where the source is first encountered, the more timely and responsive is the information collected.

9-48. In stability operations, the teams are normally centrally managed with the OMT collocated with the BCT S-2. The HCTs will normally be in GS to the brigade but will operate throughout the brigade AO within the AO of the brigade's subordinate units. The placement and distribution of the teams will be based on the brigade OPORD and the MI Company commander's evaluation of the collection potential of each area.

9-49. Limiting HUMINT collectors' access to potential sources or placing the collectors in locations that prevent them from contacting sources in time to affect operations severely curtails the effectiveness of HUMINT collection. For example, in a stability and civil support, the HUMINT collectors must be in continual contact with the local population to provide reliable FP information. As the threat level increases, commanders have the tendency to restrict units to their base camps. This is counterproductive for HUMINT collectors because it restricts their source access at precisely the time that the source information may prove critical to FP.

Command and Control

9-50. In terms of C2, the chain of command extends from the BCT MI Company to Ground Collection Platoon to OMT to HCT. In terms of parallel technical authority channels, the BCT S-2X coordinates through the OMT to provide priorities and taskings to HCTs. Technical authority channels ensure adherence to existing policies or regulations and provide technical guidance for MI operations. The BCT MI Company provides HCTs logistic and administrative support. The maneuver battalion S-2 directs the DS HCT. The S-2X/OMT provides technical expertise to assist the MI Company and battalion S-2 plan, prepare, execute, and assess portions of the HCT's collection efforts. For more information on this relationship, see TC 2-22.303 (S/NF).

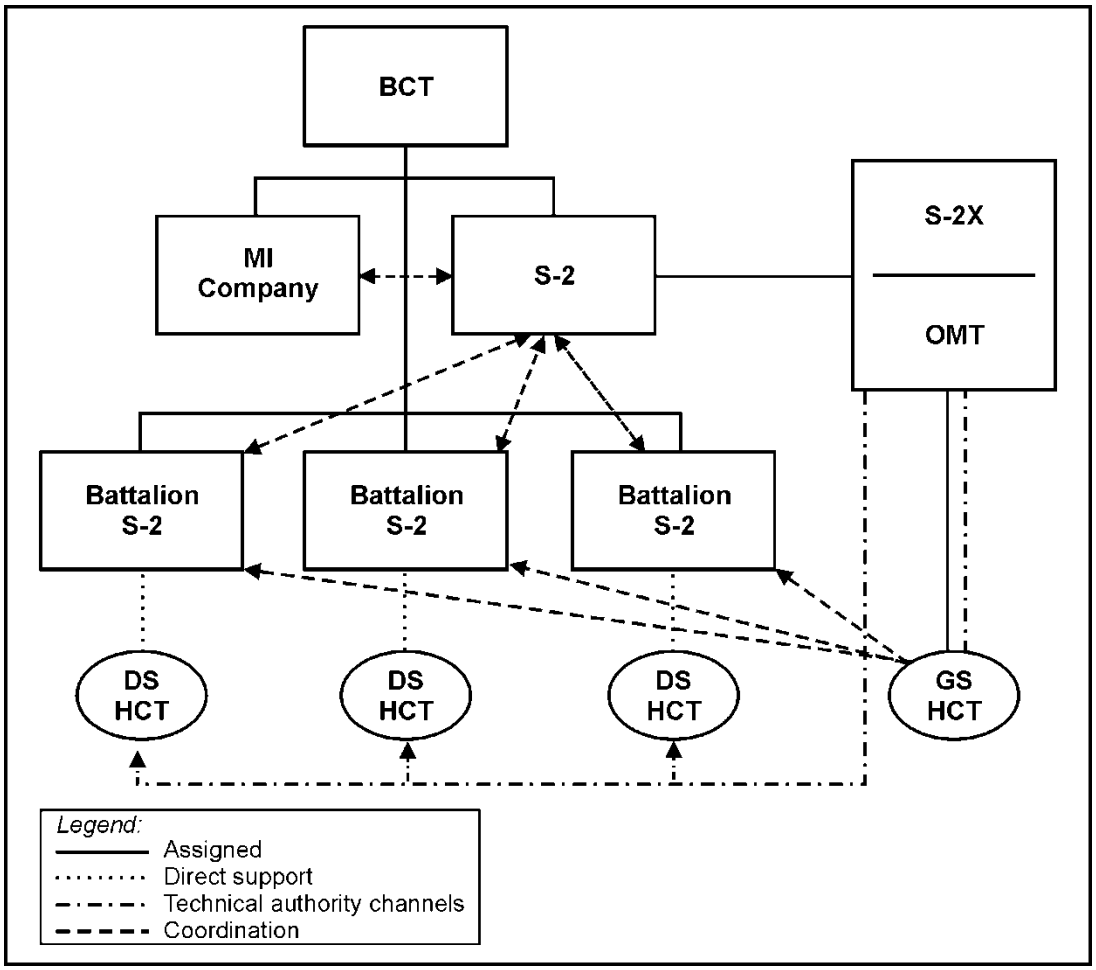


Figure 9-1. BCT HUMINT relationships

9-51. The HCT is a working part of the intelligence warfighting function of the maneuver battalion it is directly supporting. Therefore, an HCT in DS to a maneuver battalion must be collocated with the battalion TOC or S-2. The continuity gained from collocation with the battalion S-2 or TOC is invaluable. The HCT cannot practically support the maneuver battalion without being embedded within the battalion staff. When HCT's are located outside of the battalion S-2/TOC, the potential for HUMINT operational planning parallel with maneuver operational planning is severely limited. Another point of consideration is the "out of sight, out of mind" mind set. It is hard to convince a maneuver battalion commander and staff to provide support required by the HCT to conduct efficient military source operations (MSO) when the HCT is not physically present. This physical presence allows the supported battalion command and staff to see the consistent value added of the DS HCT and increases the likelihood that the DS HCT will be effectively integrated into operational planning.

9-52. When available it is recommended that an HCT be retained in a GS relationship to the BCT. This GS HCT would receive specific collection guidance from the 2X/OMT in order to answer the BCT commander's PIR. The BCT S-2X/OMT would coordinate all GS HCT movement through the BCT operations officer (S-3). The S-2X/OMT would provide tasking and guidance to the GS HCT, coordinated through the S-2/S-3. A GS HCT provides a BCT a significant advantage when the commander's line of operation spans multiple battalion boundaries.

Use of GS HCT in OIF

In OIF a particular adversary Sunni network stretched from the extreme southeastern corner to the far western edge of one BCT's AO. This adversary network—consisting of enablers, direct action members, financiers, coordinators, and explosives experts—operated across three battalion sectors. The adversary network took advantage of a gap created by unit boundaries. Because each battalion's DS HCT could not traverse their own unit's boundaries, no one HCT could effectively pursue establishing a source network to successfully target along this line of operation. To overcome this challenge, the BCT employed a GS HCT to help target the adversary network across the entire BCT AO, uninhibited by battalion boundaries. The GS HCT source pool derived from (and later restored to) DS HCT source pools as BCT targeting efforts shifted.

9-53. When a GS HCT operates in a maneuver battalion AO, the 2X/OMT must coordinate with battalion S-2s. The 2X/OMT must direct the GS HCT to address battalion-level as well as BCT-level intelligence collection requirements. When operating in a battalion AO, recommend the GS HCT provide courtesy entry and exit briefs to the battalion S-2. The S-2X/OMT, GS HCT, DS HCT, and battalions S-2 must foster an environment of cooperation, and sharing to ensure everyone has full visibility of operational and intelligence information.

Reporting

9-54. All intelligence information reporting from the HCTs is reported to the OMT for further distribution. If deployed in a DS role, the intelligence information reports are sent to the supported S-2 with an information copy sent to the OMT.

HUMINT Collection Team Operations

9-55. HUMINT collectors must understand specific terms used to identify categories of personnel when referring to the principles and techniques of interrogation. To ensure understanding and correct identification individuals involved in HCT operations should be familiar with TC 2-22.302 (S/NF). Determination of a detainee's status may take significant time and may not be completed until well after the time of capture. Therefore, there will be no difference in the treatment of any category of detainee from the moment of capture until such a determination is made. The following terms are presented here.

- Civilian Internee: A person detained or interned in the United States or in occupied territory for security reasons, or for protection, or because they have committed an offense against the detaining power, and who is entitled to "protected person" status under the Geneva Conventions (GW).
- EPW: A detained person, as defined in Articles 4 and 5 of the Geneva Convention Relative to the Protection of Civilian Persons (GPW). In particular, one who, while engaged in combat under orders of his or her government, is captured by the armed forces of the enemy. As such, he or she is entitled to the combatant's privilege of immunity from the municipal law of the capturing state for warlike acts that do not amount to breaches of the law of armed conflict. For example, an EPW may be, but is not limited to, any person belonging to one of the following categories of personnel who have fallen into the power of the enemy; a member of the armed forces, organized militia or volunteer corps; a person who accompanies the armed forces, without actually being a member thereof; a member of a merchant marine or civilian aircraft crew not qualifying for more favorable treatment; or individuals who, on the approach of the enemy, spontaneously take up arms to resist invading forces.
- Other Detainees: Persons in the custody of the US Armed Forces who have not been classified as an EPW (Article 4, GPW), retained personnel (Article 33, GPW), and Civilian Internee (Articles 27, 41, 48, and 78, GC) shall be treated as EPWs until a legal status is ascertained by competent authority; for example, by Article 5 Tribunal.

- Retained Personnel: (See Articles 24 and 26, GWS.)
  - Official medical personnel of the armed forces exclusively engaged in the search for, or the collection, transport, or treatment of wounded or sick, or in the prevention of disease, and staff exclusively engaged in the administration of medical units and facilities.
  - Chaplains attached to the armed forces.
  - Staff of National Red Cross Societies and that of other Volunteer Aid Societies, duly recognized and authorized by their governments to assist Medical Service personnel of their own armed forces, provided they are exclusively engaged in the search for, or the collection, transport or treatment of wounded or sick, or in the prevention of disease, and provided that the staff of such societies are subject to military laws and regulations.
- Protected Persons: Civilians entitled to protection under the GC, including those we retain in the course of a conflict, no matter what the reason.
- Enemy Combatant: A person engaged in hostilities against the United States or its multinational partners during an armed conflict. The term "enemy combatant" includes both "lawful combatants" and "unlawful combatants."
  - Lawful Enemy Combatant: Lawful enemy combatants, who are entitled to protections under the Geneva Convention, include members of the regular armed forces of a State Party to the conflict; militia, volunteer corps, and organized resistance movements belonging to a State Party to the conflict, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the laws of war; and members of regular armed forces who profess allegiance to a government or an authority not recognized by the detaining power.
  - Unlawful Enemy Combatant: Unlawful enemy combatants are persons not entitled to combatant immunity, who engage in acts against the United States or its multinational partners in violation of the laws and customs of war during an armed conflict. Spies and saboteurs are traditional examples of unlawful enemy combatants. For purposes of the war on terrorism, the term "unlawful enemy combatant" is defined as, but not limited to, an individual who is or was part of or supporting Taliban or al Qaeda forces, or associated forces that are engaged in hostilities against the United States or its multinational partners.

9-56. HUMINT collection requires access to sources and contacts that have had "eyes on target." For example, HUMINT collectors can locate weapons caches through source questioning and map tracking or can support a route reconnaissance by questioning local civilians encountered along the route about threat activity. HUMINT collection is limited by their source's knowledge. Successful HUMINT collection requires that there be an individual (EPW, detainee, local civilian, refugee) that has that information and that the collector is placed in contact with that source; identifies that he or she has the required information; and questions the individual prior to the LTIOV.

9-57. A detainee is any person captured or otherwise detained by an armed force. An EPW is a detainee who meets the criteria of Articles 4 and 5 of the GPW. Detainees may be interrogated. They are frequently excellent sources of information, but in many instances the access of the HUMINT collector to the detainees may be curtailed.

9-58. For example, when supporting a counterinsurgency, the supported government may consider all captured insurgents to be criminals and not allow US forces access to them. In these instances, US HUMINT collectors should attempt to sit in during local questioning; they could submit questions or, at a minimum, coordinate to receive the reports from local authority questioning. US HUMINT collectors must remember that regardless of the legal status of the detainees, they must be treated in a manner consistent with the principles of the Geneva Conventions.

9-59. HUMINT collectors may interrogate a wounded or injured detainee provided that they obtain permission from a competent medical authority and that the questioning will not delay or hinder medical treatment. Questioning may not delay the administration of medication to reduce pain or the evacuation of the detainee to where they may receive medical treatment, nor will interrogation be allowed if it would

cause a worsening of the condition of the detainee. In most cases, this simply requires the HUMINT collector to ask the doctor, medic, or other medical personnel if it is all right to talk to the detainee.

9-60. With the doctor's permission, the HUMINT collector may talk to the detainee before, after, or during medical treatment. The HUMINT collector cannot at any time represent themselves as being a doctor or any other type of medical personnel. Nor can the collector state, imply, or otherwise give the impression that any type of medical treatment is conditional on the detainee's cooperation in answering questions.

9-61. The key to successful HUMINT operations is a thorough understanding of the human aspects of the AO, a predictive analysis of collection potential, rapid screening and evaluation of potential sources, and a detailed questioning of available sources.

9-62. Limiting HUMINT collectors' access to potential sources or placing the collectors in locations that prevent them from contacting sources in time to affect operations severely curtails the effectiveness of HUMINT collection. For example, in a stability operation the HUMINT collectors must be in continual contact with the local population to provide reliable protection information. As the threat level increases, commanders have the tendency to restrict units to their base camps. This is counterproductive for HUMINT collectors because it restricts their source access at precisely the time that the source information may prove critical to protection.

9-63. In support of combat operations, detainees, to include EPW, are normally exploited for PIRs and other combat information as close to the point of capture as operationally feasible. EPWs are evacuated as rapidly as possible to the highest echelon-holding facility in the theater for detailed interrogation. Joint forces from EAC normally staff this facility. In combat operations placing brigade HCTs at brigade detainee collection points rather than with forward combat elements may degrade their ability to collect combat information in time to support command decisions. Refugees and civilians on the battlefield are also exploited as soon as possible rather than waiting until they have been moved to collection points.

9-64. There may be occasions, particularly in the early stages of a stability operation, when they are inadequate to meet all the brigade's HUMINT mission requirements. The brigade must identify HUMINT requirements early and request additional HUMINT collectors from higher as necessary. HUMINT collectors (MOS 35M, 351M [MOS 97E, 351E]) should not be used as translators or interpreters unless that mission also includes HUMINT collection potential.

9-65. Linguist augmentation will probably be required to conduct HUMINT collection operations. While some HUMINT collectors (MOS 35M, 351M) are trained in a foreign language, it may not be the correct language or dialect, or the collector's proficiency may not be adequate to meet mission requirements. The base augmentation plan is designed to place at least two language-qualified personnel (HUMINT collectors or CI agents) with each four-person team. This plan must be modified when the BCT is operating in an area that includes more than one base language. In rapid deployment scenarios to areas with languages that are not normally present in the Active or Reserve Component forces, additional linguist support may be needed. The MI Company commander assesses the ability of the company HUMINT collectors to meet mission requirements. The commander coordinates with the S-1 to identify other language-qualified personnel in the brigade and with the S-3 to project any mission shortfall.

Human Sources

9-66. Every person—friendly, hostile, or neutral—is a potential source of information. The HUMINT information collection system uses various methods to collect information from a number of sources. The HCT does not confine itself to one method of collection or a single type of source. The effectiveness of HUMINT collection lies in creating a balanced mix of collection methods applied to a variety of sources. Three categories are used to distinguish between the types of contacts:

- Category 1 – One-time contact.
- Category 2 – Continuous contact.
- Category 3 – Formal contact.

9-67. The following sources are not all-inclusive nor are the listed categories exclusive. For example, a local national employee might be a walk-in source and later be developed as a protection requirements source operation source. With the exception of Level 1, there is no limit on the number of times a team can meet sources without making them Level 3. However, all sources must be registered with the J/G/S-2X after the first meeting.

Level 1 - One-Time Contact

9-68. The one-time contact is a source of information of value who we will encounter only once. A one-time contact could, for example, be a traveler who happened to pass through the AO. Other than the information obtained from a one-time contact, the HCT must make a reasonable effort to obtain as much basic data as possible about the one-time contact. Complete name, occupation, address, and other basic data of this source are crucial for a thorough analysis of the information provided.

9-69. The one-time contact and the information he or she provides cannot be assessed and evaluated independently; however, the information provided by a one-time contact must be reported and corroborated through other HUMINT sources and even other intelligence disciplines. If a one-time contact is encountered for a second time and provides information of value, then he or she may be treated as a developmental lead.

9-70. Walk-In Source: The walk-in is any person, regardless of affiliation, who volunteers information of value to US forces on his or her own initiative.

- The walk-in source may volunteer information by approaching a HCT, other ISR elements, or US forces.
- The supported unit must have in place a program to identify, safeguard, and direct the walk-in to the appropriate collection asset for an interview. The collection asset will interview the walk-in to determine the type of information the source has and to determine and evaluate the reliability of the individual.
- After identifying the type of information, the collector determines if he or she has the jurisdiction to collect that information. If, for example, the walk-in wishes to report a crime, the collector refers that individual to the proper agency. Systematic questioning plans, deception, detection techniques, and cross-checking of information are used extensively in the evaluation process. Concurrently, there are national level directives, DOD directives, and Army regulations that direct specific actions to be taken with a walk-in.
- When dealing with a walk-in source, the supported unit and the collection asset must guard against adversary intelligence or other intelligence collection attempts; they must also protect legitimate sources of information. The walk-in is thoroughly debriefed on all areas of information relevant to collection requirements, and any information of value is reported.

9-71. Developmental Lead: A developmental lead is an individual identified through social and professional status, leads, source profiling, or other techniques that has knowledge required by the commander.

- The HCT normally should express operational interest as soon as possible. While not every developmental lead becomes a source of information, the HCT should see each developmental lead as a potential source of information and apply the appropriate security measures.
- The developmental lead is continuously assessed to verify his or her placement and access to the type of information the HCT is seeking. Additionally, the HCT continuously assesses the motivation and characteristics of the developmental lead.

Level 2 - Continuous Contacts

9-72. These are individuals met by HUMINT and CI personnel for the purposes of collecting information in response to the commander's PIRs.

- Local National and Third-Country National Employees.

- Local national and third-country national employees are non-US personnel from either the country in which the US forces are operating or a third country who are either employed by US forces directly or through a contractor to provide logistical support and services. One of the purposes of locally employed personnel screening is to assess these individuals as potential sources of information.
- Local national and third-country national employees can be a prolific source of information about local attitudes and events, particularly in a restrictive environment where US contact with the local population is curtailed. Their information can be significant in an FP role. The collector must register these individuals with the J/G/S-2X.
- All locally employed personnel are considered a security risk and must be screened and evaluated by the collector. There are situations when locally employed personnel approach US forces to volunteer information. In these situations, they must be dealt with as walk-ins.

9-73. Dislocated Civilians: "Dislocated Civilian" is a generic term that includes a refugee, a displaced person, a stateless person, an evacuee, or a war victim.

- Dislocated civilians are an excellent source of information about denied areas and can be used to help identify threat agents and infiltrators. The degree of access HUMINT collectors have to dislocated civilians depends on the ROE and Status of Forces Agreements (SOFAs) in effect. HUMINT collectors can work with CA or other programs dealing with dislocated civilians.
- Dislocated civilians are normally considered one-time sources but may be incorporated into other long-term collection programs if their degree of knowledge warrants this. In this case adherence to the restrictions involving military source operations is necessary.
- A dislocated civilian can be detained and/or interned during an armed conflict or occupation for security reasons, protection, or because he or she has committed an offense against the detaining power.

