TC 2-50.5

Intelligence Officer's Handbook

January 2010

Headquarters, Department of the Army

This publication is available at:

Army Knowledge Online
(www.us.army.mil)

General Dennis J. Reimer
Training and Doctrine Digital Library
(http://www.train.army.mil)

United States Army Publishing Agency
(http://www.army.mil/usapa)

Training Circular
No. 2-50.5

Headquarters
Department of the Army
Washington, DC, 6 January 2010

Intelligence Officer's Handbook

Contents

Figures

Tables

Preface

TC 2-50.5 replaces FM 34-8-2, dated 1 May 1998. This publication does not replace the fundamental principles and tactics, techniques, and procedures contained in the other FM 2-series manuals; however, it does focus on their application. It is to be used in conjunction with the other FM 2-series manuals and conforms to the overarching doctrinal concepts presented in FM 3-0 and FM 2-0.

The target audience for this manual is the intelligence officers serving as the G-2/S-2 and their staffs—intelligence warrant officers, noncommissioned officers, and junior enlisted Soldiers.

TC 2-50.5 applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

The term intelligence officer generally refers to the G-2/S-2 and other intelligence positions within units and organizations. The term operations officer generally refers to the G-3/S-3, and other operations positions within units and organizations.

TC 2-50.5 uses joint terms where applicable. The terms with joint or Army definitions are in the text. They are italicized and the number of the proponent publication follows the definition.

The use or mention of any commercial or private organization's name or trademark and the organization's services or funds by the Army does not express or imply an endorsement of the sponsor or its products and services by the Army.

Headquarters U.S. Army Training and Doctrine Command is the proponent of this publication. The preparing agency is the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to: Commander, ATZS-CDI-D (TC 2-50.5), USAICoE, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017; by email to ATZS-FDC-D@conus.army.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Chapter 1

The Intelligence Warfighting Function

This chapter discusses the warfighting functions, focusing mainly on the intelligence warfighting function and its associated tasks, the characteristics of effective intelligence, and the intelligence categories and disciplines.

OVERVIEW

1-1. The intelligence warfighting function is one of six warfighting functions. A *warfighting function* is a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives (FM 3-0).

The Warfighting Functions
- Movement and maneuver
- Intelligence
- Fires
- Sustainment
- Command and control
- Protection

1-2. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment. It includes tasks associated with intelligence, surveillance, and reconnaissance operations and is driven by the commander (FM 3-0). Intelligence is more than just collection; it is a continuous process that involves analyzing information from all sources and conducting operations to develop the situation. The intelligence warfighting function includes the following tasks:

- Support to force generation.
- Support to situational understanding.
- Conduct intelligence, surveillance, and reconnaissance (ISR).
- Provide intelligence support to targeting and information superiority.

1-3. Table 1-1 (page 1-2) lists the intelligence tasks and subtasks. (See FM 2-0.)

EFFECTIVE INTELLIGENCE CHARACTERISTICS

1-4. The effectiveness of the intelligence warfighting function is measured against the relevant information quality criteria:

- **Accuracy.** Intelligence must give commanders an accurate, balanced, complete, and objective picture of the enemy and the operational environment. To any extent possible, intelligence should accurately identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and bias-free intelligence.
- **Timeliness.** Intelligence must be provided early enough to support operations and prevent surprise enemy action. It must flow continuously to the commander before, during, and after an operation. Intelligence organizations, databases, and products must be available to develop estimates, make decisions, and plan operations.
- **Usability.** Intelligence must be presented in a format that is easily understood or displayed in a format that immediately conveys the meaning to the consumer.
- **Completeness.** Intelligence briefings and products must convey all the necessary components to be as complete as possible.

- **Precision.** Intelligence briefings and products must provide the required level of detail to answer the requirements, no more and no less.
- **Reliability.** Evaluate intelligence to determine whether the collected information—used in intelligence briefings and products—is trustworthy, uncorrupted, and undistorted. Any concerns should be stated up front.

1-5. Intelligence requires three additional criteria to be effective:

- **Relevant.** Intelligence must support the commander's concept of the operation and the unit's mission. It must be relevant to the capabilities of the unit and the commander's critical information requirements (CCIRs) and preferences.
- **Predictive.** Intelligence should inform the commander about what the enemy can do—most dangerous course of action (COA)—and what the enemy is expected to do—most likely enemy COA.
- **Tailored.** Intelligence should be presented based on the needs of the commanders, subordinate commanders, and staff. Intelligence should be clear and concise so they can understand, believe, and act on it. Intelligence should support and satisfy the commander's priorities.

Table 1-1. Intelligence warfighting function tasks

Support to force generation
• Provide intelligence readiness. • Establish intelligence architecture. • Provide intelligence overwatch. • Generate intelligence knowledge. • Tailor the intelligence force.
Support to situational understanding
• Perform IPB. • Perform situation development. • Provide intelligence support to protection. • Provide tactical intelligence overwatch. • Provide intelligence support to civil affairs operations.
Support to situational understanding
Note. The police intelligence operations function is not an intelligence discipline. It is a law enforcement function. However, it is within the critical intelligence task "support situational understanding" that police intelligence operations best support the MI cycle. Police intelligence operations are essential to this task, particularly where asymmetric threats (criminal, terrorist, and insurgents) threaten the security of U.S. forces and military operations. This function supports and enhances the commander's situational awareness and COP through collection, analysis, and appropriate dissemination of relevant criminal, police information and criminal intelligence. Police intelligence operations are a vital tool to law enforcement personnel and criminal investigators who distribute and focus MP and criminal investigations assets. U.S. codes, EOs, DODDs, and ARs contain specific guidance regarding the prohibition of intelligence personnel from collecting intelligence on U.S. citizens, U.S. corporations, and non-U.S. citizen residents. Any access by the intelligence community to information or products—resulting from police intelligence operations directed against U.S. citizens—should undergo competent legal review.
Conduct ISR
• Perform ISR synchronization. • Perform ISR integration. • Conduct reconnaissance. • Conduct surveillance. • Conduct related missions and operations. • Support sensitive site exploitation. • Provide intelligence support to personnel recovery.
Provide intelligence support to targeting and information superiority
Note. This task branch supports both direct and indirect delivery of fires. This task is also linked to • Provide intelligence support to targeting. • Provide intelligence support to Army information tasks. • Provide intelligence support to combat assessment.

AR—Army regulation
COP—common operational picture
DODD—Department of Defense directive
EO—executive order
IPB—intelligence preparation of the battlefield
ISR—intelligence, surveillance, reconnaissance
MI—military intelligence
MP—military police

INTELLIGENCE CATEGORIES

1-6. As discussed in FM 2-0, Army unit intelligence staffs produce and receive, directly or indirectly, six categories of intelligence support from the U.S. intelligence community. Intelligence categories are distinguishable primarily by their intelligence product purposes. The categories can overlap and the same intelligence can be used in each category. Intelligence organizations use specialized procedures to develop these categories. The following information describes each category and the responsible organization:

- **Indications and warning (I&W).** Analysis of time-sensitive information that could involve a threat to U.S. and multinational military forces, U.S. political or economic interests, or to U.S. citizens. While the G-2/S-2 produces I&W intelligence, every Soldier, such as the one conducting a presence patrol, contributes to the I&W through awareness of the CCIRs and by reporting related information.
- **Current intelligence.** The G-2/S-2 produces accurate reporting on the current threat situation—which becomes a portion of the common operational picture (COP)—projects the threat's anticipated situation and the implication to friendly operations.
- **General military intelligence (GMI).** GMI focuses on the military capabilities of foreign countries, organizations, or on topics relating to Armed Forces capabilities, including threat characteristics (previously order of battle factors) and area or terrain intelligence. The G-2/S-2 develops initial intelligence preparation of the battlefield (IPB) products from various GMI databases, and then develops and maintains the unit's GMI database on potential threat forces and areas of concern based on the commander's guidance. This database supports the unit's plan, preparation, execution, and assessment of operations.
- **Target intelligence.** The analysis of threat units, dispositions, facilities, and systems to identify and nominate specific assets or vulnerabilities for attack, reattack, or exploit.
- **Scientific and technical intelligence (S&TI).** The collection, evaluation, and interpretation of foreign engineering science and technology with warfare potential, including military systems, weapons, weapons systems, materiel, research and development, and production methods. The G-2/S-2 establishes instructions in standing operating procedures (SOPs), orders, and plans for handling and evacuating captured enemy material for S&TI exploitation.
- **Counterintelligence (CI).** Identifying and recommending countermeasures against threats by foreign intelligence services and the ISR activities of nonstate entities, such as organized crime, terrorist groups, and drug traffickers.

INTELLIGENCE DISCIPLINES

1-7. Intelligence disciplines are categories of intelligence functions. There are nine major intelligence disciplines:

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

1-8. Table 1-2 (page 1-4) describes the Army's intelligence disciplines.

Table 1-2. Intelligence disciplines

All-source intelligence
• ***All-source intelligence***—Intelligence products or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence (FM 1-02). • MOSs/AOCs associated with all-source intelligence—35F/350F, 35D. • For more information on all-source intelligence, see FM 2-0.
Counterintelligence
• ***Counterintelligence***—counters or neutralizes intelligence collection efforts through collection, counterintelligence investigations, operations, analysis and production, and functional and technical services. Counterintelligence includes all actions taken to detect, identify, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; and is the key intelligence community contributor to protect U.S. interests and equities (FM 2-0). • MOSs/AOCs associated with CI—35L/351L, 35E. • For more information on CI, see FM 2-22.2.
Human intelligence
• ***Human intelligence***—Collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities. It uses human sources and a variety of collection methods, both passively and actively, to gather information to satisfy the commander's intelligence requirements and cross-cue other intelligence disciplines (FM 2-0). • MOSs/AOCs associated with HUMINT—35M/351M, 35F. • For more information on HUMINT, see FM 2-22.3.
Geospatial intelligence
• ***Geospatial intelligence***—The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (FM 2-0). • MOSs/AOCs associated with GEOINT—21Y, 35G, 35H/350G, 215D, 35C. • For more information on GEOINT, see FM 2-0.
Imagery intelligence
• ***Imagery intelligence***—Intelligence derived from the exploitation of imagery collected by visual photography, infrared, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media (FM 2-0). • MOSs/AOCs associated with IMINT—35G, 35H/350G, 35C. • For more information on IMINT, see FM 2-0.
Measurement and signature intelligence
• ***Measurement and signature intelligence***—Technically derived intelligence that detects, locates, tracks, identifies, and/or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from imagery intelligence and signals intelligence collection (FM 2-0). • MOSs/AOCs associated with MASINT—35G, 35S/350G, 352S, 35C. • For more information on MASINT, see FM 2-0.
Open-source intelligence
• ***Open-source intelligence***—Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to intelligence requirements (FM 2-0). • The Army does not have a specific MOS, AOC, additional skill identifier, or special qualification identifier for OSINT. • For more information on OSINT, see FM 2-0.
Signals intelligence
• ***Signals intelligence***—Category of intelligence comprising individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. Signals intelligence is derived from communications, electronics, and foreign instrumentation signals (FM 2-0). • MOSs/AOCs associated with SIGINT—35N, 35P, 35S/352N, 352P, 352S, 35G. • For more information on SIGINT, see FM 2-0.

Table 1-2. Intelligence disciplines (continued)

Technical intelligence	
• ***Technical intelligence***—Intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (FM 2-0). • The Army does not have a specific MOS, AOC, additional skill identifier, or special qualification identifier for TECHINT. • For more information on TECHINT, see FM 2-0.	
AOC—area of concentration CI—counterintelligence GEOINT—geospatial intelligence IMINT—imagery intelligence MASINT—measurement and signature intelligence	MOS—military occupational specialty OSINT—open-source intelligence SIGINT—signals intelligence TECHINT—technical intelligence

This page intentionally left blank.

Chapter 2

Role of Intelligence in Military Decisionmaking

This chapter discusses the two processes available to develop operational planning—the rapid decisionmaking and synchronization process (RDSP) and the military decisionmaking process (MDMP). The role of intelligence in each process is also discussed. See FM 5-0 for detailed information on the MDMP.

THE RAPID DECISIONMAKING AND SYNCHRONIZATION PROCESS

2-1. The RDSP is the operational planning process routinely employed by commanders and staff when MDMP and troop-leading procedures are not timely enough for mission execution. This technique is used by leaders to focus on executing rather than planning. The RDSP is based on an existing order and seeks an acceptable solution, while the MDMP seeks an optimal solution.

2-2. Intelligence support to the RDSP focuses on experience and situational awareness in predicting activities or events and managing assets dynamically to adapt rapidly to a changing threat environment. RDSP facilitates continuous integration and synchronization of the warfighting functions to address the constantly changing situations.

THE MILITARY DECISIONMAKING PROCESS

2-3. The *military decisionmaking process* is a process that integrates the activities of the commander, staff, and subordinate commanders in developing an operation plan or order. It establishes methods for understanding the situation and analyzing a mission; developing, analyzing, and comparing courses of action; selecting the most favorable course of action; and producing an operation plan or order (FM 5-0). Unlike the RDSP, the MDMP is detailed, deliberate, sequential, and time consuming. It helps the commander and staff examine the area of operations (AO) and reach logical decisions.

2-4. Commanders follow the "one-third/two-thirds rule" to allocate time available for planning and preparation: they use one-third of the time available for their planning and allocate the remaining two-thirds to their subordinates. However, modern information systems and parallel and collaborative planning techniques can enable commanders to obtain more of a one-fifth/four-fifths planning ratio.

2-5. Intelligence support to MDMP is based on continuous intelligence preparation of the battlefield (IPB), which is an integrated staff function driven by the commander. The intelligence officer must train the intelligence section to conduct IPB and coordinate closely with other staff and warfighting function representatives. The intelligence officer should have a thorough understanding of all the warfighting functions to effectively integrate intelligence during planning.

2-6. The MDMP is a seven-step analytical process with each step building from 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. The seven steps of the MDMP are—

- Receipt of mission.
- Mission analysis.
- Course of action (COA) development.
- COA analysis (wargaming).

- COA comparison.
- COA approval.
- Orders production.

2-7. Each step in the process has different intelligence requirements and imposes different tasks on the supporting intelligence, surveillance, and reconnaissance (ISR) units and/or organizations at all levels. The intelligence staff assists the commander in planning, preparing, executing, and assessing operations by—

- Providing timely, relevant, accurate, predictive, and tailored intelligence.
- Making running estimates and recommendations.
- Preparing the intelligence portions of the operation plan (OPLAN) and operation order (OPORD).
- Monitoring the execution of ISR operations.

RUNNING ESTIMATE

2-8. The MDMP is much more than simply selecting a particular COA. It results in a series of products, including updated running estimates. A *running estimate* is a staff section's continuous assessment of current and future operations to determine if the current operation is proceeding according to the commander's intent and if future operations are supportable (FM 6-0).

2-9. As staff members receive information, they prepare and maintain the running estimate. Table 2-1 lists staff duties and responsibilities for preparing and maintaining a running estimate.

Table 2-1. The running estimate

Running estimate	***The intelligence staff's running estimate***
• Staff members continuously consider the effect of new information and update facts, assumptions, friendly force status, enemy activities and capabilities, and civil considerations. • Staff members include updated conclusions and recommendations in the running estimate. • Staff members use running estimates to form, analyze, compare, and recommend friendly COAs to help commanders make decisions and establish policies. • Staff members use war game results and running estimates to compare COAs.	• Intelligence staff members use format in TC 2-33.4. • The running estimate, at an absolute minimum, focuses on the threat's most likely and dangerous courses of action. As new information is obtained, the intelligence section updates and assesses the following: ▪ Facts. ▪ Assumptions. ▪ Friendly force capabilities regarding the enemy's capabilities. ▪ Enemy capabilities for current operations and future plans. ▪ Terrain and weather effects on current and future operations. ▪ Civil considerations affecting current operations and future plans. ▪ Conclusions and recommendations.