9-74. US forces have many opportunities to interact with the local population in the normal course of their duties in operations from PMEs to MCOs. They are perhaps the most under-utilized HUMINT collection resource.

- Some US forces, such as combat and ISR patrols, are tasked and debriefed by the appropriate level S-2, but others, such as medical teams or engineers who have extensive contact with the local population, are seldom debriefed. Commanders and staff members who serve as liaison with the local population and local government officials can be fruitful sources of information. CA, PSYOP, military police (MP), and other elements also have legitimate reasons to conduct liaison and should be debriefed as appropriate.
- The friendly force debriefing effort can succeed only with command emphasis. HUMINT collection elements need to coordinate with local units to identify those individuals who would be most profitable to debrief and to further coordinate with them for time to conduct the debriefing. HUMINT collectors must ensure that their friendly force debriefing effort does not interfere with the normal duties of the person being debriefed. Except for patrols and ISR elements whose job is information collection, US forces should not be tasked to collect specific information but should be questioned only on what they encountered in the normal performance of their duties.

9-75. Official Liaison: Liaison with local military, government, or civilian agency officials provides an opportunity to collect information required by the commander.

- The HCT meets with these officials to conduct liaison, coordinate certain operations, collect information, and obtain leads to potential sources of information.
- Elicitation is the primary technique used with liaison contacts, although in many cases there is a more formal exchange of information. Information obtained by these elements through liaison normally tends to be the party line and may not be entirely accurate or complete.

9-76. Detainees: A detainee is any person captured or otherwise detained by an armed force.

- An EPW is a detainee who meets the criteria of Articles 4 and 5 of the Geneva Convention Relative to the Treatment of Prisoners of War.
- Within the limits of the theater policy and SOFAs, detained persons may be interrogated. Interrogations can only be conducted by personnel trained and certified to conduct interrogations under Department of Defense (DOD), DA, and theater policy. Detainees are frequently excellent sources of information but in many instances the access of the HUMINT collector to the detainees is severely curtailed. For example, when supporting a counterinsurgency, the supported government may consider all captured insurgents to be criminals and not allow US forces access to them. In these instances, US HUMINT collectors should attempt to sit in during local questioning. They could submit questions or, at a minimum, coordinate to receive the reports from the local authority. The US HUMINT collector must remember that, regardless of the status of the detainee, all detainees are entitled to humane treatment as well as any rights and privileges extended to them by international or US law.

Level 3 - Formal Contact

9-77. These are individuals who have agreed to meet and cooperate with HUMINT and CI Soldiers for the purpose of providing information. While these meetings are overt, Level 3 contacts are met discretely to protect their relationship with HUMINT and CI Soldiers. Knowledge of their meeting with HUMINT and CI Soldiers is restricted. CI and HCTs take extraordinary measures to protect their relationship with the contacts.

Collection Methods

9-78. The brigade RM team, with S-2X support, develops HUMINT collection requirements. The requirements will be validated by the brigade S-2 and tasked by the brigade S-3. The MI Company commander will receive the tasking. However, because of the sensitive nature of the information involved in this type of collection, specific mission parameters, technical data, and source information may be transmitted directly between the S-2X and the OMTs. CI and HCTs conduct screenings, interrogations, debriefings, elicitations, and DOMEX to obtain combat information on threat capabilities, ISP disposition, and intentions.

Screening

9-79. While screening is not in itself an information collection technique, it is vital to the rapid collection of information. Personnel screening is used in conjunction with interrogation and debriefing. Document screening is used in conjunction with DOMEX operations.

- Personnel screening is the rapid but systematic evaluation of large numbers of people to determine which individuals are the most likely to have and provide information in response to collection requirements. Personnel are evaluated on potential information and level of cooperation. Personnel screening can also be used in protection requirements operations to identify locally employed personnel who may have information of collection interest or who may pose a security threat.
- Document screening is the rapid but systematic evaluation of documents to determine which documents contain priority information. Selected priority documents will be exploited immediately for combat information and evacuated expeditiously (often electronically) to a DOMEX facility. DCGS-A provides a machine language capability that may be used for immediate document exploitation.

Interrogation

9-80. Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Some examples of persons subject to interrogation are EPWs, civilian

internees, and other detainees. Initial interrogation for PIRs and other combat information normally are conducted as close as possible to where the individual is captured or detained. More detailed interrogations are conducted at the "theater" holding facility. In stability operations, the ability to conduct interrogations may be limited by SOFAs, other international agreements, or theater policy. For questions regarding the authority to conduct interrogations, contact the BOLT.

Debriefing

9-81. Debriefing is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is not in the custody of the forces conducting the questioning. The two primary categories of sources for debriefing are friendly forces to include military and civilian personnel and foreign personnel, such as refugees, displaced civilians, government or military officials, and local inhabitants.

Elicitation

9-82. Elicitation is the gaining of information through direct interaction with a human source where the source is not aware of the specific purpose for the conversation. Elicitation is the baseline method for initiating military source operations.

Document and Media Exploitation

9-83. DOMEX is the systematic effort to extract information to answer collection requirements from documents. A document is any written or recorded information. Documents that are exploited include any document produced by the threat forces such as OPORDs, supply requests, personnel lists; other official and unofficial documents (such as government and opposition political party announcements); and open-source material (such as local newspapers and television). The HCTs supporting brigade operations perform preliminary DOMEX for information of immediate tactical interest dealing primarily with documents found on or in immediate association with EPWs, civilian detainees, refugees, and other HUMINT sources.

9-84. Large-scale DOMEX is normally conducted at a DOMEX facility located at the theater level. If, in an SSC operation, the brigade has responsibility for a DOMEX facility, augmentation from higher echelons is required. The exploitation of documents captured on or in association with HUMINT sources is done in conjunction with the initial tactical questioning of these individuals. Documents that cannot be exploited by the HCTs in a timely fashion, due to their size or technical nature, are scanned and transmitted electronically to the rear DOMEX facility for translation and exploitation. Intelligence information extracted from documents may be reported via SALUTE report or Intelligence Information Report.

This page intentionally left blank.

Appendix A

Brigade Combat Team Intelligence Readiness Training

A-1. The Army relies largely on a CONUS-based force with a relatively small forward presence that can rapidly project combat power anywhere in the world. Built on a foundation of intelligence readiness, the brigade's intelligence system provides the commander with intelligence needed to plan, prepare, and execute these force projection operations. The BCT intelligence warfighting function personnel must train continuously, both individually and collectively, in order to maintain proficiency on the wide variety of available capabilities.

MISSION

A-2. The brigade S-2 ensures the brigade intelligence disciplines successfully answer the commander's CCIRs throughout the extent of warfighting operations.

INTELLIGENCE READINESS

A-3. The scale, scope, pace, intensity, and complexity of future military operations place new demands on information collection, processing, analysis, and dissemination. The BCT S-2 must discern from the general global condition specific, current, and emerging contingency areas. The S-2 must identify windows of opportunity to shape the leadership's knowledge of potential adversaries. Successful intelligence support during force projection operations relies on continuous information collection and intelligence production before and during the operation.

A-4. The discussion below generally assumes that the BCT's part is not assuming a mission already being conducted by other US or multinational forces. If the BCT is assuming an ongoing mission from another US or multinational force, the primary source of intelligence should be the unit in theater who currently occupies the AO and is conducting the mission that the BCT is tasked to assume. Contact should be established with the outgoing unit at the earliest opportunity in order to ensure that the incoming BCT intelligence personnel gain as much situational understanding as possible prior to deployment.

A-5. Intelligence readiness operations support contingency planning and preparation by developing baseline knowledge of multiple potential threats and other conditions of operational environments. These operations and related intelligence training activities engage and challenge the intelligence warfighting function to respond effectively to the commander's contingency planning intelligence requirements.

A-6. During normal garrison activities, the BCT intelligence architecture must define the full spectrum of threats and forecast future threats and dangers so the BCT can learn to respond effectively. Real world intelligence activities in garrison are essential to maintaining the readiness of intelligence Soldiers and BCT leaders. The Brigade S-2 utilizes DCGS-A to conduct real world intelligence operations and maintain contact with current adversary information while in garrison to prepare for deployment. During planning and training, the commander conducts critical examinations of the brigade's force structure, operations, and training to improve the brigade's ability to execute ISR operations. These examinations ultimately lead to a mission-ready ISR force, which supports the needs of the commander and meets the key force projection imperatives of flexibility, scalability, and tailorability.

A-7. In a force projection operation, higher echelons will provide intelligence for situation and target development to lower echelons ("top down") until the tactical ground force completes entry and secures the lodgment area. The higher headquarters intelligence section may be reluctant to push everything down through tactical level intelligence channels due to the volume of the intelligence information available. DCGS-A provides the Brigade S-2 access to theater and national databases with the ability to collaborate with Knowledge Centers.

A-8. Intelligence readiness training helps to ensure that brigade intelligence personnel and assets are able to meet the brigade's needs during brigade operations. The BCT commander—

- Needs intelligence to support contingency-based training and planning of the brigade staff and its subordinate battalions.
- Needs the broad understanding of the operational environment of the contingency area that comes from continuous interaction with higher echelon and joint intelligence organizations.
- Must focus and drive the intelligence system daily to ensure this support is available and that the forces and staffs are ready to conduct force projection operations.

A-9. The Brigade S-2 must anticipate, identify, consider, and evaluate all potential threats to the entire brigade throughout force projection operations. This is especially critical during the deployment and entry operations stages of force projection. During these stages, the brigade is vulnerable to threat actions because of its limited combat power and knowledge of the AO. Intelligence personnel must, therefore, emphasize the delivery of combat information and intelligence products that indicate changes to the threat or other conditions of the operational environment developed during predeployment IPB.

A-10. The most significant change in the evolution of force projection operations is the enhanced information flow through hierarchical and nonhierarchical networks (computer, communications, and personal). The S-2 should—

- Review available databases on assigned contingency AOIs; conduct IPB on these AOIs; and develop appropriate IPB products.
- Be aware of higher headquarters SOPs and DIA manuals for specific ISR management guidance.
- Preplan and practice an intelligence "surge" on likely contingency crises.
- Establish and maintain (from predeployment through redeployment) connectivity and information sharing with personnel from HUMINT, IMINT, MASINT, SIGINT, IO, SWO, CA, PSYOP, and SOF units and organizations.
- Use DCGS-A enterprise to gain and maintain contact with forward units and obtain current and updated adversary information.
- Ensure the following are a part of the daily operating environment:
  - External augmentation.
  - SOPs which include a linguist plan with proficiency requirements (alert through early entry phases of deployment).
  - Training (individual and collective).
- Employ intelligence reach concepts to form ad hoc intelligence links and networks early on to meet a developing contingency.
- Incorporate, request, and receive intelligence from unfamiliar sources (linguists, MI augmentation, other services); exploit NGOs and private volunteer organizations once a crisis emerges.
- Exchange communications protocols with higher headquarters, subordinate, and lateral units.
- Forward all requests for intelligence information to higher headquarters in accordance with SOPs.

A-11. To draw intelligence from EAB and focus brigade intelligence downward based on the commander's needs, the S-2 must—

- Understand the BCT’s multiple echelon and broadcast dissemination capability to ensure NRT reporting to all deployed, in transit, or preparing to deploy forces.
- Maintain an intelligence database for each contingency.

A-12. The S-2 must also state and record the CCIR as PIRs, subordinate ISR tasks, and include the following:

- The commander's approval of the AOI, to include separate ground, air, littoral waters, and political AOIs.
- Maps, terrain, and weather products. Request from National Geospatial-Intelligence Agency (NGA) hard copies (unclassified or at the lowest classification);

- Request authority to declassify these products locally.
- Digitized products (map sheets, terrain data, and imagery).
- Physical environmental information. The TERRABASE program allows S-2s to template the effects of terrain on communications and direct fire. During mission analysis, TERRABASE or other automated terrain products provide the S-2 a tool to help the commander visualize how terrain can affect friendly and threat forces. These products can illuminate terrain effects for subordinate commanders in the OPORD brief. The supporting engineer staff officer may also have terrain visualization products.
- Threat or potential threats. The intelligence community, primarily National Ground Intelligence Center (NGIC) and open sources provide products useful for intelligence readiness. These products can be tailored to best support the commander. The S-2 can access numerous products developed at the national level via DCGS-A. Examples of these products include—
  - Daily INTSUMs and briefings.
  - Global security forecasts.
  - Battlefield development plans.
  - Automated and hardcopy databases.
  - Arms proliferation and military power studies related to the weapons acquisition strategies and the overall military power and potential of selected foreign military forces.
  - Technical intelligence (TECHINT) and user bulletins.
  - Central Intelligence Agency (CIA) World Fact Book and the DIA country studies.
  - Joint Intelligence Center (JIC) assessments.
  - Open-source studies and articles.
  - JIC threat characteristics database.
  - DIA ISPs as well as DIA contingency support studies and contingency support packages.
  - Other services.

INDICATIONS AND WARNINGS

A-13. Theater and national intelligence units monitor regional and global threats to provide I&W intelligence to the Secretary of Defense and military commanders. I&W intelligence flows to strategic, operational, and tactical commanders; it prevents surprise, reduces risk, and supports development and refinement of CONPLANs. The S-2 must assist the brigade commander in identifying PIRs, intelligence requirements, and targeting requirements for each assigned contingency area. The S-2 should—

- Review and refine unit ISR plans and preplanned ISR tasks for each contingency area.
- Review and modify reporting procedures for contingency areas.
- Prioritize and forward RFIs to higher headquarters.
- Disseminate intelligence and information to the commander, staff, and subordinate units.
- Coordinate for direct dissemination when possible.
- Adjust intelligence readiness steps according to pre-crisis I&W.

This page intentionally left blank.

Appendix B

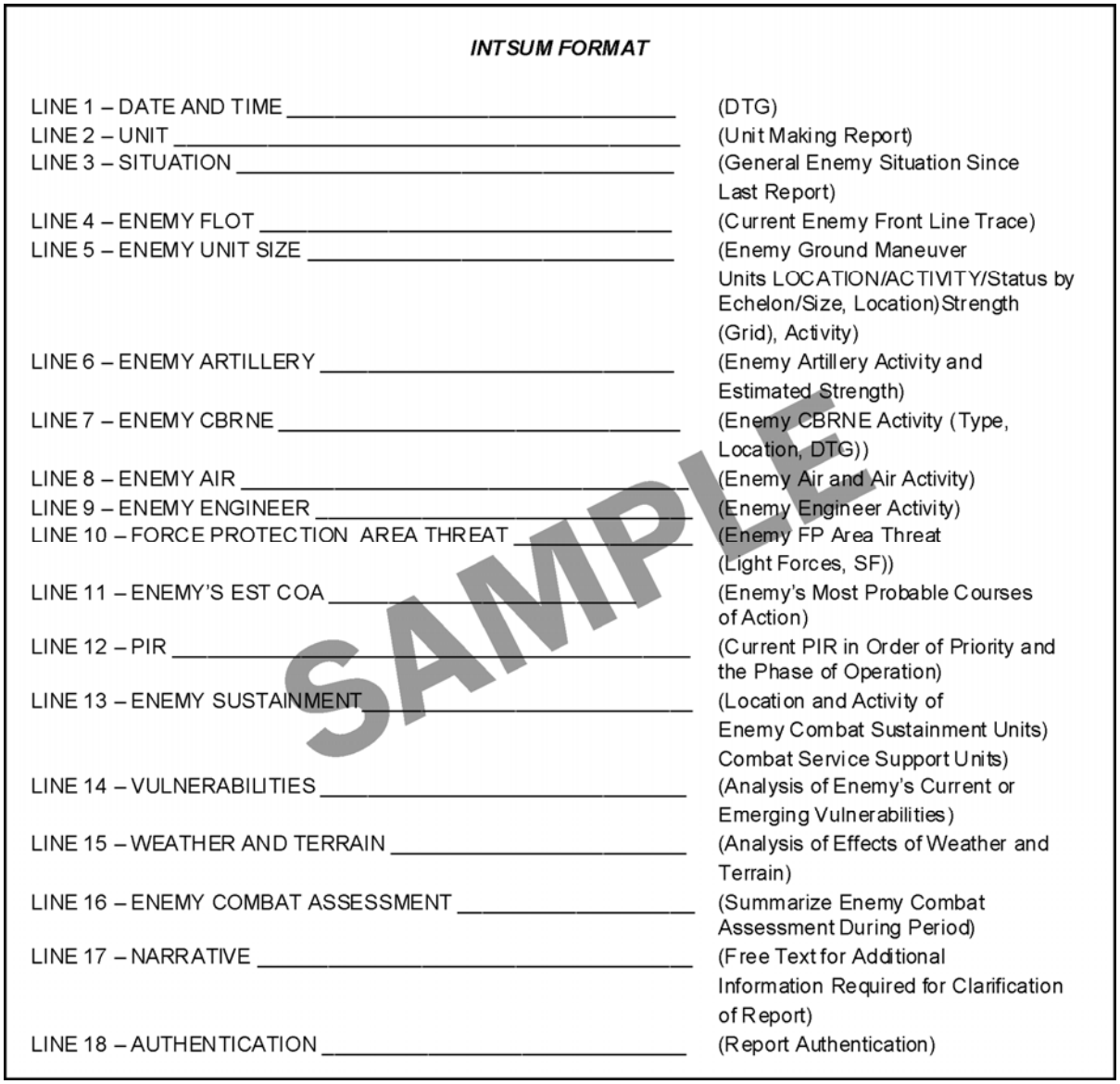
Reports

B-1. This appendix provides examples of the most common reports the BCT uses. For a full listing of all Army intelligence-related report and message formats, see FM 6-99.2.

- Example Intelligence Summary (INTSUM) – figure B-1.
- Situation Report (SITREP) – figure B-2.
- Example Intelligence Report (INTREP) – figure B-3.
- Example Tactical Report (TACREP) – figure B-4.
- Intelligence Information Report (IIR) – figure B-5.
- Biographic Report – figure B-6.
- Example Knowledgeability Brief (KB) – figure B-7.

INTELLIGENCE SUMMARY

B-2. The INTSUM provides a summary of information and intelligence developments impacting operations and planning. It is used to summarize significant enemy activities, report analysis (not just information) of the current situation and to assess the probable enemy COAs in that AO. The INTSUM can be produced in written or graphic format and is normally transmitted to higher, lower, and lateral headquarters.



INTSUM FORMAT

LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(Unit Making Report)
LINE 3 – SITUATION _____	(General Enemy Situation Since Last Report)
LINE 4 – ENEMY FLOT _____	(Current Enemy Front Line Trace)
LINE 5 – ENEMY UNIT SIZE _____	(Enemy Ground Maneuver Units LOCATION/ACTIVITY/Status by Echelon/Size, Location) Strength (Grid), Activity)
LINE 6 – ENEMY ARTILLERY _____	(Enemy Artillery Activity and Estimated Strength)
LINE 7 – ENEMY CBRNE _____	(Enemy CBRNE Activity (Type, Location, DTG))
LINE 8 – ENEMY AIR _____	(Enemy Air and Air Activity)
LINE 9 – ENEMY ENGINEER _____	(Enemy Engineer Activity)
LINE 10 – FORCE PROTECTION AREA THREAT _____	(Enemy FP Area Threat (Light Forces, SF))
LINE 11 – ENEMY'S EST COA _____	(Enemy's Most Probable Courses of Action)
LINE 12 – PIR _____	(Current PIR in Order of Priority and the Phase of Operation)
LINE 13 – ENEMY SUSTAINMENT _____	(Location and Activity of Enemy Combat Sustainment Units) Combat Service Support Units)
LINE 14 – VULNERABILITIES _____	(Analysis of Enemy's Current or Emerging Vulnerabilities)
LINE 15 – WEATHER AND TERRAIN _____	(Analysis of Effects of Weather and Terrain)
LINE 16 – ENEMY COMBAT ASSESSMENT _____	(Summarize Enemy Combat Assessment During Period)
LINE 17 – NARRATIVE _____	(Free Text for Additional Information Required for Clarification of Report)
LINE 18 – AUTHENTICATION _____	(Report Authentication)

Figure B-1. Example INTSUM format

SITUATION REPORT (SITREP)

B-3. The situation report (SITREP) summarizes significant actions and challenges facing the commander. The SITREP keeps appropriate echelons informed of changes (or lack thereof) regarding key aspects since the last report. SITREPs vary by command, theater, whether the report is real-world or exercise, and similar factors. Typical aspects that may be included are current OPLANS, situations that affect operations, current status, unit readiness, operational challenges and recommended solutions, and similar elements.

B-4. The SITREP normally contains reference to the effective time period, map reference data, and may also include some or all of the following: enemy situation changes, friendly situation changes, administrative and logistical situations, general comments and recommendations, and the originating commander's personal evaluation of the situation. The SITREP describes critical operational, military, and political conditions that affect mission readiness and ability to fill the requirements of military plans. It does not duplicate other reports but summarizes important actions and references other reports for full details. The SITREP is submitted daily unless otherwise specified. Figure B-2 is a sample of a SITREP.

SITREP EXAMPLE

TO: CDR, USAMC, ALEX, VA // AMCOC-LG-R
CDR, LSE REAR REDSTONE, AL
INFO: CDR, LSE EUROPE, SECKENHIEM, GE
CDR, 3D ARMY
CDR, 345TH TAACOM
MGR, NATIONAL SUSTAINMENT MAINTENANCE
FROM: CDR, LSE NORTH, KUWAIT
(CLASSIFICATION) (ENTER SECURITY CLASSIFICATION IAW
OPER/FORCE DEPLOYMENT
MSGID/SITREP/ 2102014
REF//
INSTRUCTIONS)
AMPN/A. (CLASSIFICATION) DEPLOYMENT ORDER 96-1, HQ, USAMC
PERID/ 0900/0900//
HEADING/ENEMY//
ACTS OF SABOTAGE IN THE THEATER OVER THE LAST 24 HOURS RESULTED IN 18 ALLIED WIA (4 US ARMY, 0 USAMCI, ONE AIR ATTACK VICINITY ALLIED LOG BASE IN PORT RESULTED IN DESTRUCTION OF 26 CONTAINERS OF CLASS II, IV, AND IX AND EXTENSIVE AREA DAMAGE
TO 24ID VEH HOLDING AREA NEAR LSE HQ, EST UP TO 35 WHEELED VEH DESTROYED AND 15 TO 25 WITH MINOR DAMAGE, LAP REP ON SCENE WILL PROVIDE DETAILED REPORT TO LSE WITHIN NEXT 8 HOURS.
HEADING/OWN SITUATION//
AMPN/A. (CLASSIFICATION) INTELLIGENCE SITUATION: THEATER EXPECTS ENEMY AIR AND MISSILE THREAT TO SUSTAINMENT AREA TO ABATE BY END OF FEB. NO EVIDENCE OF CBRN THREAT THUS FAR.

Figure B-2. Example SITREP

B. (CLASSIFICATION) OPERATIONS: DEPLOYMENT OF LSE NOW AT 85% OF REQUIREMENT WITH CLOSURE EXPECTED AT D + 34. NEW FRA FROM CECOM OPERATIONAL EFFECTIVE 28 FEB AT (GRID COORD) 2 KM EAST OF THEATER DISTRIBUTION HUB. LAP PROGRAM CONTINUES TO RECEIVE COMPLIMENTS ON QUICK RESOLUTION TO CH 47D PROBLEMS. CLASS V IS OTHER MISSION AREA RECEIVING CONSIDERABLE ATTENTION FROM THEATER LOGISTICS COMMANDERS. FORECASTED DOUBLING OF THE AMMUNITION TONNAGE OVER NEXT 30 DAYS WILL IMPACT LSE QASAS STAFFING. WILL DISCUSS IN TODAY'S VIDEO CONFERENCE WITH IOC AND LSE REAR.

C. (CLASSIFICATION) COMMUNICATIONS/ELECTRONICS/ADP/INFORMATION MANAGEMENT: CONNECTIVITY TO ALL LSE DIV, FRA, LNO, AND LAP MEMBERS WITH THEIR UNITS IS GREEN. INMARSAT CAPABILITY NEEDS TO BE ON LINE UNTIL THEATER ALLOCATES ONE MORE SATCOM TO LSE ON 31 MAR. LOGISTICS ANCHOR DESK ON
LINE HAS HELPED WITH SIMULATIONS IN RETROGRADE PLANNING, WILL NEED TO HAVE MR. KEE WORK TWO NEW ALTERNATIVES RELATING TO RECONSTITUTION PHASE MAINTENANCE OF THE M911 TRUCK FLEET. SEE TODAY'S INFO REQUEST FOR SCENARIO.

D. (CLASSIFICATION) INSTALLATION STATUS: ALL USAMC ACTIVITIES NOW OPERATING FROM ACCEPTABLE FACILITIES. NO ISSUES IN EITHER LIFE OR BASE SUPPORT REMAIN OPEN. BULK OF BASE SUPPORT NOW FROM LOGCAP.

E. (CLASSIFICATION) TRANSPORTATION: AMC INTERNAL FLEET NOW AT 28 LIGHT CARGO TRUCKS, 6 MED CARGO TRUCKS, AND 25 VANS. THEATER TRANSPORTATION SYSTEM (PORTS, LOC, AND MODES) ARE GREEN DESPITE RECENT INCREASE IN ENEMY MISSILE AND AIRCRAFT ATTACKS. MOVEMENT OF LSE PERSONNEL IN SUSTAINMENT AREA NOT HAMPERED. LAP
PERSONNEL IN THE CORPS MUST MOVE ONLY DURING PERIODS OF LIMITED VISIBILITY USING SPECIAL VISION AND NAVIGATION ASSISTANCE DEVICES.

F. (CLASSIFICATION) MEDICAL: HAVE VERIFIED ALL MEMBERS OF THE LSE ARE AWARE OF THE LOCATION OF THEIR NEAREST MILITARY MEDICAL TREATMENT FACILITY. HIGH PRODUCTION BY THE WATER SUPPLY BN IN THEATER IN RESPONSE TO SURGE IN REFUGEES AND POWs NOT CAUSING UNEXPECTED EQUIPMENT FAILURES.

G. (CLASSIFICATION) MOBILIZATION (ARRIVALS/DEPLOYMENTS): NONE SINCE LAST REPORT.

HEADING/ADMIN AND LOG//

CASUALTY/(KIA -NONE)/(WIA -NONE) /(**MIA** -NONE) / **(NON COMBAT WOUNDED-** TWO IN THIS REPORTING PERIOD: JONES, WILLIAM, E, TMDE CO, ACCIDENT AT THE WORK SITE. BROKEN PELVIS. EVACUATED TO HN TREATMENT. SECOND INJURY WAS GS 12 MARSTON, SAM 0., ATCOM LAP REP WITH THE 12TH AVN BDE, TREATED FOR CUT TO . . . . . .

Figure B-2. Example SITREP (continued)

INTELLIGENCE REPORT

B-5. Intelligence Reports (INTREPs) are used to provide the exchange of information obtained through tactical collection efforts regarding events that could have an immediate and significant effect on current planning and operations of timely interest, such as the primary means of reporting HUMINT or CI information. Figure B-3 shows a sample INTREP.

INTELLIGENCE REPORT

LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(Unit Making Report)
LINE 3 – SIZE _____	(Enemy Strength/Size/Number)
LINE 4 – ACTIVITY _____	(Enemy Activity Description, Including Direction and Speed if Moving)
LINE 5 – LOCATION _____	(UTM or Six-Digit Grid Coordinate With MGRS Grid Zone Designator)
LINE 6 – UNIT _____	(Enemy Nationality, Unit Designator/Name/Type)
LINE 7 – TIME_____	(DTG of Activity)
LINE 8 – EQUIPMENT _____	(Major Enemy Equipment)
LINE 9 – SOURCES_____	(Reliability Rating of Source and Credibility Rating of Information)
LINE 10 – EVALUATION_____	(Evaluation of Source, Information, and combat assessment)
LINE 11 – CONCLUSION_____	(Reporter's Analysis of What Reported Information Means)
LINE 12 – NARRATIVE _____	(Free Text for Additional Information Required for Clarification of Report)
LINE 13 – AUTHENTICATION _____	(Report Authentication)

SAMPLE

Figure B-3. Example INTREP

TACTICAL REPORT

B-6. The TACREP is a report format primarily used to report tactical SIGINT information. The TACREP is used to quickly report vital intelligence information such as fleeting target, threat or danger to friendly units, distress situation, radio DF and other EW information, newly discovered enemy intentions, combat assessment data, and combat information. Figure B-4 shows a TACREP format.

TACTICAL REPORT (TACREP) MESSAGE FORMAT

Line 1, CLASSIFICATION
AAAAAAA
Line 2, TACREP/ORIGINATOR//
AAAAA/AAAAAA/BBBBBBB//
Line 3, EFFECTIVE TIME/AMOUNT/SOURCE/SUBJECT TYPE/
PRIMARY IDENTIFIER /UNIT IDENTIFICATION/LOCATION//
AAAAA/NNNNNNA/N/AA/AAA/BBBB/AA: BBBBBB//
Line 4, AMPLIFYING DATA//
AAAAA/CCCCCCCCCCCCCCCCCCCCCCCCC//
Line 5, RADIO FREQUENCY/BANDWIDTH/CALL SIGNS//
AAAAA/CCCCCCC/AAAAA//
Key:
A = Alphabetic character
C = ASCII (any typed) character
B = Alphanumeric character
N = Numeric character
* field may be repeated as necessary

Figure B-4. Example TACREP message format

INTELLIGENCE INFORMATION REPORT

B-7. The IIR is used to report all HUMINT information in response to collection requirements. It is used to expand upon information previously reported by a SALUTE report or to report information that is either too extensive or not critical enough for SALUTE reporting. IIRs are written at any echelon and "released" by the appropriate authority prior to entering the general Intelligence Community. Normally the BCT S-2X will be the release authority for IIRs.

B-8. The HUMINT collectors will fill out the complete IIR. However, the requirements section may link the information collected against a unit requirement rather than against national requirements. In any case, the report will be forwarded to the OMT. The team leader will review the IIR, place a copy of it in the detainee's or source's local file and forward the IIR to OMT. (When a detainee is transferred to another facility or evacuated to a higher echelon, a copy of each IIR written from interrogations of that detainee is forwarded with him or her.) The OMT reviews the report, requests additional information as necessary from the originator, adds additional administrative detail, and forwards the report to the HOC of the supporting S-2X. The HOC and the 2-X review the report, request additional information as required, add any final required information including linking it to national requirements, and then the 2-X releases the report.

B-9. Additionally, the IIR's text information can be forwarded to the unit's analytical elements and when it contains critical time-sensitive information, such as an impending attack, it is sent to units which may be affected by the information. However, it must be clearly marked "unevaluated information, not finally evaluated intelligence." See DIAM 58-12 for additional information. Figure B-5 shows a sample of an IIR.

INTELLIGENCE INFORMATION REPORT FORMAT

ADMINISTRATIVE DATA

CLASSIFICATION: Minimum classification for an IIR is CONFIDENTIAL. The minimum classification for an IIR when a human source is used is SECRET//NOFORN. The classification at the top of each report written by a student will read as follows:

TITLE: The title of the report, "INTELLIGENCE INFORMATION REPORT" will be centered on the first line. Leave one blank line between the classification and the title.

PRECEDENCE: Message precedence indicators in decreasing order are: flash (ZZ), immediate (OO), priority (PP), and routine (RR). Unless you are the releasing authority for IIRs, you will send all IIRs to the higher headquarters/releasing authority.

DATE/TIME GROUP: The date/time group is when the report is written. Use the following format: R DDTTTTZ MMM YY, where R=Precedence (for the purposes of this course), DD=Day, TTTT=24 hour time, Z= Zulu time zone, MMM= month, and YY= year. Zulu time is calculated from Mountain Standard Time (MST) by adding 7 hours during daylight savings and 6 hours for standard time.

Example: R 170318Z MAY 05

FM: This address is the lowest flag element in the report writing chain of command. Neither the HCT nor the report writer is listed. NOTE: There is no colon after "FM". The "FM" address will be indented 1/2 inch from the left margin.

Example: **FM** A COMPANY 165, CJTF-AP

TO: This address is the final recipient of the IIR. All final IIRs go to DIA Washington D.C. The "TO" address will be indented 1/2 inch from the left margin.

Example: **TO** DIA WASHINGTON DC

INFO: This entry represents the individual parties within the report writer's information chain that will receive a copy of the report. Note that if more than one entry is listed, they are written in column format under the first listing. For the purposes of this course, the chain of people who will receive this report include the following:

Figure B-5. IIR sample

USFORSCOM/NORFOLK VA, CDR CJTF-AP, and the OMT you are assigned to. The OMT will be the team's mentor's last name.

Example: **INFO** USFORSCOM/NORFOLK VA
CDR CJTF-AP
OMT (MENTOR'S LAST NAME)

CLASSIFICATION: Enter the classification and any handling caveats. There will be a space between each letter of the classification. There will be no spaces between the letters identifying a handling caveat.

Example: X X X X X X//XXXXXX

CITE: OPTIONAL (Delete if not used). When an IIR answers follow-up questions from an IIR evaluation, list the number from the "SERIAL:" prosign of the evaluation or consumer input to evaluation. This allows the consumer to track responses.

SERIAL: MANDATORY. Enter "IIR," the four-digit Collector Reporter Code (CRC), a four-digit serial number of the report, and a two-digit fiscal year. The IIR number is 17 spaces in length. NOTE: The four-digit CRC is written using the following format: X XXX. For a complete list of CRCs, consult DIAM 58-12 (S), Enclosure 7-6, Section A, Section B, and Section C. The four-digit serial number of the report, which is the number of reports written by the 205th MI Bde, is annotated by the four digits following the CRC. For classroom purposes your first IIR will be numbered 0001, followed by 0002, etc. The final two digits indicate the fiscal year in which the report was written.

Example: **SERIAL:** (U) IIR 2 362 0003 07

PASS: OPTIONAL (Delete if not used). If used, this prosign directs one or more of the recipients in the "TO:" field to pass on the report to the specified individual(s) or office(s) listed. Enter office symbols and personal names as necessary.

COUNTRY: MANDATORY. List the country(s) most significant to the IIR first. Minimize multiple entries. Enter the full name of the subject country followed by the two-letter country code in parentheses. The country name and two-letter code are a single data entry in this prosign field. List countries which the report mentions, not necessarily the country where the report originated. List only those countries that figure prominently in the report substance. Do not use water body codes without also listing a country first, except in a case such as an unattributed event at sea. Do not use "INTERNATIONAL" or "WORLDWIDE." This field, along with "IPSP:," determines the secondary dissemination of the IIR. Consult your Map Info appendix for all relevant country codes.

IPSP: MANDATORY. List Intelligence Functional Codes (IFC) in this prosign. IFCs replace the Intelligence Collection Codes (ICC) and Intelligence Priorities for Strategic Planning (IPSP) codes. Note the IFC consists of seven spaces - IFC followed by four digits. Separate each entry with a semi-colon.

Cite IPSP codes, followed by ICC codes. Up to 14 entries are allowable. You MUST have at least one IFC, even if your report is INITIATIVE. This field, along with "COUNTRY," determines the secondary dissemination of the IIR.

SUBJ: MANDATORY. Subject titles should be specific to the incident. The goal is to entice the reader to read the entire report, so provide a creative and interesting "SUBJ:" line. Non-descriptive titles such as "ECONOMIC INFO or "DEMOGRAPHIC DATA" are not acceptable. Do not include specific names or places in the "SUBJ:" line. Some automated message queuing systems display only one line of the title, so place key words up front. Enter the IIR number, a slash and a concise descriptive title, followed by the classification in parentheses. Unclassified titles are preferred. Entries will not exceed four lines. NOTE: The "SUBJ:" line does not end with a period. Place the unclassified portion marking (U) at the end of the line.

Example: **IIR 2 216 0004 06/NEPTUNE – A TERRORIST ORGANIZATION PLANS TO USE IMPROVISED EXPLOSIVE DEVICES TO DENY ACCESS ON A MAIN SUPPLY ROUTE (U)**

WARNING: MANDATORY. Enter the following: "WARNING: (U) THIS IS AN INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE. REPORT CLASSIFIED (C L A S S I F I C A T I O N)." The minimum classification for an IIR is CONFIDENTIAL. For the purposes of this course, classification is X X X X X X - XXXXXX.

Figure B-5. IIR sample (continued)

DEPARTMENTAL LOGO: MANDATORY. Not a prosign. Type the words "DEPARTMENT OF DEFENSE" centered on the page. Enter solid lines above and below, all the way across the page. There is a space between the lines and "DEPARTMENT OF DEFENSE." The DOD logo identifies the IIR as a product of the DOD HUMINT System. It distinguishes the report from similarly formatted reports issued by intelligence agencies of other departments.

Example: **DEPARTMENT OF DEFENSE**

DOI: MANDATORY. Enter date of information in YYMMDD format. Enter six numerals. No multiple entries, no "through" dates. If month or day is not available, use zeros as placeholders. The DOI is the specific date when the event(s) described took place or when the source made his or her most recent observation. The DOI is never later than the acquisition ("ACQ :") date. It is not the same as the "ACQ:" date unless the source was the report writer, or the source was interviewed on the same day that the reportable information happened.

Example: **DOI: (U) 071127**

REQS: MANDATORY. Cite the HUMINT Collection Requirement (HCR) and other tasking documents that pertain to the report. List HCRs first, followed by Time Sensitive Collection Requirements, Ad Hoc HUMINT Requirements, and Source Directed Requirements (SDR), in that order. DO NOT ENTER PIRs. Cite multiple references when they all apply strictly to report content. Twelve data entries are possible in the "REQS:" field. Use the entry "INITIATIVE" when reporting time-sensitive or target of opportunity information and no HCR is tasked.

SOURCE: MANDATORY. The source paragraph consists of two parts: the source identifier and the source description. It does not exceed five lines. Delineate numerical source identifiers with double slashes on each side.

SOURCE IDENTIFIER:

If the source is used only one time, a one-time source number will be used. "OTS" will be the first three letters of the source identifier, indicating that this is a one-time source. The next four digits indicate the CRC, followed by a three-digit number identifying the source, followed by the two digit fiscal year.

Example: **SOURCE: (X//XX) //OTS-2 362-001-07//**

The Source Code Identifier (SCI) is used for sources contacted more than once. List multiple source identifiers within a single pair of double slashes and separated from each other by semicolons. The SCI will be the four-digit CRC followed by an assigned four-digit source identifier. The OMT will assign the four-digit source identifier once a Basic Source Data Report has been submitted. Note that this line is generally classified **SECRET//NOFORN (S//NF)** if you have a human source.