INTELLIGENCE SUPPORT TO THE MILITARY DECISIONMAKING PROCESS

2-10. Table 2-2 describes each of the seven steps of the MDMP accompanied by an intelligence support to the MDMP list of the G-2/S-2 section's responsibilities.

Table 2-2. Intelligence support to the MDMP

Step 1—Receipt of mission	***Intelligence support to step 1***
• The mission comes from higher headquarters or is derived from an ongoing mission. • Upon receipt of a new mission, the G-3/S-3 issues a WARNO to the staff. • The staff immediately prepares for mission analysis. • The commander and staff immediately perform a quick initial assessment with emphasis on an initial allocation of available time. • The commander issues the initial guidance and the G-3/S-3 issues a WARNO to subordinate units.	• Begin parallel planning and collaborate with higher and lower G-2/S-2 before and during mission receipt to facilitate the IPB process. • Focus activities on the mission variables. • Identify gaps in intelligence holdings. • Use intelligence reach to gather updated or additional enemy, terrain, weather, and civil consideration data. • Coordinate with the geospatial engineer and weather specialty teams to ensure required products are being developed and refined. • Develop and submit initial RFIs based on gaps in intelligence. • Continuously update the MCOO templates, and threat situation. • Update intelligence running estimates.
Step 2—Mission analysis	***Intelligence support to step 2***
1. Analyze the higher headquarters' order. (Seek clarification or resolution if confused or opposed.) 2. Perform initial IPB. 3. Determine specified, implied, and essential tasks. (It is important to understand specific requirements for each task.) 4. Review available assets. (Identify additional resources needed to ensure the mission's success.) 5. Determine constraints normally found in the scheme of maneuver, concept of the operation, and coordinating instructions. 6. Identify critical facts and assumptions. (List all appropriate assumptions from higher headquarters; state relevant conditions of which the commander has no control.) 7. Perform risk assessment. 8. Determine initial CCIRs (limit to 10 or less) and EEFI. 9. Determine an initial ISR plan. (The resulting ISR annex sets ISR in motion.) 10. Update operational timelines. The commander and staff refine initial plan for use of available time. 11. Write the restated mission—who, what, when, where, and why. 12. Deliver a mission analysis briefing. (Given to commander and staff, this briefing is critical to ensure a thorough understanding of planning.) 13. Approve the restated mission. 14. Develop the initial commander's intent—a clear, concise statement of what the force should do and the conditions that represent the desired end state. 15. Issue the commander's planning guidance, which provides additional guidance to focus staff planning. 16. Issue a WARNO.	• Identify gaps in higher headquarters ISR plan and IPB. • Lead the staff through the IPB process. • Begin the ISR synchronization process by identifying specified and implied intelligence tasks from the higher headquarters order. **Intelligence and intelligence-related products:** • Assist in determining the AO and AOI. • Initial information requirements (with staff). • Recommend initial PIRs to the commander. • Assist with initial OPSEC vulnerabilities and EEFI. **MCOO and terrain**—as described by observation and fields of fire, AAs, key terrain obstacles, and cover and concealment (OAKOC) and its effects. Does the MCOO— • Identify restricted or severely restricted terrain? • Identify mobility corridors (air and ground)? • Identify infiltration lanes and landing and pickup zones? • Identify key or decisive terrain? • Define defensible terrain? **Situation templates** (unrefined)—Do the situation templates— • Include all committed and reinforcing forces as well as combat multipliers? • Focus at a minimum two levels down in detail (or as command dictates) including all threat warfighting functions? • Identify with graphics threat characteristics, weaknesses and peculiarities, activities, and capabilities for each COA? **Event templates and matrices** (unrefined)—Do the event templates identify and focus on— • NAIs? • Time phase lines? • Time distance analysis? • Critical actions? • Threat decision plan?

Table 2-2. Intelligence support to the MDMP (continued)

Step 2—Mission analysis	*Intelligence support to step 2*
17. Review facts and assumptions. When facts or assumptions change, the commander and staff must assess their impact.	**IPB products—** • Identify facts and assumptions that assist in the determination of likely threat COAs. • Assist with defining threat objectives. Prepare terrain and weather analysis products to describe what effects will significantly impact the AO on both threat and friendly forces. **ISR synchronization tools (initial).** • Do the initial ISR synchronization tools— ▪ Consider the AO and the mission statement? ▪ Consider the current event template and the amount and location of all ISR assets? ▪ Incorporate higher headquarters ISR requirements? • Are the initial ISR synchronization tools based on— ▪ PIRs? ▪ Information requirements? ▪ NAIs? **Update intelligence running estimate.** These products are used to write Annex B of the OPORD or OPLAN and as the foundation for the DST later in the MDMP. Forward intelligence requirements that cannot be answered by assigned ISR assets to higher headquarters as RFIs. Start the subsequent steps of ISR synchronization to support the initial ISR plan (at a minimum; SIRs). The ISR plan is a coordinated staff effort that includes fire support, casualty evacuation, and contingency plans, for example, what the brigade does if two key scout sections are destroyed? The MI unit commander participates in mission analysis and briefs the unit asset's status and capabilities.
Step 3—COA development	*Intelligence support to step 3*
1. Analyze relative combat power. See FM 2-01.3. 2. Generate options. Develop COAs for every feasible threat COA; however, the commander usually limits that option with guidance. 3. Array initial forces. Identify number of units needed and operational methods. Develop a knowledge base for decisionmaking. 4. Develop the concept of operations. 5. Assign headquarters, which creates the task organization. 6. Prepare COA statements and sketches. The G-3/S-3 uses appropriate media to portray how unit will accomplish the mission, for example, concept of operations. Focus on threat vulnerabilities.	• **Intelligence and intelligence-related products:** ▪ Situation templates (refined and prioritized). ▪ Event templates and matrices (refined). ▪ Update the intelligence running estimate. • Provide input to the EW target list (initial). • Ensure the G-3/S-3 uses the IPB facts, assumptions, and products developed during mission analysis and subsequently refined. • Coordinate with the staff to ensure that friendly COAs take advantage of the AO, civil considerations, and threat situation. Coordinate with the staff to refine information requirements. • Provide input, which is critical when analyzing relative combat power. • Remember to support deception planning (when appropriate). • Provide critical input through continual analysis of information provided by ongoing ISR operations.

Table 2-2. Intelligence support to the MDMP (continued)

Step 4—COA analysis (wargaming)	***Intelligence support to step 4***
The war game is a critical and disciplined process used to visualize the flow of battle. 1. Gather the tools. 2. List all friendly forces. 3. List assumptions. 4. List known critical events and decision points. 5. Determine evaluation criteria. 6. Select the wargaming method. 7. Select a method to record and display results. 8. Wargame the battle and assess results. • The commander selects the order of comparison of threats to friendly COAs. • The staff must evaluate the need for branches and sequels. • When technically possible, the staff should capture as much of the war game on Army Tactical Command and Control Systems as possible, otherwise, use a wargaming worksheet or intelligence synchronization matrix. • These wargaming results are key to developing DSTs and warfighting function synchronization matrix. • Use the action, reaction, counteraction method (consider at a minimum maneuver, fire support, mobility, countermobility, survivability, intelligence, and electronic warfare). • The staff should track force ratios throughout the war game.	• **Intelligence and intelligence-related products:** ▪ PIRs with LTIOV (refined). ▪ Assist with the development of HPTL from HVTs. ▪ Assist in confirming and/or denying the threat objectives determined during step 2. ▪ Situation templates (final). ▪ Vulnerabilities to CBRNE operations. ▪ Assist with refining the EW target list. ▪ Update the intelligence running estimate. • Acting as the threat commander, project threat actions or reactions, develop decision points, and project threat losses. • During the war game, address all relevant threat warfighting function capabilities. • As the friendly G-2/S-2, identify information requirements and NAIs; refine the situation template; and participate in the targeting conference. • Ensure the G-3/S-3 honestly portrays friendly capabilities during the war game. • Coordinate with entire staff to ensure friendly COAs take advantage of the AO and threat situation. • Ensure HPTs, AGM, and TSS support the operation. • The AGM is approved by the commander and addresses which targets will be attacked, how, when, and the desired effects. • TSS are criteria used in deciding whether to pass information as a target nomination. • The MI company commander and ISR synchronization managers are important participants at the war game. • Refine all products as well as the ISR synchronization tools based on the wargaming results for the next steps (with the staff).
Step 5—COA comparison	***Intelligence support to step 5***
• Conduct a COA advantage and disadvantage analysis. • Used to identify COA that has highest probability of success. • Staff may use any technique; the decision matrix is the most common. • Staff gets its criteria from the commander (for example the principles of war or tenets of Army operations).	• **Intelligence products:** ▪ Update the intelligence running estimate. ▪ Refine products from step 4. ▪ Play a key role during this step.

Table 2-2. Intelligence support to the MDMP (continued)

Step 6—COA approval	*Intelligence support to step 6*
• The staff recommends a COA, usually in a decision briefing. (If the commander modifies a recommended COA or gives the staff a new COA, the staff wargames that COA.) • The commander decides which COA to approve. • The commander issues the final planning guidance. • The staff captures all the information in verbal orders and WARNOs and produces a written order to follow up on any previously issued orders.	• Intelligence and intelligence-related products: ▪ PIRs with LTIOV (approved). ▪ Support DST development (integrated staff product). ▪ Assist with the warfighting function synchronization matrix. ▪ Intelligence synchronization matrix (final). ▪ Event templates and matrices (final). ▪ ISR synchronization tools (refined, staff effort). • Support ISR integration (G-3/S-3) development of the ISR plan. • Begin the subsequent ISR steps synchronization, such as development of new SIRs and RFIs. • If the commander designates the staff to perform BDA to support one of the decisions, plan the BDA support and tie that plan into the ISR synch matrix.
Step 7—Orders production	***Intelligence support to step 7***
• Orders production is based on the commander's decision and final guidance.	• **Intelligence and intelligence-related products:** ▪ OPORD or OPLAN Annex B (Intelligence). ▪ Assist with OPORD or OPLAN annexes. ▪ Update intelligence running estimate. ▪ Update the ISR synchronization matrix.

AA—avenue of approach
AGM—attack guidance matrix
AO—area of operations
AOI—area of interest
BDA—battle damage assessment
CBRNE—chemical, biological, radiological, nuclear, high-yield explosives
CCIR—commander's critical information requirement
COA—course of action
DST—decision support template
EEFI—essential element of friendly information
EW—electronic warfare
HPT—high-payoff target
HPTL—high-payoff target list
HVT—high-value target
IO—information operations
IPB—intelligence preparation of the battlefield
ISR—intelligence, surveillance, reconnaissance
LTIOV—latest time information is of value
MCOO—modified combined obstacle overlay
MDMP—military decisionmaking process
METT-TC—mission, enemy, terrain and weather, troops and support available–time available and civil considerations
MI—military intelligence
NAI—named area of interest
OPLAN—operation plan
OPORD—operation order
OPSEC—operations security
PIR—priority intelligence requirement
RFI—request for information
SIR—specific information requirement
TSS—target selection standard
WARNO—warning order

Chapter 3

Intelligence Preparation of the Battlefield

Intelligence preparation of the battlefield is led by the G-2/S-2 with participation by the entire staff. It is the staff planning activity undertaken to define and understand the advantages and disadvantages presented to friendly and enemy forces. The intelligence staff conducts effective IPB when it understands the operational environment and produces IPB products that support the staff's preparation of estimates and the military decisionmaking process. (See FM 2-01.3.)

INTELLIGENCE PREPARATION OF THE BATTLEFIELD PROCESS

3-1. The G-2/S-2 staff element is the proponent for intelligence preparation of the battlefield (IPB); however, the entire staff participates in the process. The IPB process consists of four steps that are performed or assessed and refined continuously to ensure IPB products remain complete and relevant, and the commander receives intelligence support during current and future operations. The four steps are—

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat courses of action (COAs).

STEP 1—DEFINE THE OPERATIONAL ENVIRONMENT

3-2. Step 1 of the IPB process focuses the unit's initial planning efforts and the remaining steps of the IPB process. The G-2/S-2 leads the staff in identifying characteristics of the area of operations (AO) and area of interest (AOI). The AO's and AOI's effects on friendly and threat operations as well as the local population, require in-depth evaluation. See table 3-1 (page 3-2) and figure 3-1 (page 3-3).

3-3. There are multiple operational environments, and the analysis of any operational environment is a resource-intensive analytical task. The operational environment for each campaign or major operation is different, and it evolves as each campaign or operation progresses. The operational variables (political, military, economic, social, information, infrastructure, physical environment, and time—PMESII-PT) and the mission variables (mission, enemy, terrain and weather, troop and support available, time available, and civil considerations—METT-TC) are used across the different echelons to describe each operational environment. The Army uses the ASCOPE (areas, structures, capabilities, organizations, people, and events) characteristics to describe civil considerations as part of the mission variables (METT-TC) during IPB and mission analysis.

Table 3-1. Step 1—Define the operational environment

G-2/S-2 considerations
Task—Identify significant characteristics of the environment.
Identify for further analysis in step 2: **Enemy.** Identify enemy forces anticipated during the operation— • Location. • Mobility. • General capabilities. • Weapon ranges. **Terrain.** Coordinate with the geospatial engineer teams to ensure the required products are being developed and refined regarding— • Hydrological data. • Elevation data. • Soil composition. • Vegetation.
Task—Identify significant characteristics of the environment.
Weather (terrestrial and spatial). Coordinate with the weather specialty team to ensure the required products are being developed and refined regarding— • Visibility. • Wind velocity. • Precipitation. • Cloud cover. • Temperature. • Humidity. • Atmospheric pressure (as required). **Civil considerations.** Six characteristics expressed in the memory aid ASCOPE (see figure 3-1): • ***A***reas. • ***S***tructures. • ***C***apabilities. • ***O***rganizations. • ***P***eople. • ***E***vents.
Task—Identify the limitations of the command's AO.
• If not determined by the higher headquarters, the G-2/S-2 coordinates with the G-3/S-3 to develop a recommendation on the AO for the commander's approval and submission to higher headquarters. • The G-3/S-3, in coordination with the G-2/S-2, assigns AOs to subordinate units.
Task—Establish the limits of the area of influence and the AOI.
Area of influence— • Is determined by both the G-2/S-2 and the G-3/S-3. • Includes geographical areas where a commander is directly capable of influencing operations by maneuver and fire support systems. **AOI**— • Is established by the commander with input from the G-2/S-2 and G-3/S-3. • Is an area normally larger than the area of influence and may require more ISR assets to monitor. • May include staging areas.
Task—Evaluate existing databases and identify intelligence gaps.
The G-2/S-2 staff— • Conducts data mining via the DCGS-A to determine intelligence gaps using national, multinational, joint, and higher echelon databases. • Identifies and prioritizes the gaps in the current holdings. • Once approved by the commander, these gaps become the commander's initial intelligence requirements.
Task—Initiate collection of information required to complete IPB.
To fill the intelligence gaps— • The G-2/S-2 and G-3/S-3 initiate collection. • The G-2/S-2 submits RFIs.
AO—area of operations AOI—area of interest DCGS-A—Distributed Common Ground System-Army IPB—intelligence preparation of the battlefield ISR—intelligence, surveillance, and reconnaissance RFI—request for information

Areas	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
Tribes	Cemeteries	Sewer	Tribal	Phones	Weddings
Family or clans	Religious shrines	Water	Family or clans	Speeches	Birthdays
Ethnicity	Houses of worship	Electrical	Religious	Face-to-face meetings	Religious gatherings
Religion	Bars and tea shops	Academic	Ethnic	Media—radio	Funerals
Economic districts	Social gathering places	Trash	U.S./multinational forces	Media—television	Major religious events
Smuggling routes	Print shops	Medical	Governmental agencies	Media—print	Anniversaries of wars and battles
National boundaries	Internet cafes	Security	Farmers or merchants	Visual—graffiti, signs	Birthdays or remembrances
Social class—rich, middle, poor	Television stations	Market (use and controls)	Community organizations	Visual—videos, DVDs	Harvest of plantings
Political districts	Radio stations	Employment and commerce	Military and militia units	Audio—pirated or illegal radio	Reconstruction openings
Military districts	Hospitals	Crime and justice	Illicit organizations	Rallies or demonstrations	Town council meetings
School districts	Banks	Basic needs	Insurgent groups	Restaurants	Elections
Road systems	Dams	Public health	Gangs	Door-to-door	Sports events
Water sources	Gas stations	Religion	Nomads	Sports	
Construction sites	Military barracks	Displaced persons and refugees	Displaced persons and refugees	Religious gatherings	
Gang territory	Jails	Political voices	Volunteer groups	Parks	
Safe areas and sanctuaries	Water pumping stations	Civil rights, individual rights	Intergovernmental organizations	Family gatherings	
Trade routes	Oil and gas pipelines		Political	Gas lines	
Power grids	Water lines		Contractors	Bars and tea shops	
	Power lines		Nongovernmental organizations	Food lines	
	Storage facilities		Labor unions	Job lines	
	Electric substations		Indigenous groups	Speaking to reporters	

Figure 3-1. Examples of ASCOPE characteristics

STEP 2—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

3-4. In this step of the IPB process, the G-2/S-2 analyzes the environmental effects with which U.S. forces, multinational partners, threats, and local population must contend. (See table 3-2.)