Example: SOURCE: (X//XX) //2 362 HU37//

2. **SOURCE DESCRIPTION:** The Source Description outlines the background, access, and reliability of the source. It helps the analyst assess the reported information. The only time a source will be referenced is in the SOURCE line. This reference shall not reveal the identity of the source.

a. **Citizenship/nationality:** This information can be specific (e.g., U.S., CANADIAN, FRG, or BELGIAN) or, when necessary, more generic (e.g., THIRD WORLD, SOUTH AMERICAN, or WESTERN). A more generic description will be used when specific information will reveal the identity of the source. When the human source has more than one nationality, both nationalities will be annotated.

b. **Occupation/employment:** The occupation/employment line helps put source's access in context. "AN EGYPTIAN MILITARY OFFICER" or "A GERMAN BUSINESSMAN" are examples of good occupation descriptions. The statement, "PRESIDENT OF THE FIRM WHICH PRODUCES (a specific type of equipment)" is too specific. Phrases such as, source "IS IN A POSITION TO KNOW THE INFORMATION REPORTED" or "IS A TRAINED INTELLIGENCE COLLECTOR" are of little help to the analyst.

c. **Access to Information:** Statements such as, "PERSONALLY OBSERVED THE REPORTED EVENTS" or "INFORMATION BASED ON PERSONAL OBSERVATION AND EXPERIENCES" are appropriate. Recognized levels of source access are:

Figure B-5. IIR sample (continued)

EXCELLENT, ESTABLISHED, or DIRECT. Suggests high-level access to the information by virtue of source's involvement in the event described. Source may be the decision-maker in the action, or may have learned the information directly from the decision maker or a source document. Weigh the specificity of this statement against source protection concerns. Again, the source paragraph should not be specific enough to identify the source.

GOOD. Suggests credible but indirect access to the information. Perhaps the source obtained the information from a sub-source with excellent access or a sub-source with a proven reporting record.

INDIRECT. Indicates some distance between the source and the origin of the information. Source may have obtained the information from a sub-source of unknown access or of undetermined reliability, or via a convoluted chain of acquisition. Source may have overheard the information and thus could not put it into proper context.

d. **Reliability:** Statements such as "HAS REPORTED RELIABLY IN THE PAST" meet the minimum standard. An indication of how long source has reported in the past improves the statement. If the source has expertise in a certain area, include it in the source description. If the originator has comments regarding a source's honesty and forthrightness, the originator should include them in the "COMMENTS:" prosign. Once a source is recruited, the date of reliable reporting is the date of the first reportable information published from the source.

Examples:

SOURCE: (X//XX) //2 814 JA50// A RUSSIAN MILITARY OFFICER WHO HAD DIRECT ACCESS TO THE REPORTED INFORMATION. HAS REPORTED RELIABLE SINCE 25 OCTOBER 2005

SOURCE: (X//XX) //2 362 TI76// AN ATROPIAN BUSINESS OWNER WHO HAD INDIRECT ACCESS TO THE REPORTED INFORMATION. REPORTING RELIABILITY HAS NOT BEEN DETERMINED

SUMMARY: MANDATORY. Succinctly describe the most significant information in the IIR. Do not exceed five lines. Any information in the summary must also appear in the body of the text. A good summary is substantive and captures key highlights. Comments do not belong in the summary. Do not begin a summary with the phrase, "THIS IS AN IIR..." A summary NEVER contains a meaningless phrase such as, "THIS IS AN IIR WHICH FORWARDS THREAT CHARACTERISTIC INFORMATION ON ORGANIZATION, STRENGTH, EQUIPMENT AND MORALE." Do not put GEOCOORDS or grid coordinates in the summary line. Do not introduce acronyms in the summary line. Use the long form and introduce it in the text. Proper last names in the summary should be ((double parented)). Authorized military abbreviations may be used in the summary line in accordance with FM 6-99.2. If there are enclosures, the last word in the summary is ENCLOSURE or ENCLOSURES.

Example:

SUMMARY: (X) THE HIKACHDUT TERRORIST ORGANIZATION PLANNED TO ATTACK FRIENDLY FORCE PATROLS IN NORSHEN PROVINCE DURING THE WEEK OF ELECTIONS BY USE OF IMPROVISED EXPLOSIVE DEVICES AND AMBUSHES. ENCLOSURE

TEXT: MANDATORY. The text prosign contains the body of the IIR. Follow these guidelines and refer to the Alphabetical Style Guide:

a. Use the active voice. Active voice forces the originator to attribute the action to someone. Avoid using indefinite or indirect expressions (e.g., passive phrases such as: "it is believed," "it is reported," or such terms as: "reportedly," or "allegedly") in IIRs. Passive voice often leads to such expressions.

b. Divide text into individual paragraphs and subparagraphs marked with the appropriate classification. Generally, one paragraph will be written in the text for each PIR answered. Lengthy description may merit additional paragraphs.

c. In reports addressing multiple countries and subjects, link subject matter and country.

d. You may integrate source and field comments into the text for clarity. Place the comments immediately after the sentence to which they pertain, label them as source or field comments, and enclose them in parentheses.

Example:

TEXT: 1. (X) …PARTIES SIGNED THE AGREEMENT ON 6 JULY 1997. (SOURCE COMMENT - IT IS UNLIKELY THE GERMAN GOVERNMENT WILL HONOR THE CONDITIONS OF THE AGREEMENT BECAUSE....)

Figure B-5. IIR sample (continued)

e. Whenever precise geographic locations are an essential element in an IIR, place coordinates after the place name the first time the place is mentioned in the "TEXT:" or "COMMENTS:" Use Universal Transverse Mercator (UTM) Grid coordinates in addition to geographic coordinates when both are available. Refer to the Alphabetical Style Guide for the correct use of UTM and Geo Coordinates.

COMMENTS: MANDATORY. The entry "NONE" is not authorized. The comments field is free text. These generally fall into FIELD COMMENTS made by the collector, and comments made by others. Place the "type" of comments in parentheses to clarify who is talking. There is no particular order for types of comments; however, the re-contact information should come at the end. Comments include:

Three Mandatory Elements of FIELD COMMENTS:

(1) ONLY when the IIR answers an analyst's follow-up questions from an evaluation, enter: "THIS IIR RESPONDS TO FOLLOW-UP QUESTIONS CONTAINED IN (name of evaluating consumer agency) IIR EVALUATION (eval serial number)." When IIR does not respond to questions from an evaluation, do not include this phrase.

(2) Indicate source availability for re-contact. This cues consumers about the opportunity for additional exploitation of the source concerning the contents of the IIR. Example: "SOURCE IS AVAILABLE FOR RECONTACT." or "SOURCE IS AVAILABLE UNTIL 30 JUN 98."

(3) Provide point of contact office symbol and phone number of Unit Referent Reports Officer for questions concerning source re-contact for follow-up questions. Example: "ADDRESS ANY QUESTIONS CONCERNING THE CONTENTS OF THIS IIR TO (appropriate geographic office symbol) AT STU III (703) 907-XXXX, DSN 283-XXXX."

Optional Elements of Comments:

(1) SOURCE COMMENT: Observations the source made about the information he or she is reporting. The SOURCE COMMENT field is optional due to some sources of information are incapable of providing comment, i.e. newspapers, fliers, etc. When dealing with human sources, it is the responsibility of the source handler to acquire and annotate source comments.

(2) Additional FIELD COMMENTS: In addition to the mandatory entries above, field comments may include remarks reflecting the judgment and perceptions of the originator. These types of comments are very useful to the analyst. The opinion of an informed individual near the source of the information can be the key factor in evaluating the significance of a report. Field comments apply to (but are not restricted to) the following situations:

Reference previous IIRs from the same source or on the same topic.

Describe problems or special circumstances that affect the information reported.

Present an informal assessment or personal opinion on the possible meaning and/or potential impact of the reported information.

Provide supplementary information obtained from other U.S. agencies. Give credit to those agencies to avoid false confirmation. Do not reference another agency's report if it has a higher classification or more restricted distribution than your IIR.

Request evaluation of the IIR. Explain why, using the phrase, "REQUEST EVALUATION BECAUSE..."

Provide a field analysis of the reported information. Always explain the circumstances for first-time sightings and for new or potentially controversial information. Cite any reference material used to support your conclusions.

FIELD COMMENTS will include a paragraph that addresses the PIR answered by the information contained within the text of the IIR.

Example:

COMMENTS: (X) (FIELD COMMENTS) — SOURCE IS AVAILABLE FOR RECONTACT. POC FOR THIS IIR IN DH-4 IS GEORGE M. COHAN AT DSN XXX XXXX. ACCORDING TO THE DIA HANDBOOK ON RUSSIAN AIR FORCE DTD MAY 97, SQUADRON 541 OF THE TENTH FIGHTER WING LOCATED AT POVOGRAD AIR FORCE BASE IS NOT EQUIPPED WITH FRENCH-MADE MIRAGE 3000 FIGHTER BOMBERS, BUT RATHER RUSSIAN-MADE MIG-35P (FIREBLADE MOD 1) FIGHTERS. HANDBOOK INDICATES, HOWEVER, THAT THE FORMER ARE ASSIGNED TO SQUADRON 305 OF THE FIRST FIGHTER WING.

Figure B-5. IIR sample (continued)

COLL: OPTIONAL (Delete if not used). Collection Management Code (CMC). Cite appropriate two-letter codes from DIAM 58-12 (S), Enclosure 7-7. Use no more than six entries, but cite primary activity or subject first. DOD HUMINT collection elements use CMCs to link collection with certain activities or special topics (e.g. if DAO escorts a VIP aboard C-12, and spouse aids in collection, cite AA; AD; AS; NN.) The AA is the primary activity. When the IIR requires no CMC citation, do not use the prosign. DIA/DHM-1B is the proponent office; DIA/CL-2B is the database manager.

INSTR: MANDATORY. This block is for special instructions.

a. **REPORTING ON U.S. PERSONS:** Always the first entry after the "INSTR:" prosign. Enter "U.S. YES" or "U.S. NO." See guidance in DIAM 58-12 (S), Enclosure 7-8.

Example: **INSTR: (X) U.S. NO**

PREP: MANDATORY. Enter the seven-digit Field Reporter Number (FRN). The FRN replaces the use of the reporter's name in the IIR. It provides increased operational security for the reporter and for collection activities. Your FRN will be the first two letters of your last name and your class number.

Example: **PREP: (X) SM07303**

ENCL: OPTIONAL (Delete if not used). Enter the number of enclosures to follow. If the IIR has no enclosures, omit this prosign. On the next line identify the enclosures. Identify the type of enclosure (photographic, non-photographic, sketch, etc), a general description of what the enclosure is regarding, number of copies, date of creation of the enclosure, and the size of the enclosure (number of pages, length of video, size of computer file, etc.). If there is only one enclosure, list on one line after "TO FOLLOW."

In addition, the enclosure must be marked according to the following format: The classification must be marked on each page of the enclosure. List the report number and enclosure number on the first page of the enclosure. Number all pages and staple them to the IIR.

Example **- 2 Enclosures:**

ENCL: (X) TO FOLLOW — 2 ENCLOSURES.

1. SKETCH — ANTENNA FARM (X) 1 COPY, 060216, 1 PAGE (U)

2. MANUAL — SIGNALS OPERATING INSTRUCTIONS (X) 1 COPY, 840112, 135 PAGES (U)

Example - 1 Enclosure:

ENCL: (X) TO FOLLOW — SKETCH, ANTENNA FARM (X) 1 COPY, 060216, 1 PAGE (U)

ACQ: MANDATORY. Place and date of acquisition. Enter the location (e.g., town, country) where reporter acquired the information. Enter the date the reporter acquired the information in parentheses in (YYMMDD) format. The "ACQ:" date is always later than the "DOI:," unless the reporter is the source, or source is interviewed the same day as the action.

DISSEM: MANDATORY. The Dissemination line has two parts: "FIELD —" and "SENT TO —." After "FIELD —" enter all local recipients to whom the IIR is passed by the originating field element. Do not include electronic message info addressees. If the IIR was not disseminated in the field, enter "NONE." After "SENT TO —" enter "DIA/SVI-2" and specify which enclosures. For this course, DIA/SVI-2 is the recipient of all original enclosures. If the IIR has no enclosures, do not include "SENT TO —."

Example:

DISSEM: (X) FIELD – NONE. SENT TO – DIA/SVI-2 (W/ENCLS).

Example (No Enclosures):

DISSEM: (X) FIELD – NONE.

WARNING: MANDATORY. Enter the following: WARNING: REPORT CLASSIFIED (Insert proper classification.)

DRV FROM: MANDATORY. Enter the derivative classification authority. For DEFENSE HUMINT SERVICES this will normally be "DIA/DH-D MSG 291330Z JAN 96."

DECL: MANDATORY. Enter the appropriate declassification code; normally "X1."

Figure B-5. IIR sample (continued)

BIOGRAPHIC REPORT

B-10. The biographic report is a formatted IIR employed to report information collected from one human source about another individual of actual or potential intelligence interest.

KNOWLEDGEABILITY BRIEF

B-11. The KB is used to inform the Intelligence Community of a source's full identity, past history, and areas of knowledge as well as to set a suspense date for the submission of intelligence requirements. It is normally employed at operational and strategic echelons. **When completed, a KB will be classified at least Confidential in accordance with the DIA Classification Guide to protect the sources identity**. Figure B-6 is a short form KB that can be used for screening at all echelons and can also be prepared and published like the full KB. This allows the entire Intelligence Community to see who is either in custody or to whom US intelligence has access so that SDRs can be issued to help focus the intelligence collection effort. Theater-specific collection requirements may require modification of the KB-EZ format. Consider adding entries for ethnicity, language and dialect spoken, race, religion, and sect as well as tribal affiliation. Location entries may need to include a village or even neighborhood.

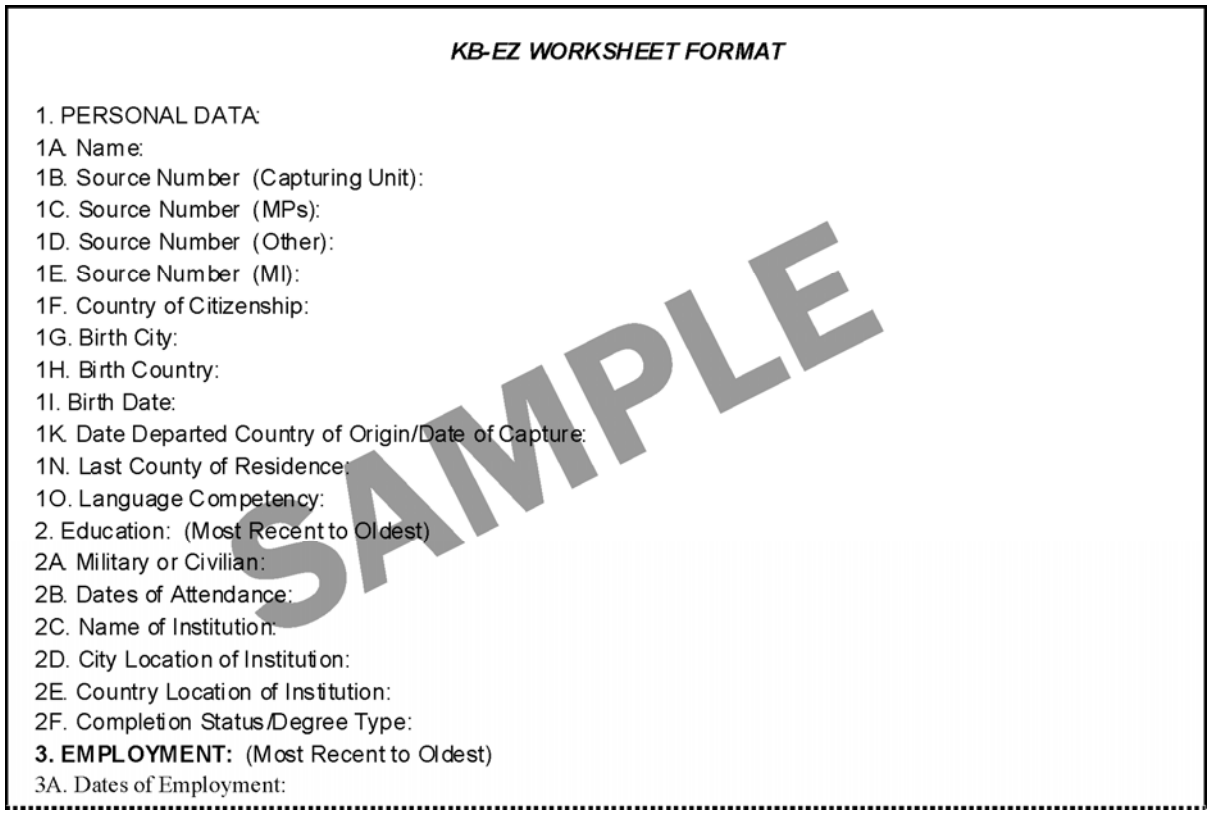


Figure B-6. KB sample

3B. Name of Place of Employment:
3C. City Location of Place of Employment:
3D. Country of Place of Employment:
3E. Employment Duty Position:
3F. Security Clearance:
4. MILITARY SERVICE: (Most Recent to Oldest)
4A. Dates of Service:
4B. Name of Base/Post:
4C. Armed Service Component:
4D. Rank of Equivalent:
4E. Name of Unit/Group:
4F. City Location of Unit/Group:
4G. Country Location of Unit/Group:
4H. Military/Group Duty Position/Title:
4I. Security Clearance:
5. Comments: (Character, intelligence, motivation, personality, cooperativeness)
5A. CIRCUMSTANCES OF CAPTURE: Capture date, capturing unit, circumstances, documents, weapons and equipment.
5B. ASSESSMENT: Physical condition, mental condition, intelligence, cooperation (1, 2, 3), knowledgeability (A, B, C), personality.
5C. ADDITIONAL PERSONAL INFORMATION: (Skills, experience, marital status, other).
6. NAME OF SCREENER:

Figure B-6. KB sample (continued)

Appendix C

Captured Enemy Documents, Media, and Equipment

C-1. One of the significant characteristics of operations is the proliferation of record keeping and communications by digital methods (faxes, e-mails, and typed or computer-generated documents). The rapid and accurate extraction of information from these captured enemy documents, media, and equipment contributes significantly to the commander's understanding the operational environment of his battlefield. Units may capture documents, media, and equipment on or in immediate association with EPWs and detainees. Units may collect documents, media, and equipment from refugees, line crossers, displaced civilians, and local civilians. Refugees, line crossers, displaced persons, and local civilians may turn in both private and public documents, media, and equipment to units. Units may find documents in abandoned enemy positions or anywhere in the AO.

C-2. A captured enemy document (CED) is any document or other media that was in the possession of an enemy force that subsequently comes into the hands of a friendly force regardless of the original of that document. Although documents may be seized by any DOD personnel, immediately forward the CED to the unit intelligence section, which will extract information of use to support current operations. CEDs can include—

- Maps.
- Propaganda materiel.
- Phone records.
- Photographs.
- Computer files.

C-3. Captured enemy equipment (CEE) includes all types of foreign and non-foreign materiel found on a detainee or on the battlefield that may have a military application or answer a collection requirement. CEE would include all electronic communication equipment with a memory card, including computers, telephones, Personal Digital Assistants, and Global Positioning System terminals, as well as all video or photographic equipment. Although materiel may be seized by any DOD personnel, immediately forward the CEE to the appropriate cell or unit for exploitation and analysis. CEE can include—

- Computers and ADP.
- Weapons.
- Property that may be of intelligence value.

C-4. Captured enemy materiel (CEM) includes any equipment, documents, media, and materiel captured on the battlefield, surrendered by locals, or obtained as a result of raids, cordon and search, or other operations. All CEM are recorded on part C of DD Form 2745 (Enemy Prisoner of War Capture Tag).

C-5. The exploitation of CEM, CED, or CEE, and other captured property is called DOMEX. DOMEX is the systematic extraction of information from all media in response to the commander's collection and operational requirements.