Table 3-2. Step 2—Describe environmental effects on operations

G-2/S-2 considerations
Task—Analyze the environment.
The G-2/S-2— • Analyzes the effects of the terrain, weather, and civil considerations with which U.S. forces, multinational partners, threats, and noncombatants have to contend. • Identifies the limitations and opportunities the environment offers to potential operations of friendly and threat forces as well as the local population. • Focuses the analytic effort on the general capabilities of each force until COAs are developed in later steps of the IPB process.
Task—Describe the environmental effects on threat and friendly capabilities and COAs.
Working with the geospatial engineer team and weather specialty teams, the G-2/S-2 section produces the following noninclusive list of products during step 2 of the IPB process. (See paragraphs following table 3-3 [page 3-7].): • Integrated products such as the MCOO. • Overlays that depict the military aspects and effects of terrain include— ▪ LOCs. ▪ Line of sight. ▪ Imagery. ▪ Urban terrain. ▪ Key infrastructure. ▪ Congregation and mass assembly points overlays. • Weather analysis matrices and graphic displays. • Population status overlays.
COA—course of action IPB—intelligence preparation of the battlefield LOC—line of communication MCOO—modified combined obstacle overlay

3-5. To achieve desired step 2 results, develop the following products as appropriate to the situation:

- Modified combined obstacle overlay (MCOO).
- Line of communications overlay.
- Line of sight overlay.
- Imagery overlay.
- Urban terrain overlay.
- Key infrastructure overlay.
- Weather analysis matrices and graphic displays.
- Congregation and mass assembly points overlay.
- Population status overlays.

MODIFIED COMBINED OBSTACLE OVERLAY

3-6. Figure 3-2 depicts an example MCOO. The MCOO fuses the—

- Combined obstacle overlay.
- Avenue of approach (AA) overlay with mobility corridors.
- Operational graphics.
- Key terrain.
- Known threat objectives into a comprehensive terrain product.

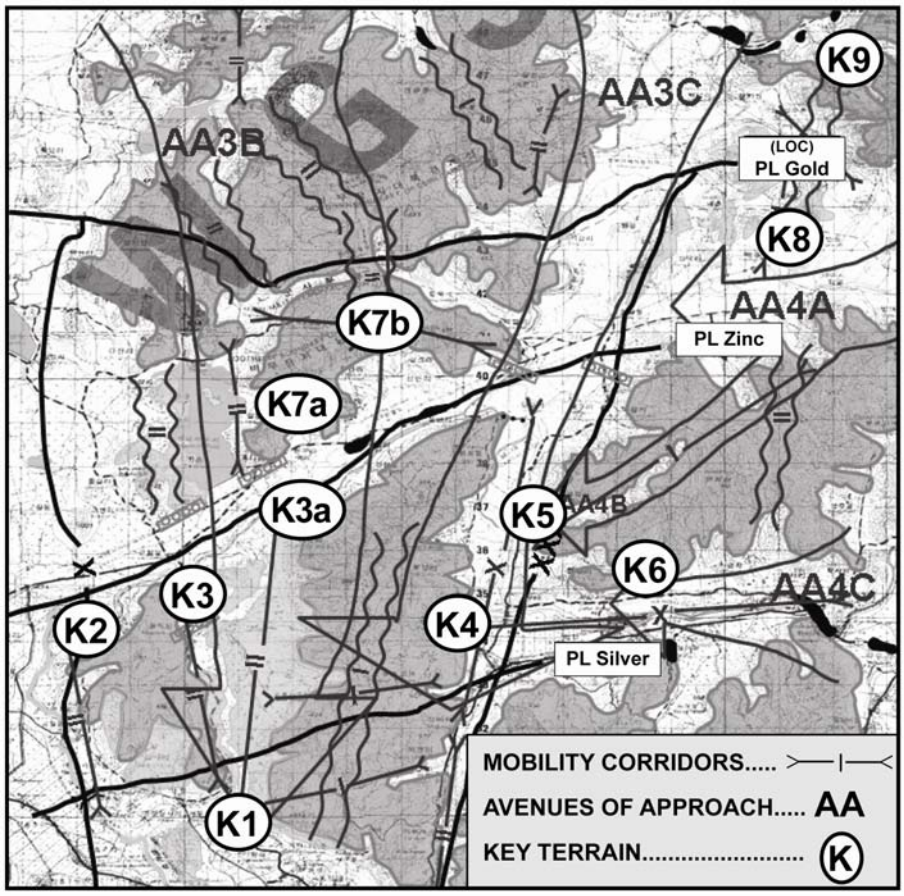


Figure 3-2. Example modified combined obstacle overlay

LINE OF COMMUNICATIONS OVERLAY

3-7. The line of communications (LOC) overlay depicts major LOCs within and around an AO. The LOC overlay—

- Includes roads, airfields, mountain passes, waterways, and footpaths.
- Includes pertinent data, such as road widths, their load capacity, sharp turns, potential ambush positions, potential sniper positions, and overhanging obstacles.
- Provides mobility information to assist planners and operators determine what personnel and equipment can move along the mobility corridors.
- In urban operations, depicts normal traffic conditions that help the unit determine the best times to operate and provide an indicator of an unusual event.
- With local water systems can list important items, such as the width and depth of the waterway, key crossing sites (depending on the size of the waterway), and key uses of that waterway (for example, commerce, water source for crops, drinking water source for the local population).

LINE OF SIGHT OVERLAY

3-8. The line of sight overlay is particularly important in complex terrain. This overlay—

- Can help define AAs to an objective.
- 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.

Note. **Reverse line-of sight** overlays, which show the friendly AAs from the enemy standpoint, are just as important as line of sight overlays. The enemy can be expected 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.

IMAGERY OVERLAY

3-9. 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, 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.

3-10. Distributed Common Ground System-Army (DCGS-A) provides the G-2/S-2 access to tactical, theater, and national imagery systems as well as the Image Processing Library. Data collected from such sources is transferred in digital format that can be manipulated to address specific requirements.

3-11. Advanced geospatial intelligence (GEOINT) 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. Combining imagery with digital terrain elevation data presents an oblique perspective. Spectral imagery accomplishes 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

3-12. Urban terrain overlays depict specific aspects of terrain unique to the urban environment, for example—

- Details of a single building, a group of buildings, a section of an urban area, or even an entire urban area.
- Different terrain zones apparent in an urban area. Different types of terrain can 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 (see FM 3-06.11), 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.
- A building type overlay that depicts particular types of buildings, such as industrial, government, and military buildings, residential areas, businesses, warehouses or storage buildings, religious centers, or media locations. Each building can be numbered or otherwise identified depending on the needs of the commander and the commander's staff.
- Entire sections of a city can be marked depending on the customary type of construction in a particular area. For example, an area of dense construction or a shantytown can be identified by appropriately labeling it on an overlay or directly onto an aerial photograph.
- Shantytowns may require highlighting because they may be areas with notable food shortages and disease and pollution are most prevalent. They may lack public utility infrastructure (for example, plumbing and electricity). Buildings are often constructed from miscellaneous materials, and there is no consistent pattern of streets or corridors, which can complicate military operations. These types of conditions result in a generally dissatisfied population—a potential source of unrest.

- Unoccupied locations or buildings should be identified, since 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 to quell an increasingly worrisome civil disturbance. Additionally, unoccupied locations or buildings could be storage or meeting sites for threat forces.
- Depicting street widths in terms of major weapons systems can help identify formations or routes that are most advisable for an area. Streets that allow two Abrams tanks to advance, side by side, enable the vehicles to better cover upper floors on opposite sides of the street, thereby providing security for each other. In addition, 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

3-13. The key infrastructure overlay is a group of products rather than a single product. (See table 3-3.) These overlays can be produced by using—

- A map.
- Aerial photography.
- A graphic design that is appropriately marked with a numbering or color-coded system that indicates the type of asset as well as its specific attributes.

Table 3-3. Key infrastructure overlay

Critical infrastructure. Anything that, if harmed, can affect the living conditions of the population.
• Electricity generation plants. • Government buildings. • Hydroelectric dams. • Oil pumping stations. • Police stations. • Public markets. • Pumping stations. • Sewage treatment plants. • Water purification plants.
Protected urban terrain. Areas that should not be destroyed, attacked, or occupied, or that have other use restrictions based on international treaties, rules of engagement, and common sense.
• Schools. • Hospitals. • Areas with large amounts of phone and/or electrical wiring. • Buildings with many stories.
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.
Media facilities include locations of—
• Transmission stations. • Transmission antennas. • Newspaper production. • Distribution sites. • Television stations. • Radio stations.
Transportation facilities include locations of—
• Rail hubs. • Major bus connection sites. • Freeways. • Subway lines. • Major thoroughfares and intersections that are significant to the operation.

Table 3-3. Key infrastructure overlay (continued)

Resource sites. The resources and infrastructure used to support the critical resource needs of a population such as—
• Building material locations. • Car lots. • Appliance warehouses. • Petroleum and natural gas processing plants.
Culturally significant structures such as—
• Places of religious worship (for example, churches, temples, mosques). • All relevant government and internationally significant buildings (for example, embassies, consulates). • War memorials.
Dangerous facilities
• Structures with known chemical, biological, or incendiary features. • Toxic industrial material sites such as pharmaceutical plants, oil refineries, or fertilizer plants. • Ammunition storage sites.
Key subterranean infrastructure
• Underground railways. • Any other underground feature of significance for the operation. • Sewer systems. • Underground electrical wiring.

WEATHER ANALYSIS MATRICES AND GRAPHIC DISPLAYS

3-14. 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 G-2/S-2 should collaborate with the weather specialty team to develop weather products that depict weather effects—

- On friendly operations.
- On enemy operations.
- That are common to both friendly and enemy operations.

3-15. Figure 3-3 exemplifies a weather effects matrix and figure 3-4 exemplifies a weather impact chart.

	Weather Effects								
Operation	***06-09***	***09-12***	***12-15***	***15-18***	***18-21***	***21-24***	***00-03***	***03-06***	***Comments***
EAC reconnaissance									• Transitional period between northeast and southwest monsoons. • Northeast monsoons provide favorable weather for operations with decreased rain and thunderstorms. • During the transitional period tropical cyclone frequency increases.
Tactical reconnaissance				**C**	**C**	**C**			
UAS—Hunter				**C**	**C**	**C**			
UAS—Predator				**C**	**C**	**C**			
Ground reconnaissance									
Armor maneuverability				**P**	**P**				
Infantry maneuverability				**P**	**P**				
Helicopter, CAS (A-10), C-130 (non-AWADS)									
CAS (Non-A-10)									
C-130 (AWADS)									
Artillery									
Air defense									
Engineers				**P**	**P**				
Laser or thermal operations			**P**	**P**	**P**				
MOPP IV		**T**	**T**	**T**	**T**	**T**	**T**	**T**	

▢—moderate degradation **T**—temperature **V**—visibility **C**—ceiling
▢—severe degradation **W**—wind **P**—perception

Figure 3-3. Example weather effects forecast matrix

Next 24 Hours		Area of Operations Forecast Overview	September	13	14	15	16
Alexandria		• Next 72 hours: 20% chance of thunderstorms in the vicinity of Alexandria and Baton Rouge. • Tropical Storm Ophelia. • Average rainfall expected to be 6 – 10 inches. • 70 mph winds. • Widespread flooding not expected.	Alexandria				
	Partly Cloudy 71/95		Rotary				TS
			Convoy	T	T	T	T
			Communications				TS
New Orleans			New Orleans				
	Partly Cloudy 71/95		APOD				
			Rotary				
			Convoy	F	F	F	F
			Communications				
			Troops	T	T	T	T
Baton Rouge			Baton Rouge				
	Sunny 70/95		APOD				TS
			Rotary				TS
			Convoy	T	T	T	T
			Communications				TS

Date	13 September	14 September	15 September	16 September
Forecast	 Sunny	 Partly cloudy	 Partly cloudy	 Partly cloudy
Low/High	69/91	69/91	71/91	71/90
Wind Direction Speed	 V 0 – 5 mph	 SW 0 – 5 mph	 SW 0 – 5 mph	 V 0 – 5 mph

APOD—aerial port of debarkation
F—flooding
mph—miles per hour
SW—southwest
T—temperature
TS—thunderstorm
V—visibility
W—wind

Figure 3-4. Example weather impact chart for civil support operations

CONGREGATION AND MASS ASSEMBLY POINTS OVERLAY

3-16. Congregation and mass assembly point overlays depict the numbers, types, and locations of sites where a large number of people can be gathered for demonstrations, protection, or feeding in the event of a disaster. 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. These sites include—

- Places of religious worship.
- Parks.
- Schools.
- Restaurants.
- Town squares.
- Recreational centers.
- Sports facilities.
- Entertainment centers.

POPULATION STATUS OVERLAYS

3-17. 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 (see figure 3-5) such as—

- Age.
- Religion.
- Ethnicity.
- Tribal affiliation.
- Income.
- Population dispersal variances (day versus night)—identifying possibly restrictive operating conditions or revealing times that are most conducive for the completion of a given mission.

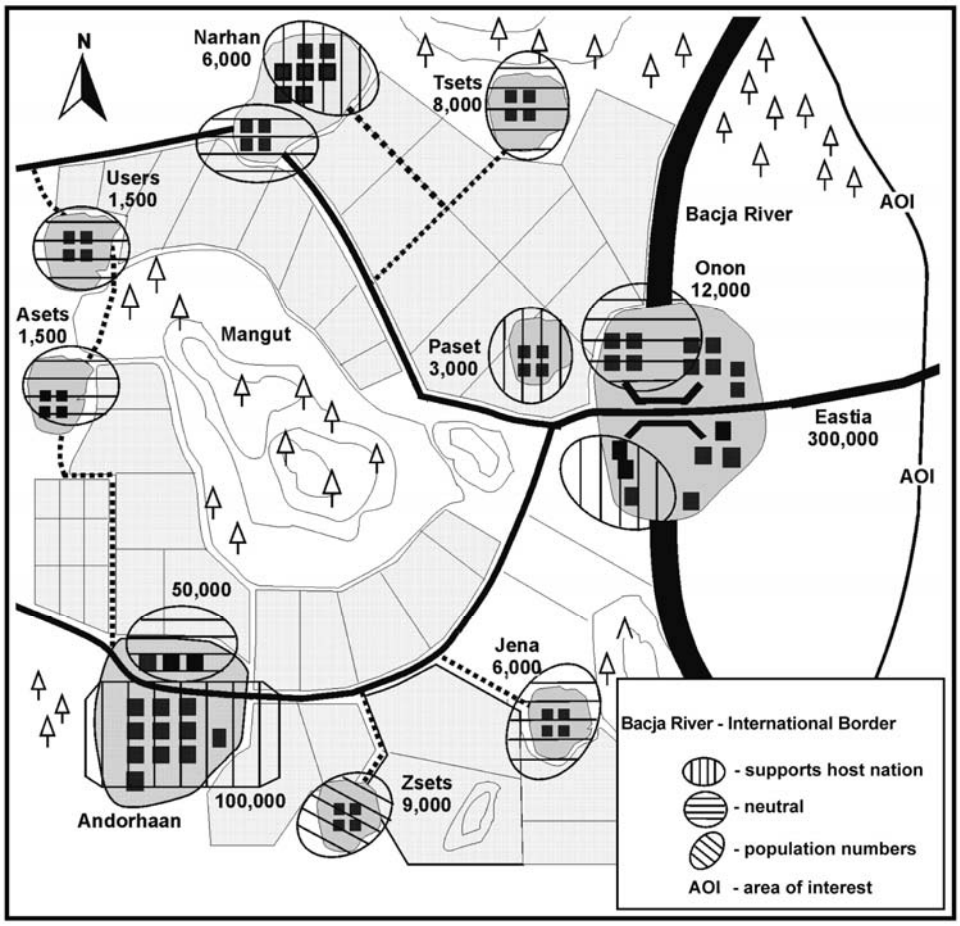


Figure 3-5. Example population status overlay

3-18. Some of the benefits of population status overlays—

- Help determine possible sources of friction (that can exist between groups).
- Identify the population or location in greatest need of a certain activity or asset.

3-19. Methods of constructing population status overlays include—

- Color-coding sections of an AO-based on the area's populations.
- Dividing the AO into specific areas such as the same service or political boundaries used by local authorities—local police precincts, municipal districts, or counties—that can help clarify

the situation and aid in coordination efforts with the local authorities. Inserting pie charts for each AO shows each group and numbers or percentages.

STEP 3—EVALUATE THE THREAT

3-20. In step 3, the G-2/S-2 and staff analyze the command's intelligence holdings, which they identified in step 1, to determine how the threat normally conducts operations under similar circumstances. When operating against a new or less-defined threat, the G-2/S-2 may need to develop or expand intelligence databases and threat models concurrently. To accomplish this, the G-2/S-2 should conduct threat characteristic (previously order of battle [OB] factors) analysis for each group identified in step 1. See table 3-4 for threat characteristic examples and table 3-5 (page 3-12) for G-2/S-2 considerations for step 3 of the IPB process.

Table 3-4. Threat characteristics

Threat characteristic	***Considerations***		
Composition	Regular Army Unit history Type of unit	Militia Uniforms	Unit designation Insignia
Disposition	Historic	Current	Proposed future
Tactics	Method of operations Conventional Terrorism	Intent Unconventional	Propaganda Asymmetrical
Training	Individual Source of training Specialized training	Team Uniforms	Unit Insignia
Sustainment	Food Spare parts Maintenance status	Transportation Water	Fuel Ammunition
Operational effectiveness	Strength Morale Equipment	Goals Weapons Chain of command	Personnel Leadership Loyalty
Communications	Written Verbal and live drops Electronic	Internet Emitter type	Signal Frequency range
Intelligence	Surveillance Reconnaissance	Countersurveillance EW capability	Deception
Recruitment	Local International Motivation	National Coercion	Regional Volunteers
Support	Financial National International	Media Regional Popular	Local Religious Tribal/Ethnic
Reach	Databases Architecture	Assets Access	Connectivity Informal networks
National agencies	Loyalties Capabilities	Agenda Relationships	Leadership
Law enforcement agencies	Loyalties Capabilities	Agenda Relationships	Leadership
IAs and NGOs	Loyalties Capabilities	Agenda Relationships	Leadership AO
Personality	Key leaders	Education level	Idiosyncrasies
Other aspects	Natural diseases Chemical hazards Criminal activity	Biohazards Wildlife	Radiological Toxic industrial material

AO—area of operations
EW—electronic warfare
IA—international agency
NGO—nongovernmental organization

Table 3-5. Step 3—Evaluate the threat

G-2/S-2 considerations
Task: Update or create threat models
Analyze the unit'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 G-2/S-2 can rely on historical databases and well-developed threat models. • When operating against a new or less well-known threat, the G-2/S-2 may need to develop intelligence databases and threat models concurrently. Convert threat doctrine or patterns of operations into graphics such as— • Threat templates. (See figures 3-6 through 3-9 [pages 3-13 through 3-15].) • Incident overlays. (See figure 3-10 [page 3-16].) • Pattern analysis plot charts. (See figure 3-11 [page 3-16].) • Time event charts. (See figure 3-12 [page 3-17].) • Association, relationship, and activities matrices. (See figures 3-13 through 3-16 [pages 3-18 through 3-21].) Describe the threat's tactics and options. Identify HVTs and HPTs.
Task: Identify threat capabilities
Define the capabilities with the use of statements. The following are examples of capability statements: • "The threat has the capability to attack with up to eight divisions supported by 150 daily sorties of fixed-wing aircraft." • "The criminal organization has the ability to pay off local law enforcement agencies." • "The terrorists have the capability to send destructive viruses over the Internet, which can destroy computer files and archives." • "The threat can establish a prepared defense by 14 May." • "The terrorists have the capability to use CBRNE." • "The drug smugglers have the ability to conduct three drug-smuggling operations simultaneously." • "The terrorists have the ability to conduct multiple car bombings simultaneously." • "The threat has the ability to target friendly convoys along main supply routes using remotely detonated IEDs." Other capabilities include supporting COAs (attack, defend, reinforce, retrograde), specific types of operations, or operations that allow the threat force to use a COA that is usually unavailable or would be severely hindered if the supporting operations were not conducted. Examples of these types of operations include— • Use of CBRNE weapons. • Intelligence collection. • EW operations. • Use of air assets (fixed and rotary). • Engineering operations. • Air assault or airborne operations. • Amphibious operations. • River operations. • Propaganda. • Deception operations. • Car bombings, bomb scares, and suicide bombers. • Raids on weapon storage facilities. • Carjacking or hijacking of vehicles used in transporting personnel, weapons, and drugs. • Theft of chemicals related to drug manufacturing. • Threat to IO.
CBRNE—chemical, biological, radiological, nuclear, high-yield explosives COA—course of action EW—electronic warfare HPT—high-payoff target HVT—high-value target IED—improvised explosive device IO—information operations

3-21. To achieve desired step 3 results, develop the following key products as appropriate to the situation:

- Threat template.
- Incident overlay.
- Pattern analysis plot sheet.
- Time event chart.
- Association matrix.
- Relationship matrix.
- Activities matrix.
- Link diagram.
- Cultural comparison chart.
- Perception assessment matrix.

THREAT TEMPLATE

3-22. Threat templates (see figures 3-6 through 3-9 [pages 3-13 through 3-15]) are tailored to the needs of the unit or staff section creating them, for example:

- Some threat templates consider the threat forces as a whole.
- Others focus on a single warfighting function, such as intelligence or fires, while other products depict pattern analysis, time event charts, and association matrices.