C-6. FM 34-54 and FM 2-22.3 provide detailed information on collecting and processing CEM.

COLLECT INFORMATION

C-7. Maneuver units and other non-military intelligence units may collect CEM during the detention or capture of detainees, EPWs, and facilities. The possession of these items by the detainee, EPW, or at an enemy facility may have intelligence value. For example, a tourist map of a city with marks and annotations on sensitive infrastructure may indicate possible targets if captured with a suspected terrorist or insurgent. Capturing units must therefore treat all documents, media, and equipment collected from people and facilities in the AO as CEM. This enables brigade and below units to execute standardized procedures for collecting, documenting, and evacuating CEM to their battalion intelligence staff or a designated CEM processing organization. The following are standard procedures for collecting information:

- Remove the CEM from person, vehicle, or facility.
- Do not mark, alter, or deface the CEM.
- Conduct hasty screening of CEM to identify time-sensitive information of immediate tactical value.
- Report time-sensitive information.
- Place CEM in waterproof container (box or plastic bag).
- Complete two copies of DD Form 2745 (Enemy Prisoner of War [EPW] Capture Tag), part C, or field expedient tag.
- Place one copy of the completed DD Form 2745, part C, inside the waterproof container.
- Attach one copy of the completed DD Form 2745, part C, to the outside of the container.
- Evacuate the CEM to battalion intelligence staff.

CEM —INDIVIDUALS AND SMALL SITES

C-8. Capturing units must remove all CEM, except one official identity document, from detainees and EPWs and safeguard these items from alteration or destruction. The unit must evacuate these items with but not on the person of the detainees and EPWs. Following interrogation, the intelligence staff, HUMINT team, or other qualified authority, determines which personal items to return to the detainees and EPWs. For further information, see article 17, part III, section I, Geneva Conventions.

C-9. If resources and time are available, the capturing unit should photograph the capture site as well as the CEM too large or dangerous to remove from the site. This material could include large equipment, graffiti on walls, ordnance, and other such items. A digital photograph also provides a graphic record of the relationship of objects at the site that supports HUMINT collection and analysis. The unit must annotate or otherwise include all the information from the capture tag with digital photographs to ensure CEM accountability and traceability.

C-10. The capturing unit completes part C of DD Form 2745 (Document/Special Equipment Weapons Tag) for each CEM. Completing the DD Form 2745 is an essential task that establishes accountability and traceability for all CEM. If the DD Form 2745 or field expedient forms are not available, the collection or exploitation team records the required data on any piece of paper. Figure D-1 shows an example of a capture tag from DD Form 2745. As a minimum, the unit should record the following information:

- Capturing unit identification.
- Date and time of capture in date-time group format.
- Location of capture including 8-digit map coordinates and a detailed physical description of the location.
- Identity of the detainee, enemy prisoner, or other human source that possessed the CEM, if applicable.
- Summary of the circumstances of capture.

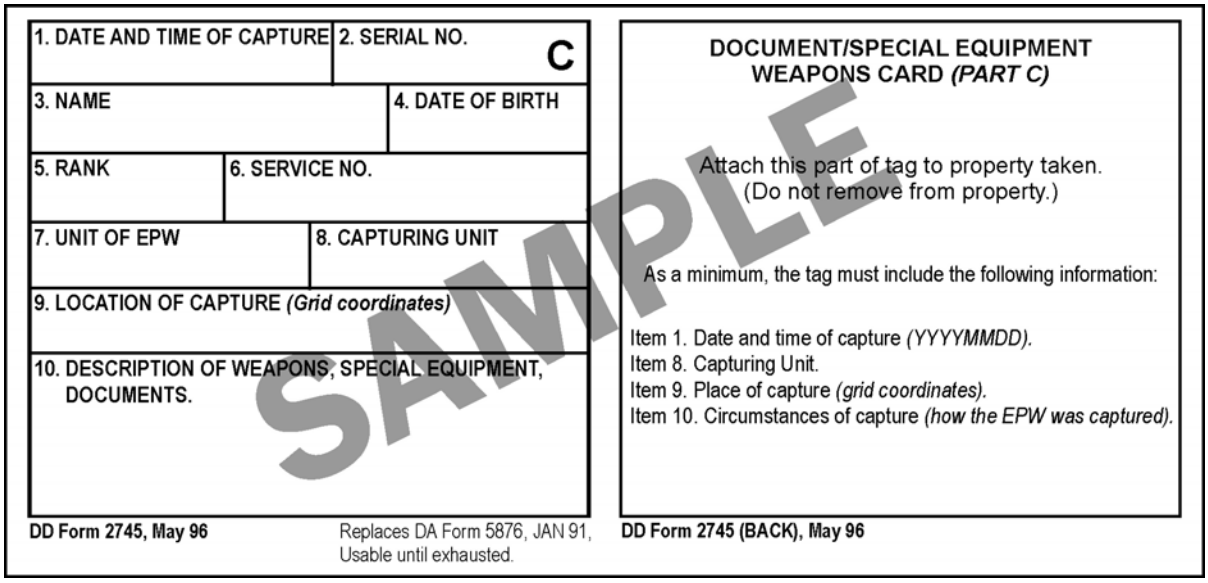


Figure C-1. Part C of DD Form 2745 (Document/Special Equipment Weapons Tag)

CEM—LARGER SITES

C-11. In situations involving large quantities of CEM, when the unit that captured or found the site has neither the resources nor the expertise to conduct the collection, the capturing unit should request a collection or site exploitation team from a supporting MI unit, the NGIC, or the Joint Document Exploitation Center (JDEC) to collect CEM. This reduces the burden on the requesting unit, facilitates the rapid extraction of information, and enables the priority evacuation of CEM of importance to higher echelons. This method requires the requesting unit to safeguard and protect the CEM until the arrival of the CEM collection or exploitation team. The capturing unit should submit a SALUTE or similar report and include a request for collection or exploitation support in the remarks line. The report should include the following:

- Location of CEM, including 8-digit map coordinates.
- Enemy situation in the vicinity of the capture site.
- Description of the capture site (such as city hall, munitions storage facility, or terrorist training camp).
- Estimate of the number and type of items.
- Presence of computers, file servers, copying machines, or similar communications and processing equipment.

C-12. The capturing unit then makes every effort to ensure that computers, magnetic media, telephones, recording devices, and communications equipment remain in the captured configuration (powered up or powered down) until relieved by specially trained collection or exploitation personnel. Personnel from the capturing unit remain in place to provide security while collection or exploitation personnel process the site.

C-13. The collection or exploitation team notifies the requesting unit of their estimated time of arrival and route as well as any other relevant protection requirements information. Upon arrival, the personnel from the capturing unit remain in place to prevent the recapture, loss, or destruction of the CEM while the collection or exploitation team processes the site. The collection or exploitation team collects, tags, inventories, and evacuates the CEM in accordance with SOPs and instructions in annex B of the OPORD. Depending upon the enemy situation and time available, the team screens the CEM prior to evacuation to ensure the identification and reporting of time-sensitive information.

DEBRIEF CED COLLECTOR

C-14. Since every Soldier is a Sensor and is a potential source of information, the battalion intelligence staff debriefing is one way that information collected by these Soldiers gets into the intelligence system. The battalion intelligence staff is responsible for debriefing returning patrols, tactical site exploitation teams, DOMEX teams, leaders who may have traveled to meetings, returning HCTs helicopter pilots, and others who may have obtained information of intelligence value. The battalion intelligence staff debriefs personnel, writes and submits reports, or reports information verbally, as appropriate. The requirement for a debriefing by the intelligence staff following each mission should be a part of the mission pre-brief. Leaders should not consider the mission complete and the personnel released until the reporting and debriefings are completed,

C-15. Once the capturing unit or exploitation team completes its mission, it gathers all collected CEM and reports to the battalion or brigade intelligence staff for debriefing and handover of collected materials. Where assets are available, other specially trained or debriefing-qualified personnel (such as HCTs, CI teams, or DOMEX teams) may conduct the debriefing of DEM collectors. The intelligence staff debriefing should follow along the lines of the capturing unit or exploitation mission briefing; for example, review the route traveled, collection objectives of the mission, methods employed. By the time the intelligence staff conducts it debriefing, it should be in receipt of the patrol report and all documents produced as a result of handling the CEM to include the mission logs, sworn statements, SALUTE reports, sketches, photographs and video. Having the collector's reporting will streamline the debriefing process, allowing the intelligence staff to concentrate on filling in gaps and following up on reported information. Photographs or video may also be used during the debriefing to ascertain the condition of the site, location, and condition of CEM.

REPORT INFORMATION

C-16. Upon receipt, the battalion intelligence staff evaluates the CEM, assigns a preliminary CEM category, and reports time-sensitive information. Table C-1 provides a list of CEM categories, basic descriptions, general classification, and common examples. At large CEM sites, collection or exploitation teams screen CEM as they tag and inventory the CEM. Upon recognition, the intelligence staff reports time-sensitive information in accordance with reporting guidance including, if authorized, direct reporting to affected units. The SALUTE report is the standard format used in most units for reporting time-sensitive information unless otherwise specified in annex B of the OPORD or other reporting guidance in specific orders and requests. The battalion intelligence staff also forwards a hardcopy of the reports with evacuated items to reduce the potential for the redundant reporting.

Table C-1. CEM categories

Category	*Description*	*General Report Classification*	*Examples*
A	Critical, time-sensitive information that requires priority reporting, evacuation, and/or special handling	SECRET	Marked Maps and Overlays Navy and Air Force Information Technical Documents War Crimes Evidence
B	Exceptional information that answers a higher echelon PIR	SECRET	Cryptographic Information Field Manuals Maintenance Records Personnel Rosters Unmarked Maps and Charts
C	Routine information that may have general Intelligence value or requires accountability	UNCLASSIFIED	Currency Narcotics Works of Art
D	Routine Information that has no Information of Intelligence Value	UNCLASSIFIED	Only a JDEC or higher processing center assigns this category
Note. **Use DA Form 4137 (Evidence/Property Custody Document) for accountability of criminal evidence, currency, and other potential high value property items such as works of art.**			

C-17. If resources and time are available, the battalion intelligence staff scans or photographs the items to create a digital record that can accompany the report or be sent directly to the processing site for processing. Digitization also enables the staff to use machine translation tools to identify important words, names, and phrases through a rough translation of the document. The staff must annotate or otherwise include all the information from the DD Form 2745 with digitized CEM to ensure accountability and traceability.

INVENTORY CEM

C-18. The battalion intelligence staff inventories all incoming CEM to ensure accountability during CEM evacuation. At large sites, a collection or exploitation team inventories the CEM. All CEM must have completed capture tags. The battalion intelligence staff must contact the capturing unit and complete the capture tag before evacuating the CEM to the processing site.

C-19. The staff uses the information on the capture tag to complete the document transmittal sheet. The staff must identify which CEM it is sending to a higher echelon or special processing site, such as DOMEX, TECHINT, criminal intelligence, or SIGINT facilities, and which are accompanying detainees . Noting attempts to process and report information from CEM on the transmittal documents prevents unnecessary duplication of effort by higher echelons. Figure C-2 provides an example of a transmittal form for CEM. The format for a materiel transmittal is in accordance with unit SOPs and reporting guidance, but it should contain at least the following information:

- Collecting or capturing unit identification.
- Capture date, time, and location.
- List of CEM by serial number.
- Forwarding unit identification.
- Destination unit identification.

- Screening category.
- Remarks including serial number and DTG of reports based on the CEM.

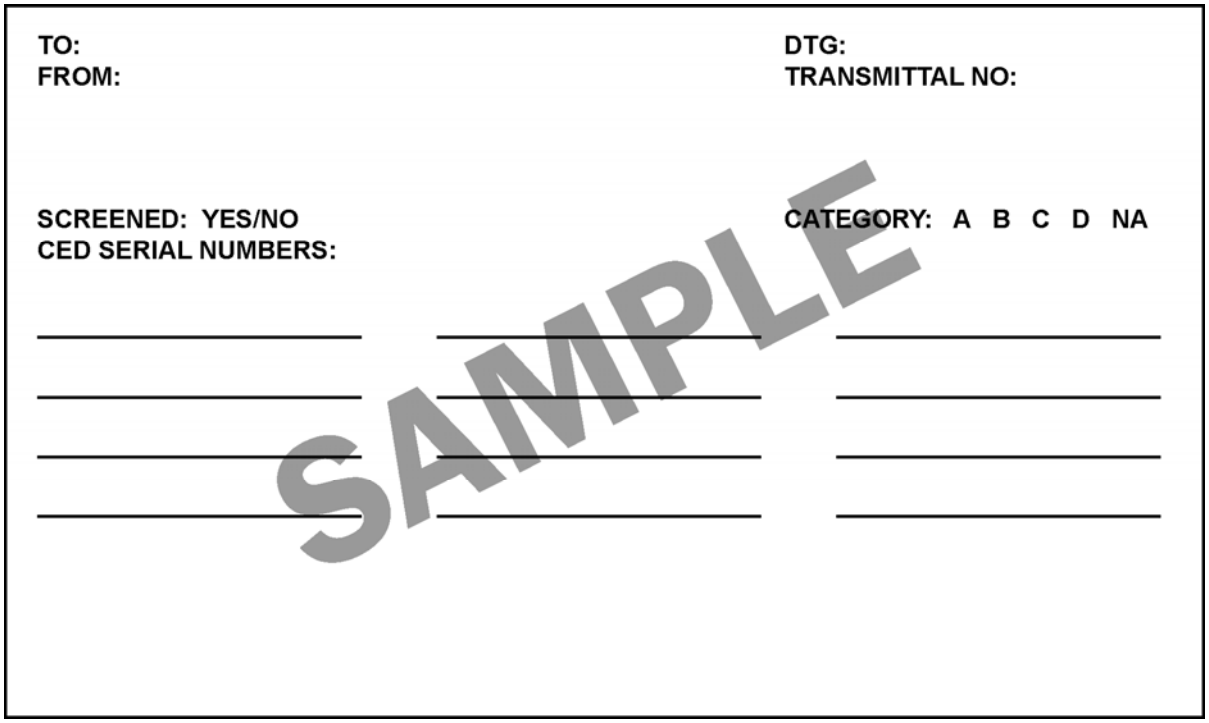


Figure C-2. Example transmittal format

C-20. Once completed, the battalion intelligence staff sends a softcopy of the transmittal sheet and an estimated evacuation time via SIPRNET to the processing site. Additional message addressees may include HUMINT, SIGINT, and TECHINT units if the CEM were captured in association with a detainee or EPW; contain cryptographic information; or technical information associated with captured equipment. Sending a softcopy of the transmittal form assists the message addressees to anticipate and organize their CEM processing resources as well as to alert multiple organizations to information of potential intelligence value.

EVACUATE CEM

C-21. The battalion intelligence staff sends CEM through intelligence channels to the supporting brigade-level processing site. Information gained from CEM is frequently time sensitive. If an item is not sent to the element most capable of exploiting it, time will be lost. Any time lost in processing and analyzing the CEM may reduce or even negate the value of the information. The CEM evacuation procedures in use at any element must ensure that items reach their proper destinations in a timely manner.

C-22. Once inventoried, the battalion intelligence staff evacuates the CEM with a hardcopy of the transmittal sheet in accordance with the CEM category, unit SOPs, and reporting instructions. As shown in figure C-3, the staff evacuates CEM to different elements based upon the information contained and the type of CEM concerned.

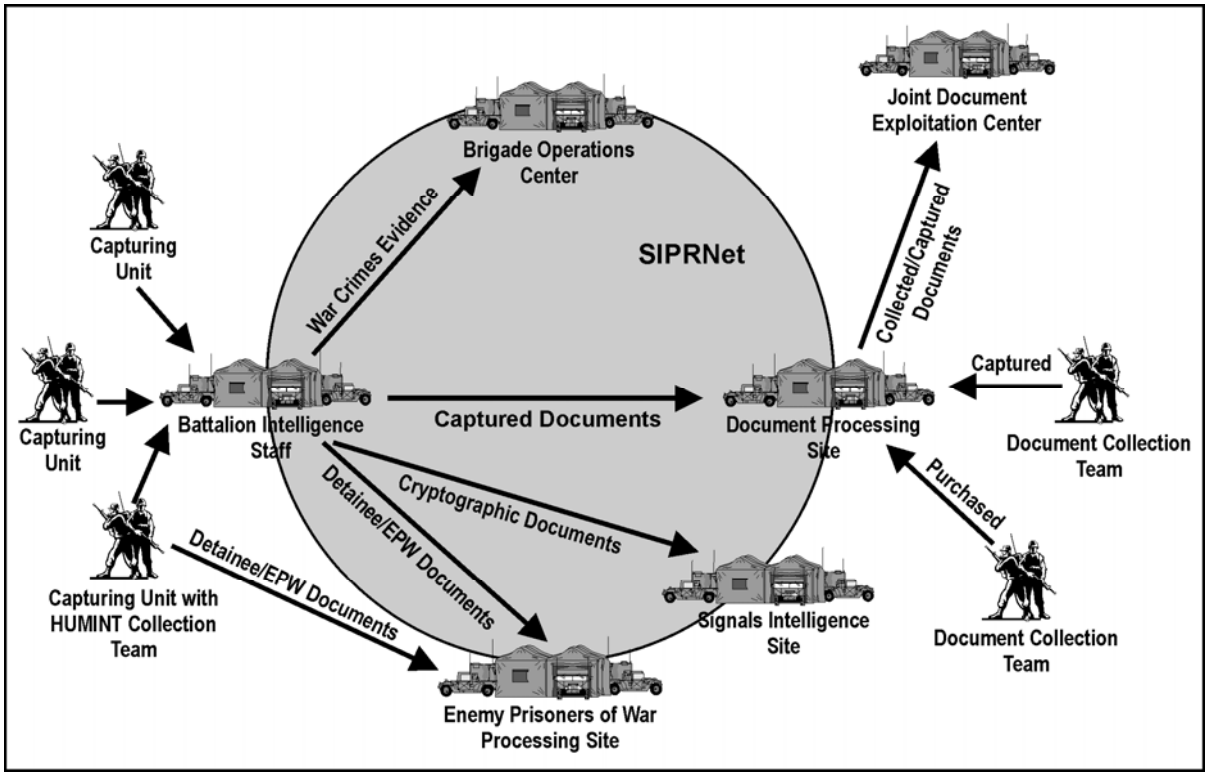


Figure C-3. Evacuating CEM

C-23. If the staff is unable to evacuate the CEM to the different locations, then the staff sends all items to the brigade-level processing site. The following describes the primary destinations of CEM.

- **Criminal Evidence.** The battalion intelligence staff separates and secures all CEM constituting evidence for use in legal proceedings against persons suspected of significant crimes such as crimes against humanity and war crimes to the staff judge advocate (SJA). The staff separates these items from other CEM; and marks them as "Criminal Evidence; and stores them under guard or in a secure area until turned over to the nearest criminal intelligence asset or a war crimes investigative unit. The unit should contact the SJA for additional guidance on chain of custody requirements.
- **Document Processing.** The battalion intelligence staff sends most CEDs to a brigade-level document processing site for screening, processing, and dissemination. The processing site serves as a clearing house as well as document processing center. In addition to evacuation, the site uses SIPRNET to send a digital version of documents to databases such as the National Harmony Database, where the documents are available to multiples users for further processing and analysis.
- **Human Intelligence.** Documents removed from detainees and EPWs must accompany the individual to holding and interrogation sites. This is an essential task since the CEM are necessary for effective HUMINT collection operations. The unit transporting the individuals and the CEM must also keep the CEM separate from detainees to ensure these individuals do not alter or destroy the documents.
- **Signals Intelligence.** The battalion intelligence staff sends CED containing cryptographic or communications systems information to the unit's supporting SIGINT unit or other SIGINT unit specified in annex B (Intelligence) of the OPORD. CED containing cryptographic or communications systems information are Category A and classified SECRET. These Category A CEM may contain time-sensitive operational and technical information requiring immediate

processing and analysis by SIGINT personnel. These documents are classified SECRET; the staff must limit the number of personnel having knowledge of the documents' capture or contents.