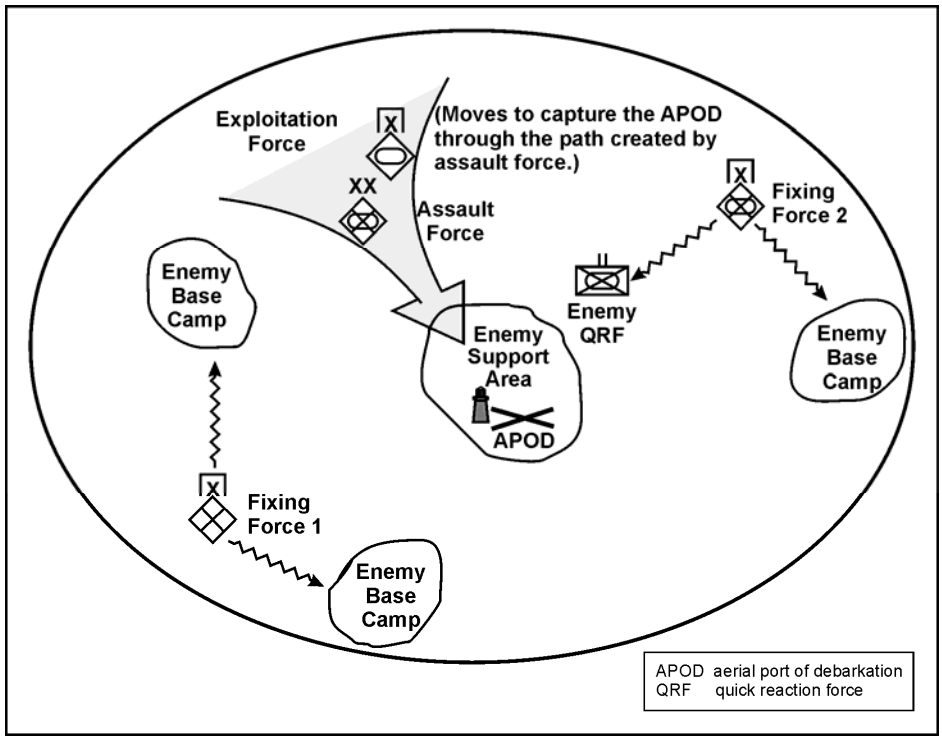


Figure 3-6. Example offensive threat template

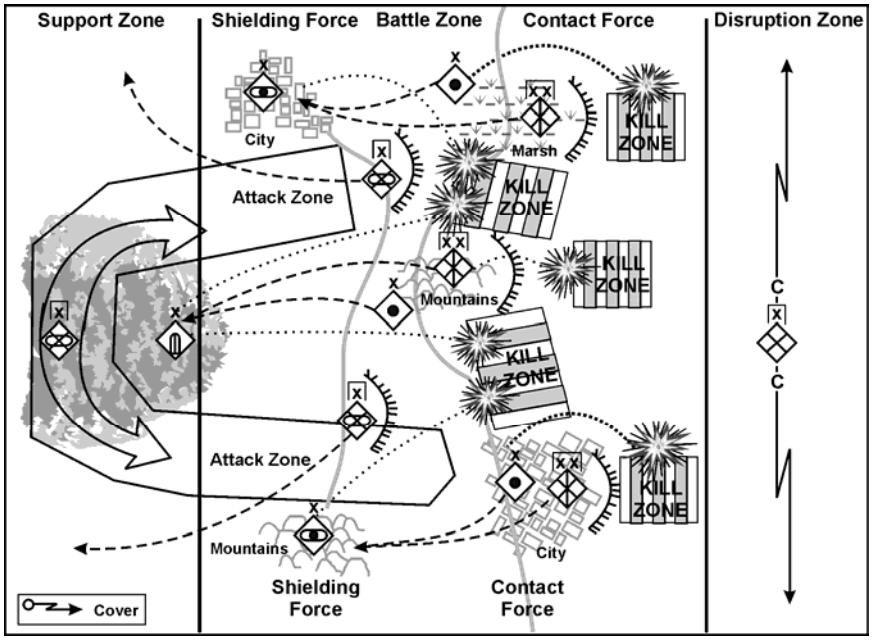


Figure 3-7. Example defensive threat template

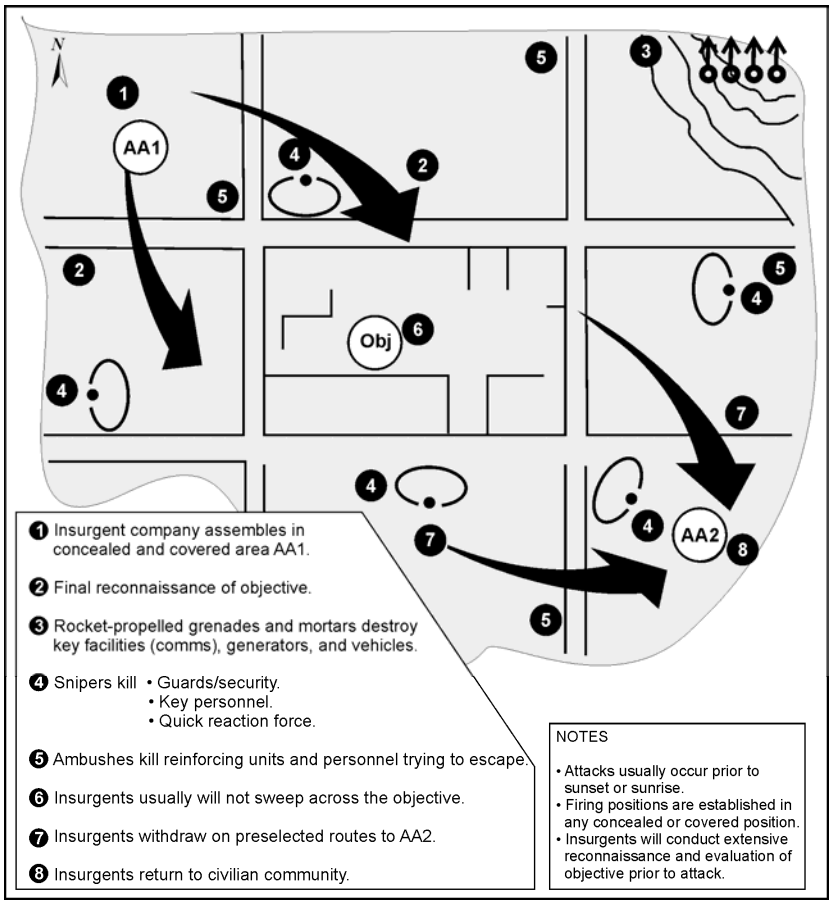


Figure 3-8. Example threat template for attacks on facilities or base camps

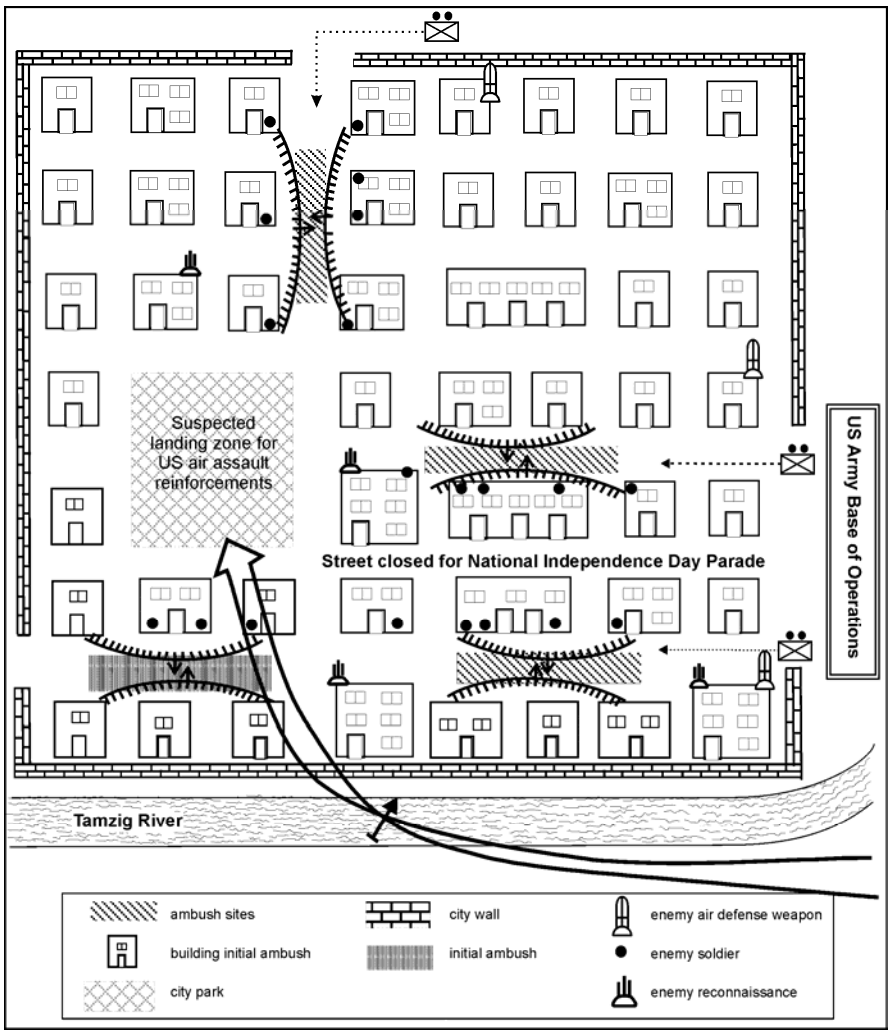


Figure 3-9. Example threat template in an urban environment

INCIDENT OVERLAY

3-23. Figure 3-10 (page 3-16) is an example of an incident overlay illustrating cumulative events that have occurred within the AO and focuses on the "where" of an event. The incident overlay—

- May be created in multiple layers to focus on different subjects or as a single overlay to blend subjects.
- Normally includes additional information such as notes or graphics.
- Should be used in conjunction with the pattern analysis plot sheet.

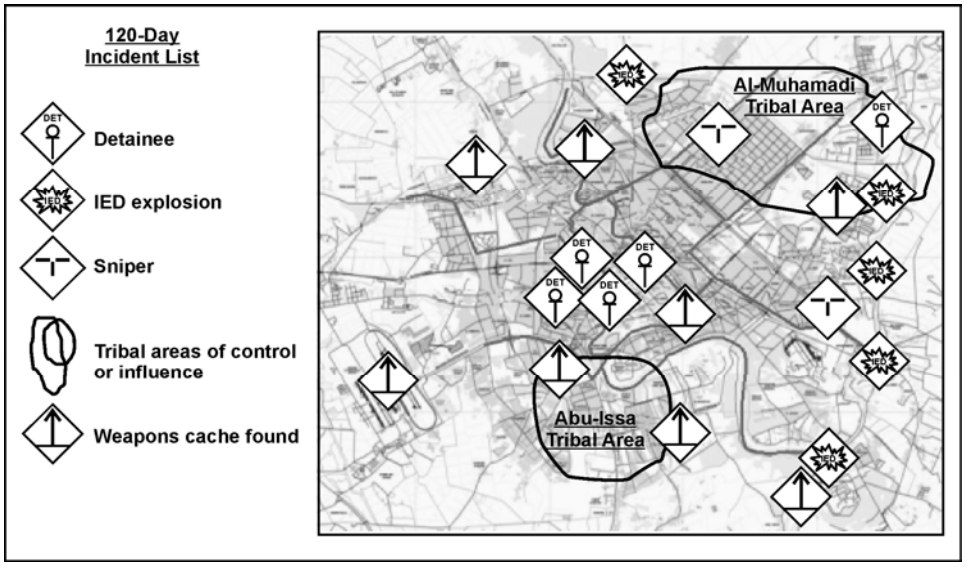


Figure 3-10. Example incident overlay

PATTERN ANALYSIS PLOT SHEET

3-24. The analyst uses the pattern analysis plot sheet (see figure 3-11) 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 activities that are tied to particular days, dates, or times.
- Supplies the bulk of the data needed to complete an event template, when used in conjunction with the incident overlay and any threat templates.

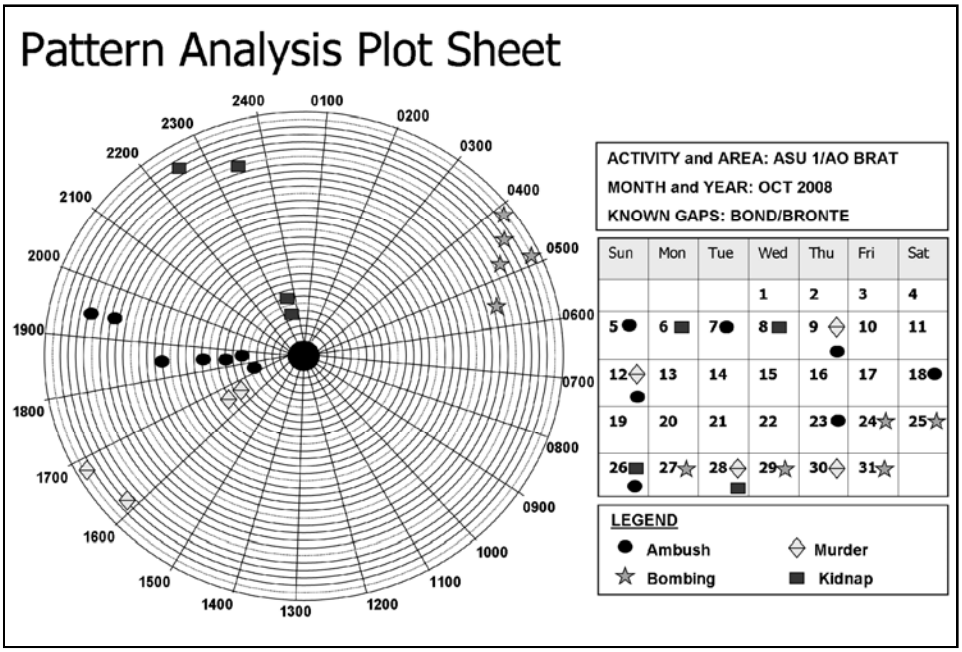


Figure 3-11. Example of a pattern analysis plot sheet

TIME EVENT CHART

3-25. Time event charts are chronological records of individual or group activities designed to store and display large amounts of information in a small space. (See figure 3-12.) The time event chart helps analyze larger-scale patterns of activity and relationships. Characteristics of time event charts include—

- Triangles representing the beginning and end of the activity.
- Rectangles representing other events.
- "Xs" through noteworthy events.
- Triangles and rectangles, each with a sequence number and date.
- Brief descriptions of each event below each rectangle.
- Arrows representing time flow from the left to the right, for each row employed.

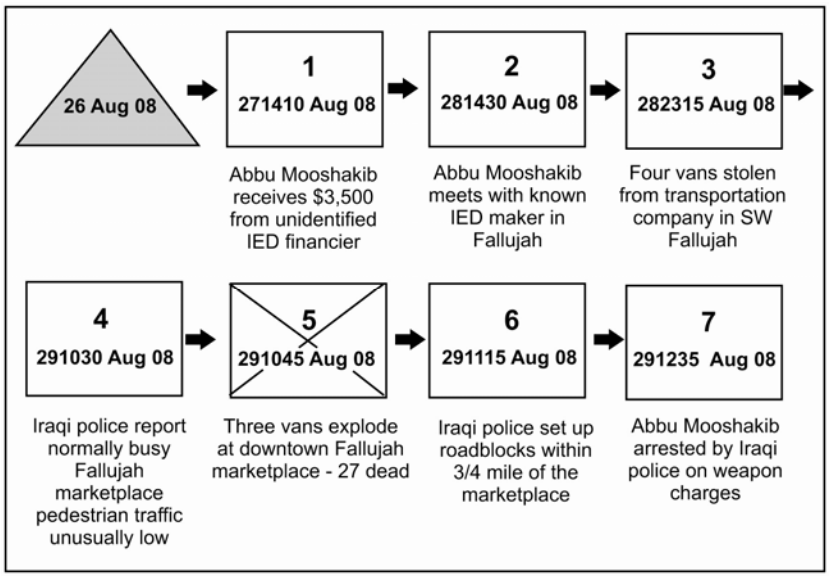


Figure 3-12. Example time event chart—Southwest Asia

ASSOCIATION MATRIX

3-26. The association matrix (see figure 3-13 [page 3-18])—

- Is used to establish the existence of an association, known or suspected, between individuals.
- Depicts "direct connections," for example, face-to-face meetings or confirmed telephonic conversations.
- Can be used to identify those personalities and associations needing a more in-depth analysis to determine the degree of relationship, contacts, or knowledge between the individuals.
- Helps form the structure of the threat organization as connections between personalities are made.

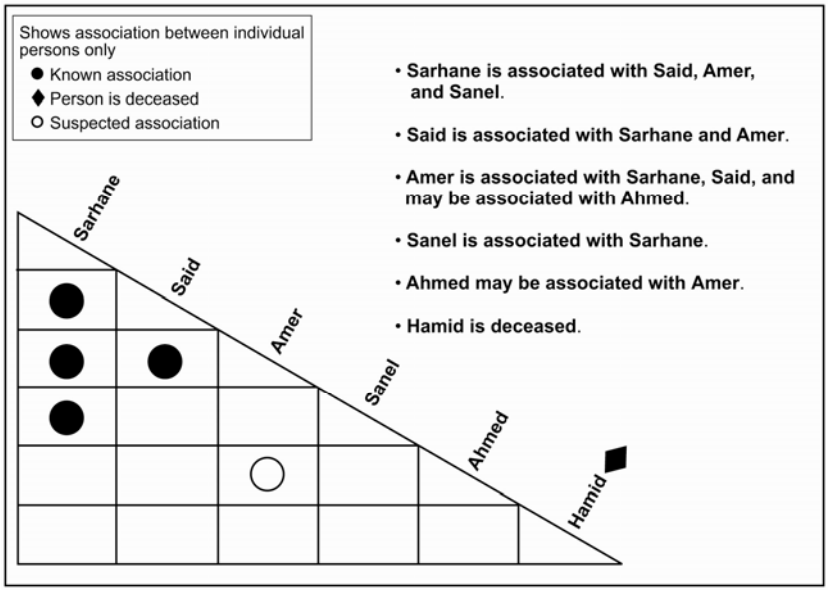


Figure 3-13. Example association matrix

RELATIONSHIP MATRIX

3-27. Relationship matrices depict the nature of relationships between elements of the AO. The nature of the relationship between two or more components includes measures of contention, collusion, or dependency. This tool demonstrates graphically how each component of the city interacts with the others and whether these interactions promote or degrade the likelihood of mission success. The elements can include—

- Members from the noncombatant population.
- The friendly force.
- International organizations.
- Adversarial groups.
- Utility infrastructure.
- Significant buildings.
- Media.

3-28. Figure 3-14 depicts the relationships among a representative compilation of population groups. This example is an extremely simple version of what might be used during an operation with many actors and other population elements. For instance, the section marked "Population" might include considerably more population subgroups than the two included in figure 3-14. 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, which could also be used to depict the perceived differences in relationships. For example, in figure 3-14, "Political Group 3" has 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.

3-29. 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.

Example

As an example, consider communist leaders who control the electricity supply. These leaders use the infrastructure at their 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.

3-30. Figure 3-14 depicts a possible collusion relationship between the Government and Political Group 3, and a friendly relationship between the Government and the Media. Listed are questions an intelligence analyst might ask when reviewing this information:

- 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?

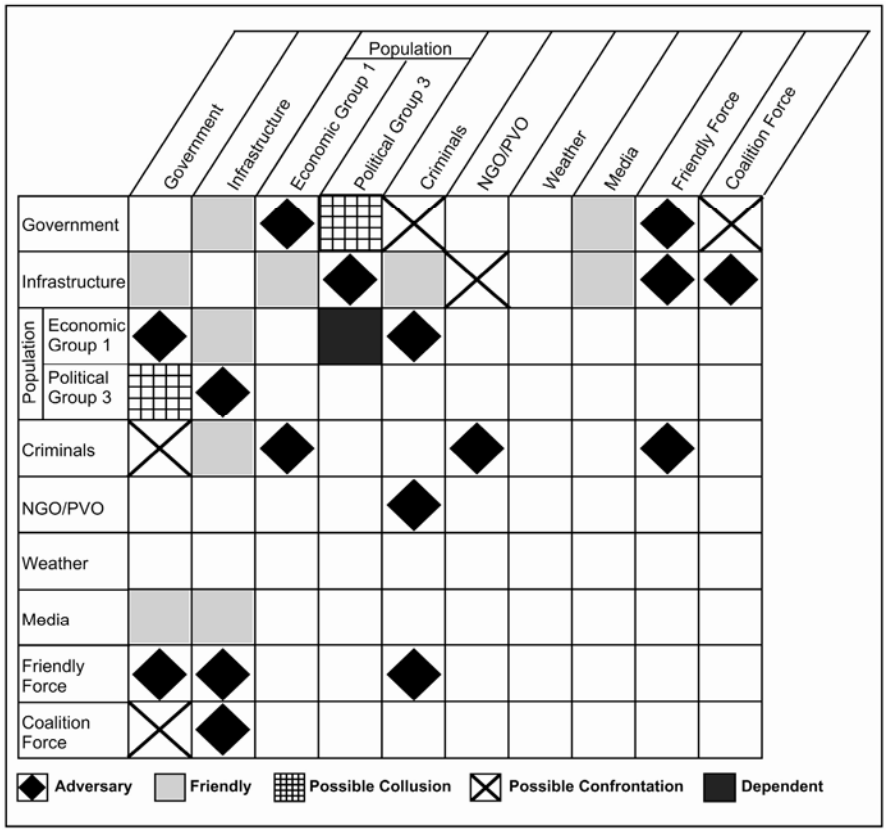


Figure 3-14. Example relationship matrix

ACTIVITIES MATRIX

3-31. Activities matrices—

- Help connect individuals (such as those in association matrices) to organizations, events, entities, addresses, and activities—anything other than people.
- When combined with information from association matrices, assists in linking personalities as well.

3-32. The activities matrix is constructed as a rectangle with rows and columns tailored to the needs of the analyst exemplifying the problem at hand. (See figure 3-15.)

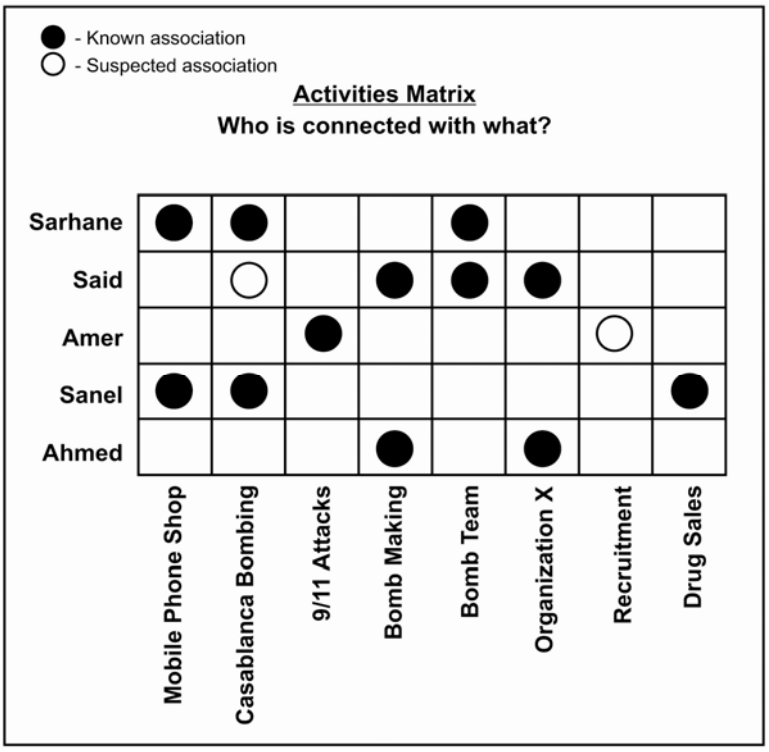


Figure 3-15. Example activities matrix

LINK DIAGRAM

3-33. A link diagram—

- Combines the association, relationship, and activities matrices into a single graphic.
- Depicts how individuals and their functional groups are related.
- When analyzed, helps determine intelligence gaps.

3-34. Figure 3-16 depicts a link diagram with a timeline of a train bombing in Madrid, Spain.

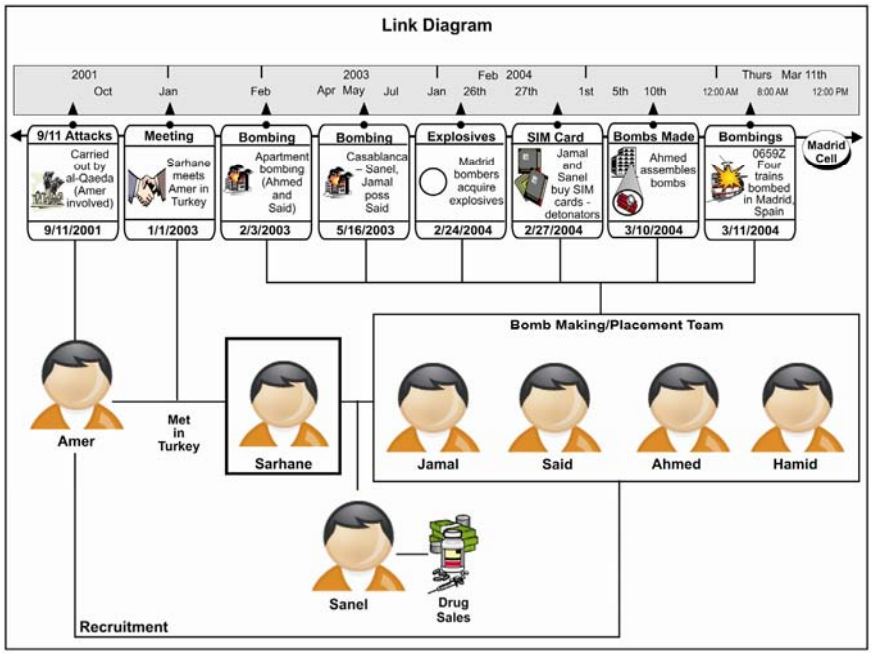


Figure 3-16. Example link diagram

CULTURAL COMPARISON CHART

3-35. A cultural comparison chart (see table 3-6):

- Is used to deter the idea 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, regional populace interests, and U.S. norms.
- Can be a stand-alone tool—listing the characteristics of the culture in question—or it can be comparative—assessing the host country population relative to known and familiar conditions.

Table 3-6. 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 situations. The same rules apply to everyone in similar situations. • **Particularists** believe one's behavior, in any given situation, depends on specific circumstances.	***Universalist*** Right is right and wrong is wrong. Treat everyone alike. Everyone has the same rights.	***Particularist*** Right and wrong are situation dependent. Life is not fair. Exceptions are 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 very 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.

PERCEPTION ASSESSMENT MATRIX

3-36. Friendly force activities intended as benign or benevolent might have negative consequences if a population's perceptions are ignored, yet assessed or measured. Perceptions—more than reality—drive decisionmaking and consequently could influence the reactions of entire populations.

3-37. Perception assessment matrices—

- Are often used by psychological operations (PSYOP) personnel.
- Can be a valuable tool for intelligence analysts once completed by trained PSYOP personnel.
- Provide some measure of effectiveness for the unit's ability to reach an effect (for example, maintain legitimacy) during an operation. The matrix can also be used to directly measure the effectiveness of the unit's civil affairs, public affairs, and PSYOP efforts.

Example

One proposed PSYOP program developed for Operation Restore Democracy in Haiti illustrates why perception assessment is necessary. Before deployment, published leaflets informed the Haitian populace of U.S. intentions. The original leaflet was published in French—the language of the Haitian elite. The leaflet 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 a wider audience. If the French leaflet had been dropped on Port-au-Prince, it could have undermined the U.S. mission in many ways. The majority of the population would have been unable to read the leaflet. The subsequent deployment of U.S. forces into the Haiti could have been perceived as hostile. The mission, which was intended, in part, to restore equity within the Haiti's social structure, could have backfired if the Haitians viewed the French leaflet as an indication of U.S. favoritism to the Haitian elite.

3-38. Perceptions can counter operational objectives; therefore, they should be assessed before and throughout an operation. Although it is impossible to read the minds of the local population, there are several means to measure the perceptions:

- Demographic analysis and cultural intelligence are key components of perception analysis.
- Understanding a population's history can help predict expectations and reactions.
- Human intelligence (HUMINT) can provide information on population perceptions.
- Reactions and key activities can be observed to decipher whether people behave 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.

3-39. Perception assessment matrices aim to measure the disparities between friendly force actions and population groups' perceptions. (See figure 3-17.) In addition to assessing each population group's perceptions, it might benefit the unit to assess its own perceptions of its activities. The unit should address the following questions to scrutinize its view of an operation:

- Are members of the unit exhibiting decidedly Western or American values that are not appreciated by the host-nation population?
- Are embedded U.S. beliefs preventing the unit from understanding the host-nation population or its multinational partners?
- Are the intelligence and command staffs' perceptions of the AO valid?
- Does the population believe what the unit believes?
- Can the population's (or a subgroup's) perception be detrimental to the unit?

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

Figure 3-17. Example perception assessment matrix

STEP 4—DETERMINE THREAT COURSES OF ACTION

3-40. The intelligence analyst describes the threat's intentions verbally, graphically, and in writing. An effective understanding and presentation of the threat's COA may be accomplished by developing a doctrinal narrative. Narratives describe the tasks the threat will accomplish during operations, and describe other factors that will affect the threat's intentions during operations. Narratives answer the questions—"What is the threat doing now?" and "What does the threat want to do?" The best technique for developing a doctrinal narrative is analyzing the threat through warfighting functions—movement and maneuver, intelligence, fires, sustainment, command and control (C2), and protection. See table 3-7 for G-2/S-2 considerations during step 4 of the IPB process.

Table 3-7. Step 4—Determine threat courses of action

G-2/S-2 considerations	
Task: Identify the threat's likely objectives and desired end state	
The G-2/S-2 depicts the threat based on the commander's guidance (for example, echelon or cell). Every staff officer possesses specific information the G-2/S-2 can use to piece together the IPB. Staff input to enemy COA development, enemy situation template and event template development are listed below.	
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 is organized to protect its forces. • Evaluate whether the enemy will use air defense in a reconnaissance or a counterreconnaissance role.
Fire support	• Determine where the enemy will deploy mortars or artillery. • Recommend HVTs (developed into HPTs during wargaming). • Anticipate the depth of range of the threat's indirect fires.

Table 3-7. Step 4—Determine threat courses of action (continued)

Engineer	• Determine where the enemy is most likely to emplace conventional (for example, mines) and unconventional (for example, IED) obstacles. • Determine the time— ▪ To emplace each type of obstacle. ▪ To breach or neutralize obstacles. ▪ For an enemy to establish a given level of defensive preparedness. • Determine ability to bridge different river and stream sizes and the time required for each. • Make an initial assessment of effort required for stability assessments, such as building construction.
CBRN	• Determine types of delivery systems, including minimum and maximum ranges. • Appraise threat CBRN protection capabilities. • Provide preparation indicators to employ CBRN weapons. • Predict friendly assets the enemy is likely to consider as HPTs for CBRN targeting. • Analyze existing contaminated areas that may indicate COAs adopted by the enemy.
Signals	• Determine the threat's ability to locate or intercept friendly systems. • Predict the speed at which the enemy can collect, process, and target communications 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.
Civil affairs	• Analyze the political and economic situation in the AO. • Determine what factions are friendly, neutral, or threatening. • Determine who the key leaders are. • Provide the cultural indicators that identify the populace (such as friendly, neutral, anti- or pro-United States). • Predict areas where civilians gather to protest or demonstrate. • Determine from whom or where to obtain information about particular AOs.
Task: Identify the full set of COAs available to the threat	
The **staff** considers— • The COAs that the threat believes are appropriate to the current situation, and the identification of the threat's likely objectives. This requires an understanding of the threat's decisionmaking process, as well as an understanding of the threat's perception of the current situation. • The threat COAs that could significantly influence the unit's mission—for example, diverting combat power to cover increasing protection requirements. • The COAs that may go beyond the boundaries of known threat doctrine or TTP, especially if the known threat is an individual terrorist, a terrorist cell, or a terrorist group. • The threat COAs indicated by recent activities and events. To avoid surprise from an unanticipated COA, consider all possible explanations for the threat's activity with an emphasis on ethnic bias, groupthink, and misunderstanding the threat's logic.	
Task: Evaluate and prioritize COAs	
The **staff** evaluates each threat COA and prioritizes each based on the threat's likelihood to adopt that COA. • Analyze each COA to identify threat strengths, weaknesses, decision points, and objectives. • Evaluate how well each COA meets the criteria—suitability, feasibility, acceptability, distinguishability, and completeness—of threat doctrine, their previous operation, and threat TTP. • Evaluate how well each COA takes advantage of the operational environment. How does the operational environment encourage or discourage COA selection? • Analyze the threat's recent activity to determine if a COA has been adopted.	

Table 3-7. Step 4—Determine threat courses of action (continued)

G-2/S-2 considerations
Task: Develop each COA in detail
Each COA answers the following six basic questions: ***Who:*** The threat and its makeup—a conventional force, terrorist organization (group or cell), insurgency, or criminal (gang, group, cartel). ***What:*** The type of operation—such as attack, defend, bank robbery, or suicide bombing. In stability operations, the ***what*** factors are target types, target selection, and objectives. ***When:*** The time of the action—***when*** usually refers to the earliest time the threat can adopt the COA under consideration. In an operational environment, consider the following factors: • Capability. • Intent. • History. • Activity. • Target environment. • Personalities. ***Where:*** The location of the objective or objectives in the AO. ***How:*** The method the threat may use to employ their assets, such as dispositions, location of main effort, scheme of maneuver, or time and place of a terrorist attack and how it may be supported. ***Why:*** The objective or end state the threat intends to accomplish. The objective or end state of an asymmetrical threat would factor in the vision or mission of that type of threat (for example, purify Islam through violence; overthrow the secular government and replace it with an Islamic state). ***Each developed threat COA has three key products:*** • Situation templates. • Threat COAs and options. • HVTs.
Task: Identify initial ISR requirements
Identify initial ISR requirements using threat COA key products: • Event template. • Event matrix. • ISR plan.

AO—area of operations
C2—command and control
CBRN—chemical, biological, radiological, nuclear
COA—course of actions
HPT—high-payoff target
HVT—high-value target
IED—improvised explosive device
IPB—intelligence preparation of the battlefield
ISR—intelligence, surveillance, reconnaissance
SIGINT—signals intelligence
TTP—tactics, techniques, and procedures

3-41. To achieve the desired results of step 4, the following key products are developed:

- Situation template.
- Event template.
- Event matrix.
- Decision support template (DST).
- High-value target list (HVTL).

SITUATION TEMPLATE

3-42. Figure 3-18 shows how situation templates are built.

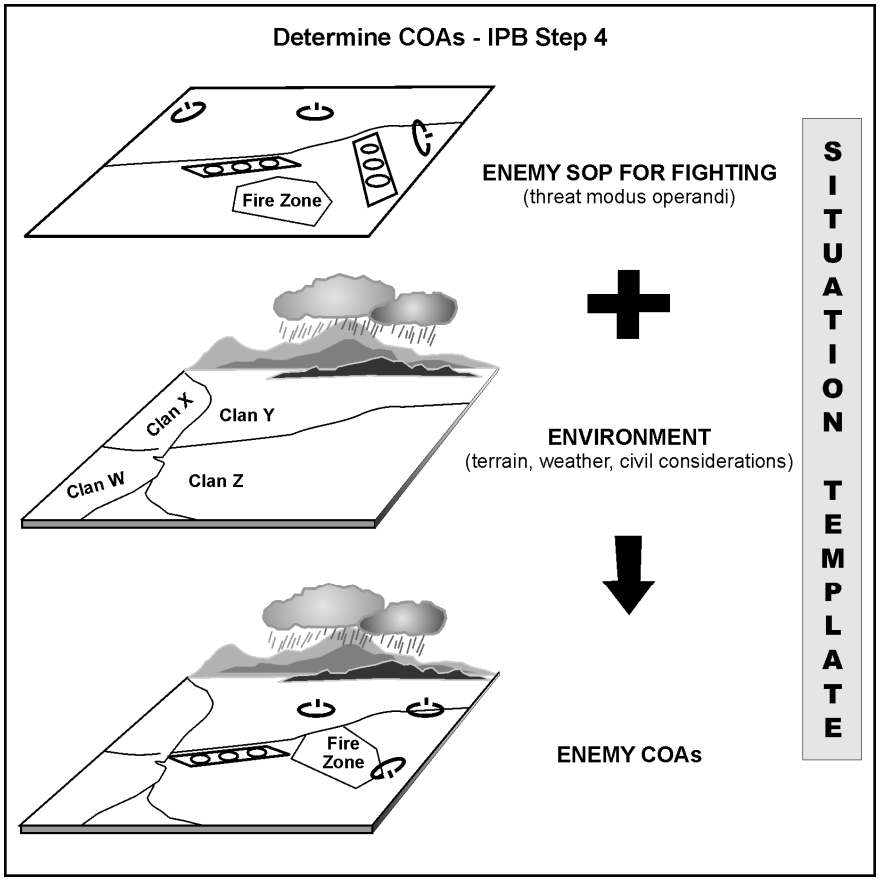


Figure 3-18. Example situation template

EVENT TEMPLATE

3-43. The event template is a guide for intelligence, surveillance, and reconnaissance (ISR) planning. (See figure 3-19.) The event template—

- Depicts the named areas of interest (NAIs) where activity (or inactivity) indicates the threat COA.
- Displays a description of the indicators and activity expected in each NAI.
- Usually cross-references each NAI and indicator with the expected times of occurrence and helps to confirm or deny threat COAs.