- **Technical Intelligence.** Items of TECHINT interest include equipment identified on the collection requirements list, annex B of the OPORD, as well as new weapons, vehicles, and equipment manuals. Equipment that remains unidentified, appears modified, or is otherwise out of the ordinary or unexpected, should cause a SALUTE report to be generated and sent back through reporting channels for disposition instructions. Equipment of TECHINT interest is typically transported to the nearest Combined Materiel Exploitation Center (CMEC) for processing and exploitation. If the tactical situation does not permit the equipment to be evacuated, the associated documents will be forwarded to the CMEC along with a description of the equipment.

C-24. When transportation assets are limited, the battalion intelligence staff evacuates CEM according to priority. The priority for transportation is determined by the category assigned to the CEM during screening. The staff evacuates all Category A CEM first, followed in order by Categories B and C. The unit evacuates unevaluated CEM as Category C, but ensures the transmittal slip indicates clearly that the CEM are "unscreened" or "not evaluated."

C-25. The staff holds lower priority CEM that it cannot evacuate immediately until scheduled transportation arrives. The staff combines these remaining items with any other CEM of the same category. When determining evacuation priorities, the staff considers all CEM that are ready for evacuation. The staff never evacuates lower priority items, no matter how old, ahead of those with higher priority. A package of CEM contains CEM of only one category. All unscreened CEM are handled as Category C material, but they are not packaged with screened Category C items. Material in a single package must have the same destination.

PROCESS INFORMATION FROM CEE

C-26. At the BCT, CEE will be collected; however, it will be processed by the CMEC. For further information on CEE processing, see FM 34-54 or AJP-2-5(A). The remainder of this appendix will discuss processing CED.

PROCESS INFORMATION FROM DOCUMENTS AND MEDIA

C-27. Unless the capturing unit has a supporting DOMEX team, translator, or linguist, most units that collect documents normally have no way of determining the intelligence value of CED. Once CED arrive at an echelon with a dedicated exploitation team, DOMEX team, or a CED processing site or other intelligence activity, MI personnel can screen, process, and extract information from the CED. The degree that the brigade-level and higher echelon sites process the CED depends on the site's resources, its mission, and the category of the CED.

C-28. The majority of material processing time involves digitizing, transcribing, and translating non-English graphics, recordings, and text documents into English text format. Language capability is therefore essential to processing non-English language items. In addition, language-based processing activities require procedures and management to ensure transcripts and translations are timely, accurate, complete, and free of bias. Generally, the priorities for processing are based on the category assigned, commander's collection requirements, established reporting guidance, and the commander's situational understanding.

C-29. Not all Army processing sites possess capabilities for voice recognition and identification; comparative analysis of video content; and cryptanalysis. The skills, knowledge, and equipment for specialized processing are available at Intelligence Community organizations through the communications architecture.

C-30. Units can request DIA, NGA, National Security Agency (NSA), National Media Exploitation Center, JDEC, NGIC, and other Intelligence Community organizations to use specialized techniques and

procedures to extract additional information from the collected audio and video information. Application of specialized processing techniques and procedures may require the classification of the processed information and restrict its dissemination.

C-31. CED processing includes the recovery of damaged documents, the decryption of encrypted documents, the translation of documents into English, and the extraction of documents from electronic media such as the extraction or downloading of files from a computer disc or hard drive. This need for document recovery, translation, and other specialized processing frequently limits the amount of processing that occurs outside processing sites such as JDEC or a combined media processing center.

LOG DOCUMENTS

C-32. The processing sites inventory incoming CEDs, media, and/or equipment and add them to the site's CED log. DA Form 4137 (Evidence/Property Custody Document) is the preferred document for managing the captured material chain of custody as it is widely recognized and encompasses an entire batch of CEDs. The inventory is an essential task; all units involved in collecting, transporting, and processing CEDs must maintain accurate records and accountability of all CEDs. The inventory consists of comparing the CED to the capture tag and accompanying transmittal documents. This comparison identifies—

- Transmittals that list missing CEDs.
- Capture tags not attached to CEDs.
- CEDs not attached to capture tags.
- CEDs not listed on the accompanying transmittal documents.

C-33. The processing site initiates trace actions on all missing CEDs, missing capture tags, and all information missing from the capture tags. The site can complete this corrective action swiftly if the capturing unit completed the capture tags correctly and retained its document transmittal forms, INTREPs, and digital images. If necessary, the trace action continues to the capturing unit and other elements that handled the CEDs if a capture tag is unavailable from elements that have previously handled or transported the CEDs. If the missing information and CEDs are unrecoverable, then the processing site completes the capture tag using available information and annotates the lost CED in the log.

C-34. When a batch of CEDs is received without a transmittal, the receiving element contacts the forwarding unit and obtains a list of CED serial numbers, if available. The receiving element records all trace actions in its journal.

C-35. The CED processing site uses the DD Form 2745, document transmittal form, and results of the inventory to create and maintain a log of all CEDs. The log is a record of what the unit knows about the CEDs. In addition to information about the CED, the log also records all actions taken with the CED at the site including INTREPs, translations, reproductions, and final disposition. The format for a document log is in accordance with unit SOPs, but it should contain at least the following information:

- File number (a sequential number to identify the order of entry).
- Date and time of receipt of the CED.
- Identification of individual that received the CED.
- CED serial number of the capture tag.
- Identification number of the transmittal document accompanying the CED.
- Complete designation of the unit that forwarded the capture tag.
- Date, time, and location of capture (as listed on the capture tag).
- Identification of the capturing unit (as listed on the capture tag).
- Description of the CED. (At a minimum, the description includes the original language; number of pages; type of CED, such as a map, computer disk, letter, or photograph; and the enemy's identification number for the CED if available.)
- CED category (after screening).

- Remarks including action taken based on the CED and any other information that can assist the unit in identifying the CED.
- Destination and identification number of the outgoing transmittal.
- Remarks to include any other information that can assist the unit in identifying the CEDs, media, and/or equipment including processing codes. These processing codes are set up by local SOPs to denote all actions taken with the CED while at the element, including INTREPs, translations, reproductions, or return of the CED to the detainee/EPW from whom it was taken.

SCREEN CEDS

C-36. During screening, the processing site conducts a systematic evaluation of the CEDs and the capture tags to identify reportable information and determine the priority of processing. This screening may change the preliminary category that was assigned during the initial evaluation of the CEDs. Also, the processing site reports any unreported time-sensitive information in a SALUTE report or IIR.

C-37. The processing site can screen CEDs using a qualified US linguist or a machine language translation tool with key word identification capability. CED screening does not require a full translation but does require sufficient translation to determine the significance of the CED. A non-linguist may be able to do a degree of preliminary screening based on the CED format and circumstances of capture.

C-38. As personnel screen each CED, they assign or reassign one of the four categories listed in table C-1. The category determines the priority for processing, reporting, and dissemination. CED screening requires that the processing site remain abreast of the current PIR and other collection requirements; current friendly and enemy situation; relevant threat characteristic information, and planned operations. Screening requires senior, experienced individuals, well versed in the target language and the collection requirements, capable of identifying time-sensitive information of national intelligence significance, and capable of making rapid decisions based on minimal information.

C-39. During screening, CEDs are first grouped according to their assigned screening category. Personnel must be careful when sorting CEDs to ensure no CED is separated from its associated documents. These large groupings can be broken down into smaller groups or batches. Each of these smaller groupings may consist of CEDs that were—

- Captured by the same unit.
- Captured in the same place.
- Captured on the same day at the same time.
- Received at the DOMEX element at the same time.

RECOVER CEDS

C-40. Recovering CEDs includes cleaning soiled documents, reassembling document fragments, decrypting coded documents, and extracting information from electronic devices or storage media. Extracting information from electronic devices and storage media is done by specially trained media exploitation personnel on a DOMEX team or media technicians at a JDEC or other site with specialized training, equipment, and software. Processing personnel at the JDEC work with TECHINT personnel to process electronic devices or storage media. In addition to special resources, processing at a fixed processing site prevents the introduction of corrupt software, malicious software, and other forms of computer attack from entering US communications and processing networks.

DIGITIZE CEDS

C-41. The processing site scans or photographs the CEDs to create a digital record that the site can use for processing and analysis. Digitization also enables the site to use machine translation tools to screen CEDs for important words, names, and phrases through a rough translation of the CED. The site must annotate or otherwise include all the information from the capture tag with digitized CED to ensure accountability and traceability. Finally, digitization enables the dissemination of the CEDs to the National Harmony Database

where other personnel such as those in the Army Reach Language Support Program or at the Army Reserve Intelligence Support Center (ARISC) can transcribe and translate the CED.

TRANSCRIBE INFORMATION

C-42. The processing site transcribes audio and video recordings into text format. For processing of non-English recordings, transcription is extremely important when the English language skills of the linguist are inadequate for authoritative, direct translation into English. A transcript is a verbatim, native language rendering of the information in the audio or video recording. The transcriber uses native font or transliteration to represent the spoken language in the recording. The transcript, particularly of video files, includes descriptions of the activity, setting, and conditions that the transcriber hears in the audio and observes in the video. Once completed, language-qualified analysts use the transcript to produce intelligence and update technical information. If required, the processing site translates the transcript into English for non-language qualified analysts and other users.

C-43. During transcription, a linguist provides an extract or a full translation of the original audio or video recording. The linguist provides an extract of the recording when time and resources are insufficient for a full transcript or the content does not meet reporting criteria. A full transcript requires the linguist to render all information in the recording into a standard transcription report format

TRANSLATE INFORMATION

C-44. The processing site translates CEDs and transcripts into English-language text format. Translation requires linguists who are qualified in both the target language and English. In addition, the linguists must have language proficiency and target knowledge commensurate with the target population of the information. These skills and knowledge are important because a translation, unlike a transcript, is normally not a simple word-for-word interpretation but an approximation of the literal and implied meaning of the spoken or written language. To ensure consistency and quality, the processing site applies a standard process to translate spoken and written information into English.

C-45. During translation, a linguist provides an extract, summary, or a full translation of the original CED or transcript. The linguist provides an extract or summary of the CED or transcript when time and resources are insufficient for a full translation or the content does not meet reporting criteria. A full translation requires the linguist to translate all information in the CED or transcript into a standard translation report format. The linguist uses online dictionaries, gazetteers, and working aids to improve the translation.

REVIEW INFORMATION

C-46. Technically proficient linguists review each transcription and translation to ensure consistency with reporting standards and quality of the translation. With some exceptions, a US Government linguist should review all information that a non-US linguist processes. Exceptions include operations involving long-term allies of the US and US contractors with the requisite skills and the command's confidence. Each transcript and translation undergoes two levels of review:

- **Quality Control.** For quality control purposes, a qualified linguist ensures that the transcript or translation report is accurate and that it clearly expresses the meaning of the original CED. The quality control linguist reviews the report to ensure that it is accurate, complete, free of bias, and in accordance with reporting standards. The linguist returns the report for correction or, personally, adds missed content, corrects minor translation errors, and fixes minor format errors. Upon completion of quality control, the translation is available for analysis.
- **Quality Assurance.** For quality assurance, a qualified individual reviews the report to ensure that it contains all required information and that the translation reads naturally in English. Once reviewed, the quality assurance linguist saves the completed transcript or translation report to the local database and notifies the control team. If authorized, a quality assurance linguist disseminates the report to external databases such as the World Basic Information Library or the National Harmony Database, linking it to the original CED.

PRODUCE INTELLIGENCE

C-47. As part of a multidiscipline intelligence effort, the use and integration of intelligence derived from CEDs ensures decision makers have the benefit of all sources of available information. Intelligence personnel use processed DOMEX-derived information to support situational awareness strategic responsiveness, and ISR. DOMEX-derived information may provide information on threat capabilities, limitations, and intentions that are crucial for our ability to plan, prepare for, and execute military operations. During tactical operations, tactical DOMEX-derived information may provide time-sensitive information of immediate tactical value to facilitate follow-on tactical operations.

C-48. Intelligence personnel apply intelligence analysis techniques and procedures to extract, understand, and report information of intelligence value from collected and processed information. An initial or hasty analysis occurs at or near the point of collection and processing. This initial analysis focuses primarily on identifying facts, evaluating the source's reliability, and evaluating the information's accuracy from a single source. Subsequent analysis and intelligence production uses information from multiple information sources. At each point in the transformation of information into intelligence, analysts at each echelon assess, extract, analyze, and report information and intelligence to their supported command in response to known or anticipated intelligence requirements. Although useful and important by themselves, transcripts and translations are processed information, not intelligence.

C-49. Producing intelligence requires analysts to—

- Identify information meeting the reporting criteria—information which answers the PIR, CCIR, or SIR, or otherwise poses an immediate threat to US or multinational forces.
- Evaluate information source reliability and evaluate information content accuracy.
- Analyze information and utilize analytical tools.
- Assess reporting.
- Update databases.

C-50. Analysts within the exploitation team or processing site identify information from the processed information meeting the reporting criteria. Analysts must be able to readily identify indicators of activity or identify the significance of minute pieces of information that could contribute to answering requirements. The analysis of the processed information varies based on the team's mission, capabilities, and time available. As a minimum, the team identifies and reports the basic facts (who, what, when, where, why, and how) from the information based on IRs. If the analysts have the time, target knowledge, and situational awareness then the analysts use analysis techniques and procedures to reach conclusions about the meaning of the information. The analyst can solve problems through two types of reasoning: deductive and inductive.

EVALUATE SOURCE RELIABILITY

C-51. The analysts evaluate the reliability of the information source based on previous reporting as well as exploitation team and processing site comments. As shown in table C-2, reliability ratings range from A (Reliable) to F (Cannot be Judged). If the source has not provided CEDs in the past, then the team rates the source as F (Cannot be Judged). An F rating does not necessarily mean the source is unreliable but that the team has no previous experience with the source upon which to base a determination. For CEDs discovered on the battlefield or in the possession of a detainee or EPW, the type and origin of the CED may carry more weight in determining reliability than the source of the CED itself. A hand-written note with apparent contact information may be judged as fairly reliable when considered with other factors such as the circumstances of capture, location, or condition of the CED.

C-52. Since a CED is usually something that the enemy has written for personal use, CEDs are usually truthful and accurate. There are cases in which falsified documents have been permitted to fall into enemy hands as a means of deception, but these cases are not the norm. Normal policy of not relying on single-source information should help prevent deceptions of this type from being effective. Documents also do not forget or misinterpret information although it must be remembered that their authors may have. Usually,

each document provides a portion of a larger body of information. Each CED, much like a single piece of a puzzle, contributes to the whole. In addition to tactical intelligence, technical data and political indicators that are important to strategic and national level agencies can sometimes be extracted from CEDs, while not affected by memory loss, are often time sensitive; therefore, they are to be quickly screened for possible exploitation.

Table C-2. Source reliability

Code	*Rating*	*Description*
A	Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability; usually demonstrates adherence to known professional standards and verification processes
B	Usually Reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time; may not have a history of adherence to professionally accepted standards but generally identifies what is known about sources feeding any broadcast
C	Fairly Reliable	Doubt of authenticity, trustworthiness, or competency but has provided valid information in the past
D	Not Usually Reliable	Significant doubt about authenticity, trustworthiness, or competency but has provided valid information in the past
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information
F	Cannot Be Judged	No basis exists for evaluating the reliability of the source

EVALUATE INFORMATION ACCURACY

C-53. The exploitation team or processing site also includes in the report an evaluation of the accuracy of the information based on previous reporting from that source and information from other sources. Accuracy ratings range from 1 (Confirmed) to 8 (Cannot be Judged) as shown in table C-3. If the information is new, the site rates the content as an 8 (Cannot be Judged). An 8 rating does not necessarily mean the document is inaccurate but that the team has no means of verifying the information.

Table C-3. Information accuracy

Code	*Rating*	*Description*
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject
2	Probably True	Not confirmed; logical in itself; consistent with other information on the subject
3	Possibly True	Not confirmed; reasonably logical in itself; agrees with some other information on the subject
4	Doubtfully True	Not confirmed; possible but not logical; no other information on the subject
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject
6	Misinformation	Unintentionally false; not logical in itself; contradicted by other information on the subject; confirmed by other independent sources
7	Deception	Deliberately false; contradicted by other information on the subject; confirmed by other independent sources
8	Cannot Be Judged	No basis exists for evaluating the validity of the information

REPORT INFORMATION

C-54. Information collected from CEDs is normally reported in accordance with unit SOPs and reporting guidance. Reporting involves placing extracted information into a coherent, properly formatted report so that the all-source analyst can add it to the intelligence picture. Report formats include standardized reports such as the SALUTE report and specialized INTREPs such as the TACREP or the IIR. DOMEX teams and intelligence staffs disseminate analytical summaries to the tactical level in the form of DOMEX or Batch Reports giving consumers the ability to access the original document in the National Harmony Database with its linked translation reports as well. Army SIGINT units exploiting CEDs may use specialized reports as specified in the US SIGINT Directives. INTREPs are normally forwarded electronically or as otherwise directed by unit SOPs and operational instructions.

C-55. Reporting through other reporting formats is discouraged. Intelligence staffs are responsible for reporting information derived from CEDs in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

C-56. Normally an electronic or hardcopy file of each report is maintained at the unit of origin; one electronic or hardcopy is submitted through intelligence reporting channels; and one is forwarded with evacuated CEDs to the next unit to receive the CED to prevent redundant reporting. In the event that the CED itself cannot be evacuated in a timely manner, a verified copy of a translation report can be forwarded separately from the original CED to an exploitation agency. This action would then be annotated in the captured document log or evidence property custody document.

C-57. When a collector includes intelligence derived from CEDs in an INTREP, the collector references all identification letters and numbers, to include the National Harmony Database numbers of the CED concerned to avoid false confirmation.

REPORTING GUIDELINES

C-58. Intelligence personnel should consider the following guidelines when preparing, submitting, and using INTREPs:

- **Timely Information.** Personnel must remember that timely reporting, especially of enemy activity, is critical. They must report accurate information as quickly as possible and not delay reports for the sole purpose of assuring the correct format.
- **Relevant Information.** Reports should contain only relevant information. This information should support decision making and the execution of operations. Limiting reports to essential information reduces the amount of time and effort subordinates must spend on collecting, organizing, and transmitting reports. Also, personnel should send only the parts or lines of a report that contain new information or changes. In radio communications, brevity reduces transmission time and avoids overloading radio nets.
- **Complete Information.** Most reports have prescribed formats to ensure completeness of transmitted information. The unit SOP should outline the format for each report. It should also explain how personnel use the format and under what conditions to submit each report.

C-59. The DOMEX team or processing site disseminates the original CED, a copy, a transcript, or a combination of these CEDs to joint, interagency, and multinational organizations. At the tactical level, the Brigade DOMEX team or processing site sends the majority of its CEDs to the Division or Corps DOMEX element or the JDEC. At operational levels, processing sites send processed CEDs to the JDEC as the central theater processing point, which ensures the dissemination of materials to the entire Intelligence Community. For transcripts and translations, the site uses a free-flow message, a format in translation software tool, or a translation format specified in annex B (Intelligence). The DOMEX team or processing site processes and uploads digital forms of all original CEDs and processed information to the National Harmony Database, thereby making it available to the entire Intelligence Community as well as echelons brigade and below.