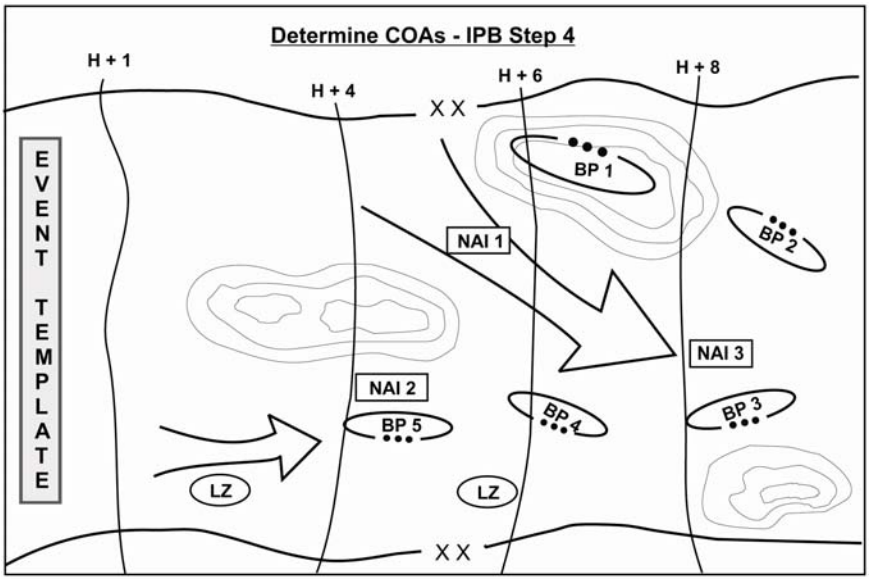


Figure 3-19. Example event template

EVENT MATRIX

3-44. The event matrix is an intelligence tool that works in conjunction with the event template. (See figure 3-20.) The event matrix—

- Is the basis for building the ISR plan, and with the event template for building the DST.
- Used in conjunction with the event template as an analytical tool to analyze threat actions and intentions during battle tracking.
- Has no prescribed format. However, disseminate it along with the event template to the subordinate intelligence staff as long as it remains within intelligence channels.

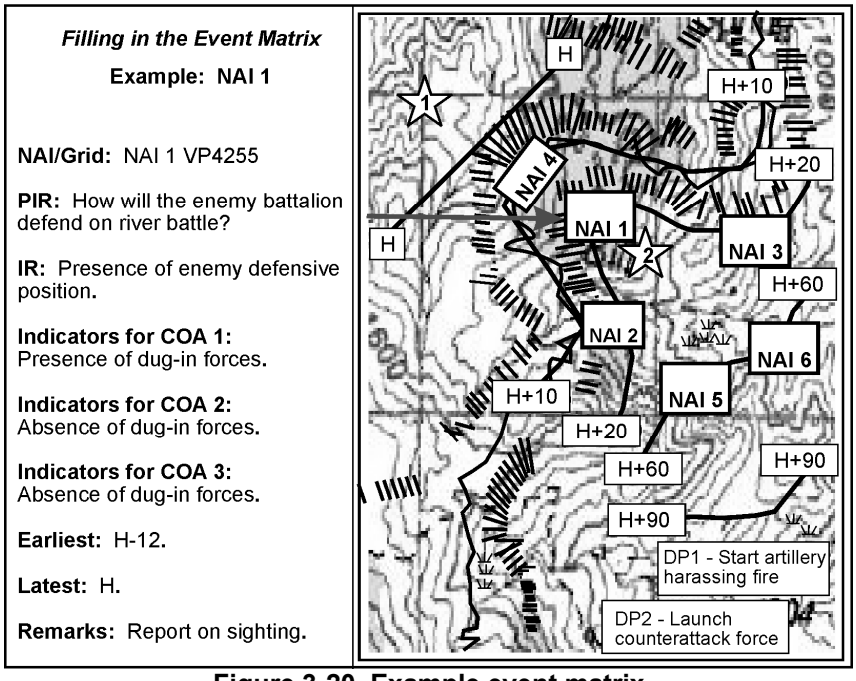


Figure 3-20. Example event matrix

DECISION SUPPORT TEMPLATE

3-45. The DST is used to depict current and predicted threat locations—designated as NAIs on the DST. Once identified, NAIs can then be used to confirm or deny a threat's activities or adoption of a particular COA. Additionally, threat decision points or decision phase lines, target areas of interest (TAIs), and high-payoff targets (HPTs) are identified. (See figure 3-21.)

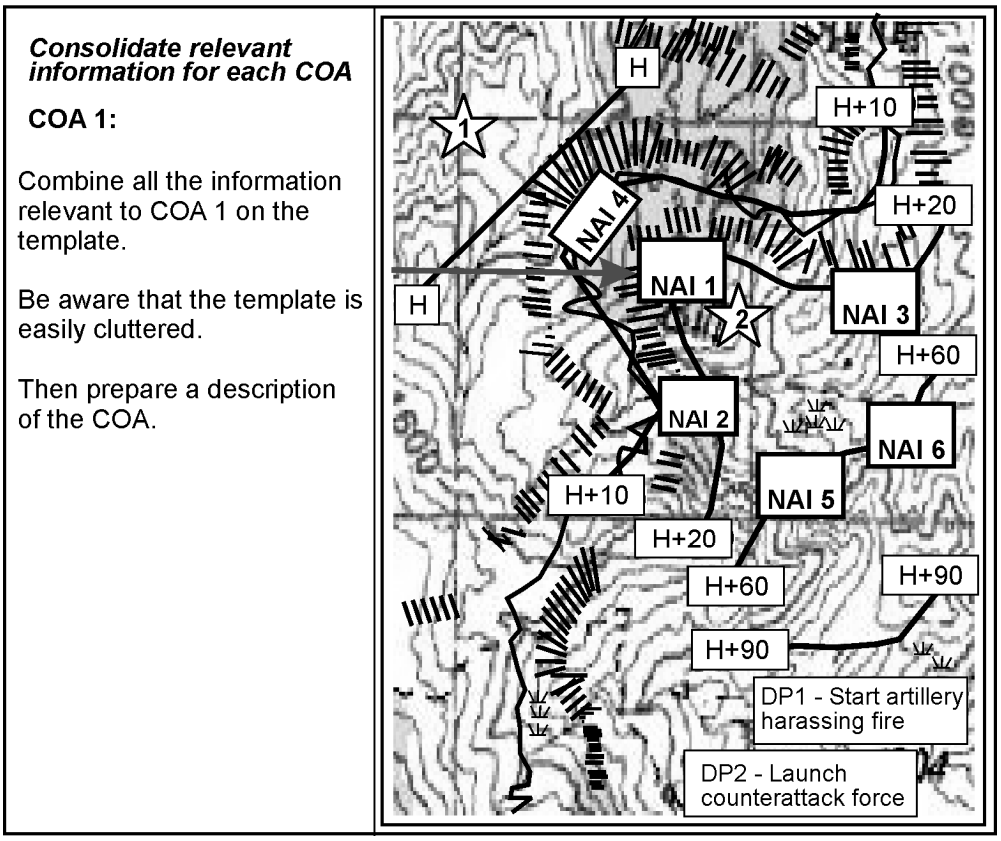


Figure 3-21. Decision support template

HIGH-VALUE TARGET LIST

3-46. A HVTL is a list of targets the enemy commander requires for the successful completion of a mission. The loss of an HVT could seriously degrade important enemy functions throughout the friendly commander's AO. Figure 3-22 shows an example of a HVTL.

Category	*High-value target*	*Justification*
Engineers	MTK	Necessary to clear route for assault force.
Fire support	2S1	Necessary to neutralize friendly forces in BP1 to support the assault force.
Command and control	BMP-2K	Necessary to control close fight and commit the exploitation force.

Figure 3-22. Example high-value target list

Chapter 4

G-2/S-2 Operations

The G-2/S-2 can use the information in this chapter to monitor intelligence readiness before receipt of a mission and subsequently to verify preparations and facilitate mission planning. It is critical that the intelligence section have deliberate procedures that are diligently followed for successful mission accomplishment. See appendix A for intelligence readiness during persistent conflict in which the Army employs Army force generation (ARFORGEN), a process that progressively builds unit readiness over time during predictable periods of availability to provide trained, ready, and cohesive units prepared for operational deployments.

OVERVIEW

4-1. This chapter uses the five processes of force projection, and the intelligence operations that support each. FM 3-0 has a detailed discussion of force projection. The G-2/S-2 answers the commander's critical intelligence requirements (CCIRs) during the force projection processes. Until the unit's intelligence, surveillance, reconnaissance (ISR) assets are operational in the area of operations (AO), the G-2/S-2 depends on intelligence from the senior Army force component or joint task force intelligence sections to answer the unit's intelligence needs. The five processes of force projection are—

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

MOBILIZATION

4-2. *Mobilization* is the process of assembling and organizing resources to support national objectives in time of war and other emergencies (FMI 3-35). During the mobilization process the G-2/S-2—

- Establishes habitual training relationships with their Active and Reserve augmentation units as well as higher echelon intelligence organizations as identified in existing operation plans (OPLANs).
- Identifies ISR force requirements for the different types of operations and contingency plans.
- Identifies individual military, civilian, and contractor manpower augmentation requirements for intelligence operations.
- Supports the Reserve Component units by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identifies individual mobilization augmentees to fill gaps created by personnel shortages. If possible, these augmentees should be individuals with a working knowledge of unit standing operating procedures (SOPs) who understand the mission.
- Monitors intelligence reporting on threat activity and indications and warning (I&W), data and watches condition levels.
- Manages information requirements and requests for information (RFIs) from the unit and subordinate units.
- Updates ISR synchronization planning based on augmentation or changes to task organization.

- Notifies attachments to provide updated access rosters and obtains higher headquarters access rosters. Updates throughout mission cycle as required.
- Within the unit, verifies clearances and accesses, including sensitive positions and radiotelephone operators.
- Coordinates the subversion and espionage directed against the Army program, counterintelligence (CI), and operations security (OPSEC) training and operations.
- Verifies access to intelligence databases through division or subordinate units. Ensures unit intelligence personnel have access to national and strategic databases.
- Obtains current technical intelligence (TECHINT) and user bulletins and the Defense Intelligence Agency (DIA) "Top Ten Equipment Acquisition" list from the 203d Military Intelligence (MI) Battalion (TECHINT).
- Acquires information on disposition directives from the Joint Chiefs of Staff and combatant commanders.
- Reviews section files. Designates deployable and nondeployable records.
- Coordinates contingency area of interest (AOI) briefings.
- Inspects unit areas and equipment for physical security deficiencies. Coordinates for support and access.
- Coordinates security force requirements with tasked units and military police (MPs).
- Provides updated section alert notification roster to the G-1/S-1.
- Finalizes security plans and instructions. Checks guard and MP patrols.

DEPLOYMENT

4-3. *Deployment* is the relocation of forces and materiel to desired operational areas (JP 1-02). Deployment has four supporting phases that are not always sequential, could overlap, or occur simultaneously (see FMI 3-35 for more information on the deployment phases):

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

4-4. In deployment, the commander—

- Ensures Active and Reserve MI organizations or augmentees are trained and equipped to conduct ISR operations.
- Focuses on intelligence to support specific mission decisions and planning requirements, as OPLANs are activated.
- Begins planning for the crossover point in intelligence when tactical ISR assets within the AO replace initial reliance on higher echelon intelligence.

4-5. In deployment, the G-2/S-2—

- Establishes collection strategies that will activate upon alert notification.
- Coordinates collection and communications plans before a crisis occurs.

- Uses the OPLAN, which identifies the intelligence requirements supporting the ISR synchronization tools, including—
  - ISR elements providing support, both in and outside the AO.
  - Command and support relationships of ISR assets (agencies and systems) at each echelon.
  - Report and request procedures not covered in unit tactical SOPs.
  - Sequence of deployment of MI personnel and equipment. Early deployment of key ISR personnel and equipment is essential for protecting the force and combat readiness. Composition of initial and follow-on deploying ISR assets is influenced by the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations [METT-TC]), availability of communications, availability of lift, and ability of the national collection system to support the operation.
  - Communications architecture supporting both intelligence staffs and ISR assets. Signal commands must be involved in communications planning.
  - Friendly vulnerabilities to hostile intelligence threats and plans for conducting OPSEC, deception, and other measures to protect the force. CI personnel plan as early as possible to ensure adequate CI support to protect deploying and initial entry forces.

4-6. The G-3/S-3 and ISR assets must continually monitor and update their OPLANs to reflect the evolving situation, especially during a crisis. National intelligence activities monitor regional threats throughout the world and can answer some intelligence requirements supporting OPLAN development. The commander and G-2/S-2 must proactively identify requirements that can be answered by national and theater intelligence.

4-7. Upon alert notification—

- The G-2/S-2 updates estimates and intelligence preparation of the battlefield (IPB) products needed to support command decisions on force composition, deployment priorities, and sequence, as well as in the AO.
- ISR elements reassess requirements immediately after alert notification.
- G-2/S-2 or ISR planners begin verifying planning assumptions within the OPLANs.
- CI and ISR personnel provide support to optimize OPSEC and antiterrorism measures.

4-8. Throughout the deployment process, intelligence activities provide the deploying forces with the most recent intelligence in the AO. The G-2/S-2 and ISR elements update technical databases and situation graphics. The G-2/S-2—

- Understands the unit, Army Service component command (ASCC), and joint task force intelligence organizations.
- Conducts a predeployment site survey with commander and staff elements if mission and time allow.
- Determines and coordinates any special access required for personnel to conduct operations.
- Develops intelligence and intelligence-related communications architecture:
  - Use Army intelligence communications and reporting systems such as the Distributed Common Ground System-Army (DCGS-A) to access other Army, joint intelligence, and national databases.
  - Establish automated message handling system profiles.
  - Establish unclassified and classified databases, including addressing the requirements for format and standardization, indexing and correlation, storage, procedures for establishing new databases, security protocols, and associated applications.

- Plans for requirements to support 24-hour operations:
  - Automation.
  - Communications capacity.
  - Personnel necessary to provide continuous intelligence, ISR synchronization, collection, processing, and reporting.
- Prepares and submits a request for forces for U.S. Air Force (USAF) weather specialty teams.

Note. Weather specialty teams must be requested for deployments since they are not a permanent part of Army units. Weather specialty teams will be deployed by the USAF to theaters and then assigned to support units using METT-TC considerations. These teams may or may not come from the same installation as the deploying Army unit.

- Plans all procedures to access specific intelligence products and reports:
  - Obtain status of ISR assets, and provide the current intelligence picture from the lodgment back to the senior echelon commanders, if not in theater.
  - Plan all links to higher intelligence organizations, including joint intelligence operations centers (JIOCs) and the elements designed to leverage theater intelligence.
  - Understands the capabilities of and coordinates with joint task force intelligence organizations, including the national intelligence support team if formed.
- Provides higher headquarters intelligence organizations with the unit's priority intelligence requirements (PIRs), as well as any special intelligence requirements.
- Coordinates an electronic intelligence (ELINT) "reach" link (Web page) for the unit to extract information as required.
- Determines transportation requirements and availability (aircraft or naval vessel) for deployment.
- Determines all sustainability requirements.
- Determines intelligence release requirements and restrictions such as releasability to multinational forces or the host nation.
- Reviews status of forces agreements (SOFAs), defense cooperation agreements, rules of engagement (ROE), international laws, and other agreements, emphasizing the effect each has on ISR operations. (Coordinates with the staff judge advocate on these issues.)
- Establishes force deployment priorities to support intelligence collection and analysis operations based on the mission variables:
  - Sequence initial required forces and capabilities, build-up priorities, and follow-on forces to ensure a sequenced plan, a tailored force, and established command and support relationships.
  - Consider sensors, processors, preprocessors, human intelligence (HUMINT), and CI.
  - Maintain unit integrity.
  - Plan phased communications architecture. (Build redundancy when possible.)
- Ensures intelligence links provide the early-entry commander with vital access to multisource Army and joint intelligence ISR assets, processing systems, and databases. Ensures collection is synchronized with production, and intelligence is synchronized with operations. (Specify reporting procedures and timelines.)
- Determines gaps in finished products, databases, and collection by discipline.
- Develops and submits production requirements for identified gaps.
- Develops and submits ISR requirements for identified gaps.
- Coordinates with the reconnaissance squadron and MI commanders on their tactical military decisionmaking process (MDMP).
- Incorporates all augmentation and support elements quickly within unit SOPs and unit training.
- Continuously updates databases to support the IPB process that follows.