C-60. A detailed DOMEX report containing a copy of the translation should accompany the original CED: a copy of the translation should accompany any copies of the original CED and, as required, the INTREPs.

For recorded audio and video, a transcript as well as translation should accompany the original audio and video CED. A DOMEX report should contain the following information:

- Identity of the element to which the report will be sent.
- Identity of the element which prepared the report.
- DTG of the CED translation.
- Report number as designated by local SOPs.
- National Harmony Database numbers assigned to exploited CEDs.
- CED serial numbers taken from the capture tag.
- CED description including type of CED, number of pages, physical construction of CED, and enemy identification number, if applicable.
- Original CED language.
- DTG the CED was received at element preparing the report.
- DTG the CED was captured.
- Location where CED was captured.
- Identity of capturing unit.
- Circumstances under which the CED was captured.
- Name of translator.
- Type of translation: full, extract, summary, or gist.
- Remarks for clarification or explanation, including the identification of the portions of the CED translated in an extract translation.
- Classification and downgrading instructions in accordance with AR 380-5.

C-61. Web-based reporting is an effective technique for disseminating reports and transcripts, audio and video files, and technical data to multiple users within and outside the AO. Through various websites the DOMEX team or processing site provides units visibility on the status of CEDs as well as links to associated reporting. The DOMEX team or processing site can also provide collection team personnel with access to online databases that help locate target databases to help detect, identify, and locate their targets.

ASSESS REPORTING

C-62. The DOMEX team or processing site continuously assesses reporting to ensure analytical products are satisfying the SIRs and reporting guidance in the commands' collection requirements. Ideally, the team's efforts enable the DOMEX team to anticipate requirements and deliver information to the tactical commander in time to influence decisions and actions.

- **Evaluate Reports**. Each report is then screened for timeliness, completeness, and relevance to the command's collection requirements.
- **Integrate.** This information is then used to confirm or deny information collected by a single discipline.
- **Provide Feedback.** After evaluating the reports, the DOMEX team or processing site provides feedback to the processing teams on what to sustain or adjust in their processing, analysis, and reporting.

DISSEMINATION

C-63. The final step of the DOMEX process' reporting and dissemination phase is to disseminate intelligence or information. Dissemination need not be limited to standard reporting as outlined above. Dependent upon the tactical situation, available resources, PIR, CCIR, or SIR, as well as critical pieces of information are passed quickly to those who can use them, specifically combatant commanders. The intelligence staff must be prepared to use any form of communication to pass vital information. Again, intelligence staffs are responsible for reporting and disseminating information derived from CEDs in a manner that ensures the information reaches not only the next higher echelon but also the tactical commander most affected by the information.

C-64. The current methodology for intelligence dissemination sends reporting through an echeloned structure from national, to theater, to corps, to division, and so on. Recent military operations have shown that this methodology is not timely and seldom results in lower tactical echelons receiving intelligence critical to their AO.

C-65. Dissemination through the use of websites as indicated above, as well as reporting via the DOMEX or Batch reports, has proven to be an effective method for ensuring maneuver elements receive time-sensitive information in a timely manner. This method requires maneuver elements to search for feedback (pull) rather than to receive the information as disseminated from higher echelons (push).

C-66. Finally, an electronic copy of CEDs, their translations, and all associated reports are sent to the JDEC for inclusion in a Theater CED database.

Appendix D

Intelligence Oversight

D-1. Executive Order (E.O.) 12333, US Intelligence Activities, stems from activities that DOD intelligence and CI units conducted against US persons involved in the Civil Rights and anti-Vietnam War movements in the 1960s and 1970s. DOD intelligence personnel used overt and covert means to collect information on the political positions and expressions of US persons, then retained the information in a nationwide database and disseminated the information to law enforcement authorities. In response to these abuses, the President issued E.O. 12333 to provide principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests.

D-2. The purpose of E.O. 12333 is to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents being essential to informed decision making in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the US was founded.

D-3. E.O. 12333 states the goal of the National intelligence effort is to provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy; and the protection of US national interests from foreign security threats. Supporting this goal are the following principles which apply to all intelligence components of the US Intelligence Community:

- Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.
- All means, consistent with applicable US law and E.O. 12333 and with full consideration of the rights of US persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.
- Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the US Government, or US corporations, establishments, or persons.
- To the greatest extent possible consistent with applicable US law and E.O. 12333, and with full consideration of the rights of US persons, all agencies and departments should seek to ensure full and free exchange of information to derive maximum benefit from the US intelligence effort.

INTERPRETATION

D-4. AR 381-10 promulgates the instructions of E.O. 12333 and DOD Directive 5240.1. The following summary of AR 381-10 does not modify or supersede published regulatory instructions, policy, or legal opinions. A thorough understanding of this regulation is necessary during the planning, preparation for, execution, and assessment of any intelligence operation. AR 381-10 directs intelligence organizations to refer questions concerning the interpretation of the instructions on collection, retention, and dissemination of US person information to the responsible legal office.

D-5. For current policy information on AR 381-10 and Army Intelligence Oversight, visit the Army Deputy Chief of Staff, G-2 website at http://www.dami.army.pentagon.mil/offices/damich/io/io_home.html. AR 381-10 is available from the Army Publication Directorate at http://www.army.mil/usapa/epubs /index.html.

This page intentionally left blank.

Appendix E

Operational Environment

E-1. The operational environment is defined as 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). While the operational environment includes all enemy, adversary, friendly, and neutral systems across the spectrum of conflict, it also includes an understanding of the physical environment, the state of governance, technology, local resources, and the culture of the local population

CHALLENGES OF THE OPERATIONAL ENVIRONMENT

E-2. US military forces face a dynamic, multidimensional, and increasingly interconnected global operational environment. The world situation is complicated and split into many different factions with many possible conflicts. In addition, the characteristics of warfare continue to change as the nature of conflicts change. Different threats require intelligence operations to adapt to the ever-changing operational environment. This necessitates that all MI personnel maintain or very quickly build cultural awareness (to a high level of detail) specific to the regional and local environment in the AO. These conditions greatly affect MI, as they increase the degree of difficulty and complexity in determining not only who constitutes the enemy but also which of the many possible enemy COAs the enemy could implement.

E-3. The overall ability of US forces to defeat adaptive ingenious adversaries depends upon the ability of MI personnel to analyze the current and anticipate future methods and capabilities of potential adversaries and incorporate those considerations into training, planning, and executing military operations. The operational environment will continue to change, thus US military forces and MI must continue to evolve and advance in order to provide relevant and timely intelligence.

OPERATIONAL AND MISSION VARIABLES

E-4. Army forces use operational variables to understand and analyze the broad environment in which they are conducting operations. They use mission variables to focus analysis on specific elements of the environment that apply to their mission.

Operational Variables

E-5. The operational environment is analyzed in terms of political, military, economic, social, infrastructure, and information operational variables. Army doctrine adds the variable of the physical environment and time. Collectively, these variables are often abbreviated as PMESII-PT. Analysis of these variables provide relevant information that senior commanders use to understand, visualize, and describe the operational environment. The following is a description of each of the PMESII-PT variables:

- **Political**. Describes the distribution of responsibility and power at all levels of governance or cooperation.
- **Military**. Explores the military capabilities of all relevant actors in a given operational environment.
- **Economic**. Encompasses individual behaviors and aggregate phenomena related to the production, distribution, and consumption of resources.
- **Social**. Describes the cultural, religious, and ethnic makeup within an operational environment.
- **Information**. Describes the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information.
- **Infrastructure**. Composed of the basic facilities, services, and installations needed for the functioning of a community or society.
- **Physical Environment**. Defines the physical circumstances and conditions that influence the execution of operations throughout the domains of air, land, sea, and space.

- **Time**. Influences military operations within an operational environment in terms of the decision-cycles, operational tempo, and planning horizons. (See FM 3-0.)

E-6. Conceptually, the study of the operational variables provides an unconstrained view of the operational environment, with an emphasis on human aspects. Such a comprehensive view assists commanders in appreciating how the military instrument complements the other instruments of power. To gain a broad understanding of these influences, commanders will normally consult with specialists in each area. In some cases, senior commanders will have specialists in nonmilitary subjects assigned to their staffs. (For more information on the operational variables see FM 3-0).

MISSION VARIABLES

E-7. While analysis of the operational variables improves understanding at all levels, land operations require more specific information. The operational variables are directly relevant to campaign planning; however they are too broad to be applied to tactical planning. Upon receipt of a warning order or mission, Army leaders narrow their focus to a set of mission variables applicable to a specific geographical area. These variables are: mission, enemy, terrain and weather, troops and support available, time available and civil considerations (METT-TC). Each variable is individually described below:

- **Mission.** The mission is the task, together with the purpose, that clearly indicates the action to be taken and the reason.
- **Enemy.** Relevant information regarding the enemy may include the following:
  - Dispositions (including organization, strength, location, and mobility).
  - Doctrine (or known execution patterns).
  - Personal habits and idiosyncrasies.
  - Equipment, capabilities, and vulnerabilities.
  - Probable courses of action.
- **Terrain and Weather.** Terrain and weather are natural conditions that profoundly influence operations. Terrain and weather are neutral; they favor neither side unless one is more familiar with—or better prepared to operate in—the environment.
- **Troops and Support Available.** The number, type, capabilities, and condition of available friendly troops and support available. These include the resources available from joint, interagency, multinational, host-nation, commercial (via contracting), and private organizations.
- **Time Available.** Time is critical to all operations. Controlling and exploiting time is central to initiative, tempo, and momentum. By exploiting time, commanders can exert constant pressure, control the relative speed of decisions and actions, and force exhaustion on enemy forces.
- **Civil Considerations.** Understanding the operational environment requires understanding the civil aspects of the AO. Civil considerations reflect how the manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an AO influence the conduct of military operations.

E-8. METT-TC enables leaders to synthesize operational level information with local knowledge relevant to their missions and tasks in a specified AO. Tactical and operational leaders can then anticipate the consequences of their operations before and during execution. (For further information on METT-TC see FM 3-0.)

E-9. Successful mission accomplishment requires thorough understanding of the operational environment. Today's operational environments are complex and require continuous learning and adaptation. Commanders use experience, applied judgment, and various analytic tools to gain the situational understanding necessary to make timely decisions to maintain the initiative and achieve decisive results. The more commanders understand their operational environment, the more effectively they can employ forces

E-8. METT-TC enables leaders to synthesize operational level information with local knowledge relevant to their missions and tasks in a specified AO. Tactical and operational leaders can then anticipate the consequences of their operations before and during execution. (For further information on METT-TC see FM 3-0.)

E-9. Successful mission accomplishment requires thorough understanding of the operational environment. Today's operational environments are complex and require continuous learning and adaptation. Commanders use experience, applied judgment, and various analytic tools to gain the situational understanding necessary to make timely decisions to maintain the initiative and achieve decisive results. The more commanders understand their operational environment, the more effectively they can employ forces

This page intentionally left blank.

Appendix F

Force Projection

F-1. The S-2 must answer the commander's intelligence requirements during the five stages of force projection operations, which are—

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

F-2. Until the brigade's ISR assets become operational in the AO, the S-2 will depend upon intelligence from the senior Army Force component or JTF to answer the brigade's intelligence needs. These processes occur in a continuous, overlapping, and repeating sequence throughout an operation. The brigade's S-2 and ISR organizations must be prepared to assist the commander in overcoming any planning or execution challenges.

MOBILIZATION

F-3. While the BCT is designed to be a short-notice deployment force, there may be a time in which the brigade is brought to a state of readiness for a specific mission or other national emergency. This process, called mobilization, is where specific Active Army and USAR units, capabilities, and personnel are identified and integrated into the brigade. Prior to mobilization, the commander integrates mobilization and deployment tasks into the unit's METL and training. Commanders also emphasize and integrate critical aspects of force projection into battle tasks and planning. The brigade S-2 must—

- Establish habitual training relationships with their Active Army and USAR augmentation units as well as higher echelon intelligence organizations as identified in existing OPLANs.
- Identify ISR force requirements for the different types of operations and CONPLANs.
- Identify individual military, civilian, and contractor manpower augmentation requirements for intelligence operations.

F-4. During the mobilization phase, the S-2 should—

- Support the USAR units by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify individual mobilization augmentees to fill gaps created by personnel shortages. If possible, these IMAs should be individuals who already have a working knowledge of unit SOPs and understand the mission.
- Monitor intelligence reporting on threat activity and I&W.
- Conduct or coordinate CI and OPSEC training and operations.
- Manage information requirements and RFIs from their unit and subordinate units.
- Update ISR planning based on augmentation.

DEPLOYMENT

F-5. Deployments consist of four distinct but interrelated deployment phases. Deployment is the relocation of forces and materiel to a desired operational area in response to a contingency. A successful deployment requires smooth and rapid implementation of each phase with seamless transitions and interactions among all of them. The four phases are not always sequential and could overlap or occur simultaneously. The four supporting components are—

- Predeployment activities.
- Fort-to-port.

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

F-6. Predeployment activity provides the foundation for subsequent force projection operations. Units must acquire movement expertise, knowledgeable deployment support teams, joint deployment process improvement tools, and an understanding of the Joint Operation Planning and Execution System to enable seamless deployment operations. The Mobility Officer (specialty 882A) Program was established to embed deployment expertise in the BCTs, and these officers have demonstrated the value added from the outset (FMI 3-35).

F-7. A deploying unit undergoes a series of transformations during its movement to an AO. Initially at its home station, personnel and equipment are separated in preparation for movement by different strategic lift modes—typically personnel via airlift and equipment by surface. Both personnel and equipment may arrive at different ports of debarkation and come together again as a combat-ready unit following the RSOI process. Experience has shown RSOI is difficult, and unprepared and untrained units find this to be the "Achilles heel" of their movement to the new area of operations.

F-8. The manner in which the unit conducts predeployment and prepares for fort-to-port movement will have a direct impact on RSOI. Bringing the right equipment, marking and tagging equipment, proper sequencing of personnel, having and following a deployment plan, setting and meeting established timelines, and marking and packaging of hazardous materials are all elements that set the stage for a seamless transit into the new theater of operations. A detailed and integrated plan, along with a well-organized and trained team is fundamental to the success of RSOI.

F-9. During deployment, intelligence organizations in the sustainment areas (such as the intelligence cell of the Army service component command [ASCC]) take advantage of modern SATCOM, broadcast technology, and ADP systems such as DCGS-A to provide graphic and textual intelligence updates to the forces in movement. Enroute updates help eliminate information voids and allow the commander to adjust the OPORD prior to arrival in theater.

F-10. Intelligence units extend established networks to connect intelligence staffs and collection assets at various stages of the deployment flow. Where necessary, units establish new communications paths to meet unique demands of the mission. The ASCC and corps intelligence cells play a critical role in making communications paths, networks, and intelligence databases available to deploying forces. See FMI 3-35 for detailed information on the four phases of deployment.

EMPLOYMENT

F-11. With sufficient combat power and resources in place, the focus shifts from intelligence support for deployment to support required for sustained operations. At the beginning of the operations stage, intelligence reaches the crossover point where 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 threat in combat operations. In stability operations and civil support operations the commander may use all levels of intelligence to accomplish the mission.

F-12. During all operations, the S-2 staff and ISR units support the development and execution of plans by identifying threat COGs and decisive points within the operational environment. The S-2 ensures the ISR synchronization processes focus on the commander's PIRs. ISR units continually evolve their concepts of employment to reflect changes in the operation

SUSTAINMENT

F-13. The sustainment process involves providing and maintaining personnel and materiel required to support a joint force commander. See JP 4-0 and FM 4-0 for details on the sustainment process of force projection operations.

REDEPLOYMENT

F-14. Redeployment is the return of forces to home station or demobilization station. Previously redeployment was almost an afterthought but with the introduction of Army Forces Generation (commonly referred to as ARFORGEN), redeployment has taken on a new significance. Reuniting unit personnel and their equipment at their home station triggers the start of the lifecycle management process (reset and train, ready, and available). The importance of this event is obvious now that required delivery dates are set for equipment returning from theater. (See FMI 3-35 for more information on redeployment.)

F-15. Commanders plan for redeployment within the context of the overall situation in the theater. The four phases of redeployment are—

- Redeployment preparation activities.
- Movement to and activities at port of embarkation.
- Movement to port of debarkation.
- Movement to home or demobilization station.

F-16. As combat power and resources decrease in the AO, protection to include force protection and I&W becomes the focus of the commander's intelligence requirements. This in turn drives the selection of those ISR units that must remain deployed and those that may redeploy. The S-2—

- Monitors intelligence reporting on threat activity and I&W data.
- Continues to conduct intelligence support to protection planning.
- Requests intelligence support (theater and national systems) and provides intelligence in support of redeployment and reconstitution (reverse intelligence crossover point).

This page intentionally left blank.

Appendix G

DCGS-A OVERVIEW

BACKGROUND

G-1. The DCGS-A program was created in response to the DOD Distributed Common Ground/Surface System (DCGS) Mission Area Initial Capabilities Document, which captured the overarching requirements for an ISR Family of Systems that will contribute to joint and combined Warfighter needs. DCGS-A facilitates "Seeing and Knowing" on the battlefield—the fundamental precursor to the understanding that underpins the Army's Battle Command concept.

SYSTEM OBJECTIVES

G-2. DCGS-A provides a net-centric, enterprised ISR, weather, geospatial engineering, and space operations capability to maneuver, maneuver support and maneuver sustainment support organizations at all echelons from the battalion to JTFs. DCGS-A will be the ISR component of the modular and future force Battle Command System and the Army's primary system for ISR tasking, posting, processing, and using information about the threat, weather, and terrain at all echelons.

G-3. DCGS-A provides the capabilities necessary for commanders to access information from all data sources and to synchronize non-organic sensor assets with their organic assets. DCGS-A provides continuous acquisition and synthesis of data and information from joint and interagency capabilities, multinational partners, and nontraditional sources that will permit modular forces to maintain an updated and accurate understanding of the operational environment. DCGS-A contributes to visualization and situational awareness, thereby enhancing tactical maneuver, maximizing combat power, and enhancing the ability to operate in an unpredictable and changing operational environment throughout full spectrum operations.

G-4. DCGS-A will facilitate the rapid planning, execution, and synchronization of all warfighting functions resulting in the current and future force's ability to operate within the enemy's decision cycle. The core functions of DCGS-A are—

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

G-5. DCGS-A systems (starting with DCGS-A(V4) described below) will be a net-centric, web-enabled, enterprise-based, open-architecture system of systems deployed across the force in support of ground forces commanders. It will function as a first step toward the ability to systematically access and leverage other Service ISR datasets and build an ISR architecture that integrates and synchronizes on-scene, network-distributed, and reach activities. The DCGS-A objective (DCGS-A (V5)) architecture will be capable of supporting multiple, simultaneous, worldwide operations through scalable and modular system deployments.

OPERATIONAL DESCRIPTION

G-6. DCGS-A is the Army's ground processing system for all ISR sensors. DCGS-A integrates existing and new ISR system hardware and software that produces a common net-centric, modular, multi-security, multi-intelligence, interoperable architecture. DCGS-A provides access to data across the Intelligence Enterprise as well as facilitating Reach Operations with Knowledge Centers.

G-7. DCGS-A provides access to JWICS, NSANet, SIPRNET, and NIPRNET. DCGS-A links tactical ISR sensors along with weather, space, and geospatial analysis capabilities into the Intelligence Enterprise. The DCGS-A net-centric capability enhances distributed operations by allowing ISR data access down to tactical units. Additionally, it provides the analyst data mining, fusion, collaboration, and visualization tools to conduct situational awareness, ISR synchronization, targeting support, analysis, and reporting.

G-8. DCGS-A provides users access to ISR raw sensor data, reports, graphics, and web services through the DCGS-A Integration Backbone (DIB). The DIB creates the core framework for a distributed, net-centric Intelligence Enterprise architecture. The DIB enables DCGS-A to task, process, post, and use data from Army, Joint, and National ISR sensors. The DIB provides a meta-data catalog that defines how you describe data. The meta-data allows DCGS-A to expose the required data elements to the user.

G-9. DCGS-A is the primary ISR processing system from the JTF down to battalion and below units. DCGS-A is the ISR component of the Battle Command System and provides the intelligence, weather, and geospatial engineering data to Battle Command. It provides threat reporting and the threat portion of the COP to the Publish and Subscribe Services for ABCS users, as well as accesses friendly unit information for DCGS-A users. DCGS-A provides the analyst data mining, fusion, collaboration, and visualization tools to quickly sort through large amounts of data to provide timely, relevant intelligence to the commander.

G-10. DCGS-A tools assist the targeting process as well as synchronize ISR collection. DCGS-A not only provides the analyst access to national and theater data sources but also serves as a ground station for organizational ISR sensors. DCGS-A facilitates distributed operations and reduces the forward physical footprint.

DCGS-A CONFIGURATIONS

G-11. There are three major DCGS-A configurations: embedded, mobile, and fixed.

EMBEDDED

G-12. The embedded configurations will be the common software baseline for all users. When connected to the DCGS-A enterprise, the embedded configuration will provide access to the enterprise of ISR sensor data, information, and intelligence. Immediate access to weather, geospatial engineering, and multi-INT data along with ISR synchronization, collaboration, fusion, targeting, and visualization tools provided in the DCGS-A embedded configuration will enable users to collaboratively access, plan, task, collect, post, process, exploit, use, and employ relevant threat, non-combatant, geospatial engineering, and weather information. Embedded DCGS-A software will enable access to the DCGS-A enterprise where users will subscribe to data services and acquire on-demand software applications to perform unique or new information processing tasks. The DCGS-A embedded configuration provides the ISR component to the Battle Command System at all echelons and within all units connected to the Future Force Network. DCGS-A will be an embedded component of the Future Combat System (FCS) Family of Systems and the Ground Soldier System. Because it is a component of Battle Command, DCGS-A permeates the entire Army force structure to facilitate combat and staff functions.

DCGS-A MOBILE

G-13. DCGS-A Mobile configurations will be organic to and directly support deployed modular brigades and Division G-2s, BFSBs, Corps G-2s, and Military Intelligence Brigades (MIBs) of the ASCCs. DCGS-A Mobile capabilities will be modular and scalable to meet supported unit deployment and tactical mobility criteria. They will operate independently, but will be more capable when connected to operational and strategic level sensors, sources, and people. DCGS-A Mobile brings sensor data to the deployed unit and provides a dedicated processing and analysis segment for organic sensors as well as the capability to use unexploited data from all sensors. DCGS-A Mobile extends the strategic and operational level joint, interagency, and multinational ISR network into the tactical operational environment. The DCGS-A Mobile will provide a wide range of ISR capabilities including direct access and control of select sensor platforms.

G-14. When not deployed, mobile assets will operate as part of the ISR network and be fully integrated into DCGS-A Fixed and home station operations. Upon full fielding, the DCGS-A Mobile capabilities will displace (physically) and replace (functionally) current tactical intelligence tasking, posting, processing, and using systems within the Corps G-2s/Division G-2s/BFSBs/MIBs and BCTs. The DCGS-A Mobile configuration includes man-portable and vehicle-based hardware platforms.

G-15. The man-portable system is titled Multi-Function Workstation-Mobile (MFWS-M) and the vehicle transportable system is titled the Mobile Intelligence Service Provider (MISP). Each MISP will contain a mixture of Multi-Security Level-Multi-Function Workstations (ML-MFWSs) and MFWS-Ms based on the number of personnel supported and the unit's mission. The MFWS-M includes the embedded software baseline plus additional applications exclusive to MI professionals. These additional applications are required to allow MI Soldiers to perform more complicated processing tasks that require specialized training to perform. The MFWS-M will be found primarily with the S-2 sections in the Maneuver Battalions, Separate Brigades, and other areas with MI professionals where an MISP cannot be supported.

FIXED

G-16. DCGS-A Fixed facilities are regionally located and provide overwatch to tactical units. The Fixed configuration conducts the day-to-day "heavy-lifting" support to all echelons. This configuration possesses a robust hardware processing and data storage capacity. Forward deployed organizations collaborate with, and reach to, fixed configurations across the network to substantially expand the commander's situational awareness without increasing the forward footprint. Fixed configurations are expected to be "always on" providing general and direct ISR processing, exploitation, analysis, and production support to all echelons.

DCGS-A INCREMENTAL DEVELOPMENT

G-17. DCGS-A will follow an evolutionary acquisition strategy to develop and field capabilities incrementally throughout its life cycle. This evolutionary approach is divided into three increments and provides the ability to field the best possible capability available at any point in time. This incremental approach will be executed through a series of software releases. For the most part delivered capabilities will be software only but could include some hardware products as necessary. It should be noted that although there are some DCGS-A capabilities that will not be available until Increment 3 (fiscal year [FY] 13 and beyond) Increment 2 systems will be designed to support the objective system requirements. This should allow Increment 3 upgrades to be executed as software only modifications to fielded systems. DCGS-A fielding was accelerated and delivered incrementally based on operational requirements associated with the war on terrorism. The incremental development includes consolidation and replacement of the capabilities found in the following current force systems:

- All versions of ASAS.
- CI & Interrogation Workstation.
- Human Domain Workstation.
- All versions of the Tactical Exploitation System.
- All versions of the GRCS ground processors (for example, the Integrated Processing Facility and the Guardrail Ground Baseline).
- PROPHET Control.
- JSTARS CGS.
- Digital Topographical Support System-Light (DTSS-L).
- IMETS.
- Space Support Enhancement Toolset.

Increment -1

G-18. Increment 1 includes initial efforts to improve interoperability between current force systems and related modification to program of record (POR) systems to provide an early DCGS-A-like capability.

Increment 1 also includes the integration of the Joint Intelligence Operations Capability-Iraq (JIOC-I) QRC. Responsibility for all JIOC capabilities transitioned to the program manager DCGS-A. At that time JIOC systems were re-designated DCGS-A(V2). This product was fielded to OIF/OEF units in FY 06-07 and provides access to over 200 data sources. Version 3.0 hardware and software upgrades added the DCGS Integrated Backbone (DIB) as well as two-way battle command interoperability. Version 3.1 will add the DCGS-A architecture framework. Increment 1 supports the migration of functionality and capabilities from existing POR systems, providing a means to support replacement of ASAS-L with V3.1 software.

Increment -2

G-19. Increment 2 provides ongoing development, through successive DCGS-A software baseline releases, and integration of EAC to battalion fixed and mobile systems that provide for full net-centric operations. This increment includes DCGS-A enabling of current POR systems at the BCT in FY09, at division and above in FY10, and the DCGS-A mobile test article development and follow-on production.

G-20. Increment 2 includes the DCGS-A enabling of BCT POR systems (Analysis and Control Team-Enclave, DTSS-L, IMETS, CGS and Prophet Control). When the DCGS-A capability is hosted on fielded POR systems, these systems are termed “DCGS-A enabled”.

Increment -3

G-21. Increment 3 (“Objective” DCGS-A) includes the embedded ISR toolset for ABCS and FCS and the delivery of capabilities requiring the maturity of technology or developments from complementary systems such as FCS and Aerial Common Sensor not available during the previous increments. For additional information on DCGS-A see Commanders Handbook 2-50.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

1SG	first sergeant
AA	avenue of approach
ABCS	Army Battle Command System
ACE	analysis and control element
ADA	air defense artillery
ADP	automated data processing
AFATDS	Advanced Field Artillery Tactical Data System
AFW	Air Force Weather
AMDWS	Air and Missile Defense Workstation
AO	area of operation
AOI	area of interest
AR	Army regulation
ARISC	Army Reserve Intelligence Support Center
ARL	airborne reconnaissance low
ASAS	All-Source Analysis System
ASAS-L	All-Source Analysis System-Light
ASCC	Army service component command
ASCOPE	areas, structures, capabilities, organization, people, and events
ATCCS	Army Tactical Command and Control Systems
BCT	Brigade Combat Team
BDA	battle damage assessment
BFSB	Battlefield Surveillance Brigade
BN	Battalion
BOLT	Brigade Operational Legal Team
BSB	brigade support battalion
BWT	battlefield weather team
C2	command and control
C2PC	Command and Control Personal Computer
CA	civil affairs
CAB	combined arms battalion
CAS	close air support
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high yield explosives
CCIR	commander's critical information requirement
CED	captured enemy document
CEE	captured enemy equipment
CEM	captured enemy materiel
CGS	common ground station

CI	counterintelligence
CIA	Central Intelligence Agency
CIC	combat information center
CICA	Counterintelligence Coordinating Authority
CMO	civil-military operations
COA	course of action
COG	center of gravity
COMINT	communications intelligence
COMSEC	communications security
CONPLAN	contingency plan
CONUS	continental United States
COP	common operational picture
CP	command post
CRC	Collector Reporter Code
DA	Department of the Army
DC	displaced civilian
DCGS	Distributed Common Ground System
DCGS-A	Distributed Common Ground System-Army
DF	direction finding
DIA	Defense Intelligence Agency
DIB	DCGS Integration Backbone
DISE	divison intelligene support element
DOMEX	document and media exploitation
DOD	Department of Defense
DP	decision point
DPM	disseminaton program manager
DTSS	Digital topographic Support System
DS	direct support
DSN	Defense Secure Network
DST	decision support template
DTG	date-time group
DTSS	Digital Topographic Support System
EA	electronic attack
EAB	echelons above brigade
EAC	echelon above corps
EEFI	essential elements of friendly information
ELINT	electronic intelligence
EOB	electronic order of battle
EPW	enemy prisoner of war
ES	electronic warfare support

EW	electronic warfare
FA	field artillery
FBCB2	Force XXI Battle Command Brigade and Below
FBI	Federal Bureau of Investigation
FCS	Future Combat System
FDA	functional damage assessment
FFIR	friendly forces information requirement
FP	force protection
FRAGO	fragmentary order
FS	fire support
FSCOORD	fire support coordinator
FSE	fire support element
FY	fiscal year
G-2	Assistant Chief of Staff, Intelligence
G-3	Assistant Chief of Staff, Operations
G-4	Assistant Chief of Staff, Logistics
G-5	Assistant Chief of Staff, Civil/Military Affairs
G-6	Assistant Chief of Staff, Signal
GCCS-A	Global Command and Control System-Army
GEOINT	geospatial intelligence
GMI	general military intelligence
GPW	Geneva Convention Relative to the Protection of Civilian Persons
GRCS	Guardrail Common Sensor
GS	general support
GWS	Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field
HBCT	heavy brigade combat team
HCT	HUMINT collection team
HHC	headquarters and headquarters company
HN	host nation
HOC	HUMINT operations cell
HPT	high-payoff target
HUMINT	human intelligence
HVT	high-value target
I&W	indications and warnings
IBCT	infantry brigade combat team
ICC	Intelligence Collection Code
ICF	Intelligence Contingency Fund
ICL	Intelligence coordination line
IEW	intelligence and electronic warfare

IFC	Intelligence Functional Code
IIR	intelligence information report
IMETS	Integrated Meteorological System
IMETS-L	Integrated Meteorological System-Light
IMINT	imagery intelligence
INSCOM	United States Army Intelligence and Security Command
INTREP	intelligence report
INTSUM	intelligence summary
IO	information operations
IP	Internet Protocol
IPB	intelligence preparation of the battlefield
IR	information requirement
ISP	intelligence support package
ISR	intelligence, surveillance, and reconnaissance
JCDB	Joint Common Data Base
JDEC	Joint Document Exploitation Center
JDISS	Joint Deployable Intelligence Support System
JIC	Joint Intelligence Center
JIOC	Joint Intelligence Opeations Capability
JIOC-I	Joint Intelligence Operations Capability-Iraq
JSTARS	Joint Surveillance Target Attack Radar System
JTT	joint tactical terminal
JWICS	Joint Worldwide Intelligence Communications System
KB	knowledgeability brief
LEIOV	latest event information is of value
LN	local national
LNO	liaison officer
LOB	line of bearing
LOC	line of communication
LOO	line of operation
LTIOV	latest time information is of value
MASINT	measurement and signature intelligence
MCO	major combat operations
MCOO	modified combined obstacle overlay
MCS	Maneuver Contol Systrm
MDMP	military decsion-making process
MEA	munitions effects assessment
METL	mission-essential task list
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations

MI	military intelligence
MFWS	Multi-Function Workstation
MFWS-M	Multi-Function Workstation-Mobile
MIB	Military Intelligence Brigade
MILES	Multiple Integrated Laser Equipment System
MISP	Mobile Intelligence Service Provider
ML-MFWS	Multi-Security Level-Multi-Function Workstation
MOS	military occupational specialty
MP	military police
MTI	moving target indicator
MTOE	modified table of organization and equipment
NAI	named area of interest
NCO	noncommissioned officer
NCOIC	noncommissioned officer in charge
NFA	no-fire area
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NLOS	night line of sight
NRT	near-real time
NSA	National Security Agency
O/I	operations and intelligence
OIC	officer in charge
OIF	Operation Iraqi Freedom
OMT	operational management team
OPCON	operational control
OPLAN	operations plan
OPORD	operation order
OPSEC	operations security
OSINT	open-source intelligence
OWS	operational weather squadron
PDA	physical damage assessment
PGM	precision-guided munitions
PIR	priority intelligence requirement
POR	program of record
PSG	platoon sergeant
PSYOP	psychological operation
QRC	quick reaction capability
RC	Reserve Component
RDSP	rapid decision-making and synchronization process
RFI	request for information

RHO	reconnaissance handover
RM	requirements management
RSOI	reception, staging, onward movement, and integration
S&T	scientific and technical
S-2	Staff Officer, Intelligence
S-2X	Staff Officer, Intelligence (CI and HUMINT)
S-3	Staff Officer, Operations
SAEDA	Subversion and Espionage Directed Against the US Army
SALUTE	size, activity, location, unit, time, and equipment
SAR	synthetic aperture radar
SATCOM	satellite communications
SBCT	Stryker Brigade Combat Team
SCI	sensitive compartmented information
SIGINT	signals intelligence
SIR	specific information requirement
SJA	Staff Judge Advocate
SOF	special operations forces
SOP	standing operating procedure
SSC	small-scale contingency
SSO	special security office
STANAG	standardization agreement
SWO	staff weather officer
TA	target acquisition
TACON	tactical control
TAI	target area of interest
TECHINT	technical intelligence
TES	Tactical Exploitation System
TOC	tactical operations center
TOE	table of organization and equipment
TRADOC	United States Army Training and Doctrine Command
TSA	target system assessment
TTP	tactics, techniques, and procedures
TUAS	tactical unmanned aircraft system
UAS	unmanned aircraft system
US	United States
USAF	US Air Force
V	version
WARNO	warning order
XO	executive officer

References

SOURCES USED

These are the sources quoted or paraphrased in this publication.

ARMY PUBLICATIONS

AR 380-5, *Department of the Army Information Security Program*, 29 September 2000

AR 381-10, *US Army Intelligence Activities*, 3 May 2007

FM 1-02, *Operational Terms and Graphics*, 21 September 2004

FM 2-0, *Intelligence*, 17 May 2004

FM 2-22.3, *Human Intelligence Collector Operations*, 6 September 2006

FM 3-0, *Operations*, 27 February 2008

FM 3-05.40, *Civil Affairs Operations*, 29 September 2006

FM 3-06, *Urban Operations*, 26 October 2006

FM 3-20.96, *Reconnaissance Squadron (RSTA)*, 20 September 2006

FM 3-20.98, *Reconnaissance Platoon*, 12 February 2002

FM 3-20.971, *Reconnaissance Troop RECCE Troop and Brigade Reconnaissance Troop*, 2 December 2002

FM 3-21.94, *The Stryker Brigade Combat Team Infantry Battalion Reconnaissance Platoon*, 18 April 2003

FM 3-24, *Counterinsurgency*, 15 December 2006

FM 3-90.6, *The Brigade Combat Team*, 4 August 2006

FM 3-90.61, *The Brigade Special Troops Battalion*, 22 December 2006

FM 4-0, *Combat Service Support*, 29 August 2003

FM 5-0, *Army Planning and Orders Production*, 20 January 2005

FM 6-0, *Mission Command: Command and Control of Army Forces*, 11 August 2003

FM 6-20-10, *Tactics, Techniques, and Procedures for the Targeting Process*, 8 May 1996

FM 6-99.2, *US Army Report and Message Formats*, 30 April 2007

FM 7-92, *The Infantry Reconnaissance Platoon and Squad*, 23 December 1992

FM 17-97, *Cavalry Troop*, 3 October 1995

FM 27-10 (FM 1-27.1), *The Law of the Land Warfare*, 18 July 1956

FM 34-2, *Collection Management and Synchronization Planning*, 8 March 1994

FM 34-2-1, *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance, 19 June 1991*

FM 34-3, *Intelligence Analysis*, 15 May 1990

FM 34-37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations*, 15 January 1991

FM 34-45, *Tactics, Techniques, and Procedures for Electronic Attack*, 9 June 2000

FM 34-54, *Technical Intelligence*, 30 January 1998

FM 34-60, *Counterintelligence*, 3 October 1995

FM 34-130, *Intelligence Preparation of the Battlefield*, 8 July 1994

FM 55-15, *Transportation Reference Data*, 27 October 1997

FM 55-30, *Army Motor Transport Units and Operations*, 27 June 1997

FM 71-100, *Division Operations*, 28 August 1996

FMI 3-0.1, *The Modular Force*, 28 January 2008

FMI 5-01.1, *The Operations Process*, 31 March 2006

TB 55-46-1, *Standard Characteristics(Dimensions, Weight, and Cube) for Transportation of Military Vehicles and Other Oversize/Overweight Equipment (In TOE Line Item Number Sequence)*, 15 January 1993

TC 3-34.489, *The Soldier and the Environment*, 8 May 2001

TC 34-55, *Imagery Intelligence*, 3 October 1988

Geneva Convention of 1949 (http://usmilitary.about.com/od/deploymentsconflicts/l/blgenevaconv.htm)

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field

Geneva Convention Relative to the Protection of Civilian Persons

AJP-2-5(A), *Handling of Captured Personnel, Equipment, and Documents*, September 2001

JP 2-01, *Joint Intelligence Support to Military Operations*, 20 November 1996

JP 4-0, *Joint Logistics*, 18 July 2008

NOTE: All JP publications are available at http://jdeis.js.mil/jdeis.

MIL STD 2525B, *Common Warfighting Symbology*, 30 January 1999, with Change 2 dated 7 March 2007 (http://www.everyspec.com/MIL-STD/)

DOCUMENTS NEEDED

DA forms are available on the APD website (www.apd.arm.mil). DD Forms are available on the OSD website (www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm)

DD Form 2745, *Enemy Prisoner of War (EPW) Capture Tag*

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

DA Form 4137, *Evidence/Property Custody Document*

Index

This page intentionally left blank.

FM 2-19.4
25 November 2008

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army,
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to
the Secretary of the Army
0830901

DISTRIBUTION:

Active Army, Army National Guard, and U. S. Army Reserve: Not to be distributed.
Electronic Media Only.

PIN: 085230-000