- Supports the protection warfighting function:
  - Determine threat vulnerabilities for route to staging areas.
  - Intelligence operations identify, locate, and target the threat ability to target and affect friendly forces, facilities, and operations.
  - Intelligence support conducts threat and risk assessments and develops a counterreconnaissance plan.
- Develops a familiarity with supporting units.
- Uses CI personnel to assess and review friendly vulnerabilities to foreign intelligence collection and the threat's ability to exploit them:
  - Provide intelligence analysis to commanders and operators.
  - Incorporate CI threat assessments into the situation and decision briefings and all planning (especially deception planning).
  - Assign CI personnel to appropriate missions and analytical responsibilities.
- Uses the intelligence enterprise to access national geospatial intelligence (GEOINT), HUMINT, imagery intelligence (IMINT), measurement and signature intelligence (MASINT), signals intelligence (SIGINT), and CI databases, as well as automated links to joint Service, multinational, and host-nation sources.
- Supports further contingency plan and OPLAN development. ISR elements continually monitor and update their contingency plans to reflect the evolving situation, especially during crises.
- Immediately before deployment, updates deploying forces, technical databases, and situation graphics with the most recent intelligence on the AO.
- Develops contingency-tailored packages that allow placement of the right force support team in a deployable posture with adequate training.
- Coordinates security requirements for augmentees.
- Prepares DA Form 3964 (Classified Document Accountability Record) for classified materiel transported with deploying elements.
- Finalizes section personnel and equipment support list.
- Briefs rear detachment commander on unit's security plan.
- Notifies and assembles units.
- Initiates telephone control.
- Initiates area security plan.
- Prepares staff equipment to be transported to the staging area.
- Verifies section's basic load and load plans, including such items as maps and batteries.
- Distributes updated access roster.
- Presents the intelligence update to unit personnel.
- Coordinates with G-3/S-3 to initiate OPSEC plan.
- Presents the intelligence running estimate.
- Verifies attachments' security clearances through supporting G-2/S-2.
- Imposes restrictions on incoming and outgoing mail when given proper authority.
- Issues guard instructions. Provides access rosters to rear-detachment personnel and to higher and supported headquarters.
- Provides latest intelligence update to commander and staff.

4-9. Depending on the exact parameters of the contingency mission, the unit may be supported by a division intelligence support element or joint intelligence support element.

- The **division intelligence support element**—
  - Provides the deployed commander with timely, relevant, accurate, predictable, and tailored intelligence to support the quick introduction of U.S. forces.
  - May be the only MI asset deployed in the country to support the unit, depending on the size and mission of the deployed force.
  - In large operations, may deploy—as the entry force—with and support a brigade combat team (BCT) until the division and the remaining analysis and control element (ACE) arrive. Once the ACE is established, the division intelligence support element moves forward to support the tactical command post, or moves to wherever its capabilities are required.
- The **joint intelligence support element—**
  - May be established during the initial phases of an operation to augment the subordinate joint force intelligence element.
  - Usually manages the intelligence collection, production, and dissemination for a joint force.
  - Is scalable and can expand to meet the needs of the joint task force and the deployed commander.

4-10. Intelligence organizations in sustainment areas (such as the corps ACE) use modern satellite communications, broadcast technology, and automated data processing systems, such as DCGS-A, to provide graphic and textual intelligence updates to the forces in movement:

- In route updates help eliminate information voids and allow the commander to adjust the operation order (OPORD) before arrival in theater.
- Intelligence units extend established networks to connect intelligence staffs and ISR assets at various stages of the deployment flow.
- Where necessary, units establish new communications paths to meet unique mission demands.
- The ASCC, MI brigades, and corps G-2 elements play a critical role in making communications paths, networks, and intelligence databases available to deploying forces.

4-11. Space based systems play an important role in supporting intelligence during the deployment and the subsequent processes of force projection operations by—

- Providing communications links between forces in route and in the continental United States (CONUS).
- Permitting ISR assets to determine their position accurately through the Global Positioning System (GPS).
- Providing timely and accurate weather information to all commanders through the Integrated Meteorological System (IMETS) or DCGS-A.

4-12. Situation development dominates ISR activities during the initial employment process:

- The G-2/S-2 attempts to identify—from all threats to arriving forces—and assists the G-3/S-3 and commander in developing protection measures.
- ASCC organizations provide major intelligence support, which includes providing access to departmental and joint intelligence and deploying scalable echelon above corps intelligence assets.
- The entire effort focuses downwardly to provide tailored support to deploying and deployed echelons in response to their PIRs and information requirements.

4-13. As ISR assets build up in the deployment area, collection and processing capabilities are enhanced:

- Emphasis is placed on the build-up of the in-theater capability required to conduct sustained ISR operations.
- As the build-up continues, the G-2/S-2 strives to reduce total dependence on extended split based "top-driven" intelligence from outside the AO.
- As organic ISR assets flow into the theater, the G-2/S-2 relies on them for tactical intelligence although division and higher organizations remain a source of tactical and operational intelligence.

4-14. The G-2/S-2 provides the commander with support in planning the composition and deployment of follow-on units:

- As the Army forces enter the theater of operations, the joint task force J-2 implements and modifies, where necessary, the theater intelligence architecture planned during predeployment.
- Deploying intelligence assets establish liaison with staffs and units present in the AO.
- Liaison personnel and basic communications should be in place before the scheduled arrival of parent commands.
- ISR elements establish intelligence communications networks to support combat commanders.
- Coordinating staffs at all levels establish reporting and request procedures to ensure the timely receipt of intelligence.

4-15. CONUS and other secure intelligence support bases outside the AO and continue to support deployed units:

- As systems, such as Joint Surveillance Target Attack Radar System (JSTARS), begin operating, units equipped with the common ground station or DCGS-A will receive downlink data in near real time tailored to each unit's AO.
- Systems capable of rapid receipt and processing of intelligence from national systems and high capacity, long-haul communications systems are critical to the success of split-based support of a force projection operation.
- DCGS-A integrates the ISR feeds of these systems to provide a continuous flow of intelligence, including annotated imagery products, to satisfy many operational needs. Examples of these systems include the Tactical Exploitation System (TES), TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT), and the synthesized ultra-high frequency computer controller enhanced subsystem radio.

EMPLOYMENT

4-16. *Employment* is the strategic, operational, or tactical use of forces (JP 5-0). (See FM 3-0 and JP 3-0 for further discussion of employment. For a list of the intelligence tasks, see chapter 1.) At the beginning of the employment process, intelligence reaches the crossover point. Tactical intelligence becomes the commander's primary source of support, replacing "top driven" national and theater intelligence. The commander uses both tactical and operational intelligence to decisively engage and defeat the enemy in combat operations. In stability operations or civil support operations, the commander may use all levels of intelligence to accomplish the mission.

4-17. During all operations, the G-2/S-2 staff and ISR elements support the development and execution of plans by identifying threat objectives and decision points within the AO. The G-2/S-2 ensures the ISR synchronization processes focus on the PIRs. ISR elements continually evolve their concepts of employment to reflect changes in the operation.

4-18. The Army is restructuring to a modular, capabilities-based force to meet combatant commanders' requirements. Modularity gives smaller units a greater degree of flexibility and increased combat power. These modular units constitute a uniquely organized force capable of early entry to counter the threat, but are highly dependent on ISR to achieve dominant maneuver and precision engagement. See FM 2-19.4 for information regarding MI units and their capabilities.

SUSTAINMENT

4-19. *Sustainment* is the provisions of logistics and personnel required to maintain and prolong operations until successful mission accomplishment (JP 3-0). See JP 4-0 and FM 4-0 for details on the sustainment process of force projection operations.

REDEPLOYMENT

4-20. *Redeployment* is the transfer of forces and materiel to support another joint force commander's operational requirements, or to return personnel, equipment, and materiel to the home and/or demobilization stations for reintegration and/or out-processing (JP 3-35). (See FMI 3-35 and FM 4-01.011 for further discussion of redeployment.) As combat power and resources decrease in the AO, protection and I&W become the focus of the commander's intelligence requirements. This drives the selection of ISR elements that remain deployed and those that may redeploy. The G-2/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 to support redeployment (reverse intelligence crossover point).
- Captures consolidated databases.
- Transfers data to appropriate repository such as national databases.
- Evaluates the need for individual mobilization augmentees.
- Captures lessons learned after-action reviews.
- Maintains intelligence readiness.

4-21. If the unit is replaced by another U.S. or multinational force, the mission continues, but there is a parallel focus to provide the incoming unit with situational understanding before conducting relief in place (RIP)/transfer of authority (TOA) operations. Products and product sources should be shared at the earliest time possible to facilitate the transition. Table 4-1 provides factors to address during a transition of intelligence responsibility from a departing unit to an incoming unit and when transitioning an area between units. The status of all items listed is thoroughly coordinated between the transitioning G-2s/S-2s to ensure an effective hand-off of responsibility.

Table 4-1. Intelligence transition factors

Current situation
Threat disposition (the threat warfighting functions): • Movement and maneuver. • Intelligence. • Fires. • Sustainment. • Protection. • C2. • Communications. • Deception. Threat strength: • Percentage strength of units. • BDA: ▪ Personnel. ▪ Equipments. ▪ Weapons. ▪ Sustainment. Threat vulnerabilities. Threat capabilities. Probable COA. HVTs. Previous and current threat TTP, such as attack methods used IEDs. Areas prone to frequent insurgent attacks.
Friendly intelligence situation
ISR synchronization tools: • IMINT: ▪ Required coverage. ▪ Focus (CCIRs). • SIGINT: ▪ Required coverage. ▪ Focus (EEFI, PIRs, SIRs). • HUMINT: ▪ NAIs. ▪ Surveillance. ▪ Detainee/EPW. ▪ Focus (RFIs, PIRs, SIRs). ▪ Assist with DOMEX. • CI: ▪ NAIs. ▪ Surveillance. ▪ Focus (RFIs, PIRs, SIRs). • ISR asset status: ▪ Assets. ▪ Asset schedule—previous 24 hours, next 24 hours. ▪ Focus (CCIRs). • Points of contact. • Downlinks. • Reporting times (time to report, due times). • Lists of stay-behind elements. • Intelligence assets (organic, theater, national). • Communications architecture and frequencies. SIGINT: • Technical data (additions, changes, deletions). Detainee/EPW: • Numbers, locations, Category A, SOFA. • Handover to JTF or Army forces. • Host-nation handover. Host-nation intelligence/security: • Support, assets, communications. • Points of contact and liaison officers.

Table 4-1. Intelligence transition factors (continued)

Key terrain
Map updates and corrections
Detainable, of interest, and protectable lists
ISR synchronization tools
Coordination for stay-behind personnel
Status and plans for cover, security, and OPSEC
List of stay-behind products
Annex B. Single-source estimates. Military source operations (source registry). Current operational picture, intelligence running estimate, and supporting intelligence products. All-source intelligence support and sources. Imagery products and sources. Current weather forecast and on-hand weather, light data, and sources. Historical documents, locations, and sources.
Enclosures
List of threats, strengths, capabilities, COAs, weaknesses and vulnerabilities, and effects of friendly action. Threat situation overlays. Troop list of friendly ISR assets. Friendly ISR asset location overlays. Intelligence communications net diagrams and points of contact list. Key terrain, overlays. Map updates and corrections (may be overlay). Detainable, of interest, and protectable lists. ISR synchronization tools.
Other
ROE. Written guidance and policy letters. Battle rhythm. SOPs. TTP—friendly, host-nation, and threat. Hand receipts. Technical manuals and training for stay behind equipment.

BDA—battle damage assessment	EPW—enemy prisoner of war	PIR—priority intelligence requirement
C2—command and control	HUMINT—human intelligence	SIGINT—signals intelligence
CCIR—commander's critical information requirement	HVT—high-value target	RFI—request for information
	IED—improvised explosive device	ROE—rules of engagement
CI—counterintelligence	IMINT—imagery intelligence	SIR—specific information requirement
COA—course of action	ISR—intelligence, surveillance, and reconnaissance	SOFA—status-of-forces agreement
DOMEX—document and media exploitation	MI—military intelligence	SOP—standing operating procedure
EEFI—essential element of friendly information	NAI—named area of interest	TTP—tactics, techniques, and procedures
	OPSEC—operations security	

Appendix A

Intelligence Readiness Training

This appendix is designed to assist newly assigned S-2s in maintaining technical and tactical intelligence proficiency for themselves, their subordinates as well as the intelligence Soldiers within the parent unit. It is the S-2's responsibility (in coordination with the military intelligence (MI) company commander) to ensure the intelligence Soldiers are provided every opportunity to continually meet and maintain their technical skills. The tables are designed in a building-block approach that is systematic and consistent with the Army force generation (ARFORGEN) three-phased readiness cycle—**reset, train/ready**, and **available** force pools—to meet operational requirements at the brigade level. Tables A-1 (page A-2), A-2 (page A-5), and A-3 (page A-6) show sample factors that may be modified for any echelon.

INTELLIGENCE READINESS TRAINING

A-1. Intelligence readiness training can be streamlined if the intelligence officer and staff—

- Practice battle rhythm and prepare operational products in garrison.
- Preplan and practice an intelligence "surge" on likely contingency crises.
- Prepare and practice—from predeployment through redeployment—in coordination with personnel (including databases and connectivity) from—
  - Counterintelligence (CI).
  - Geospatial intelligence (GEOINT).
  - Human intelligence (HUMINT).
  - Imagery intelligence (IMINT).
  - Measurement and signature intelligence (MASINT).
  - Open-source intelligence (OSINT).
  - Signals intelligence (SIGINT).
  - Information operations (IO).
  - Staff weather officer (SWO).
  - Civil affairs.
  - Psychological operations (PSYOP).
  - Special operations forces units.
- Use Distributed Common Ground System-Army (DCGS-A) enterprise to gain and maintain contact with forward units and adversary.
- Ensure the following are a part of daily operations:
  - External augmentation.
  - Standing operating procedures (SOPs) that 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 (MI augmentation and other Services); exploit nongovernmental organizations (NGOs) and private volunteer organizations once a crisis emerges.

- Implement "Every Soldier is a Sensor" program, which ensures all Soldiers understand the commander's critical information requirements (CCIRs), priority intelligence requirements (PIRs), and information requirements, and are trained to actively observe, detect, and report changes in the area of operations (AO) to support the fusion of collected information into intelligence.
- Exchange communications protocols with higher headquarters, subordinate, and lateral units.
- Forward all requests for intelligence information to higher headquarters in accordance with SOPs.
- Take advantage of the Foundry Program training opportunities as well as mobile training team (MTT) opportunities.

RESET

A-2. The **reset** force pool redeploys from operations, receives and stabilizes personnel and reset equipment, and conducts individual and collective training. (See table A-1.) Unit collective training is focused on the unit's mission essential task list (METL). Units in the reset force pool are not ready or available for major combat operations. However, they are ready to respond to civil support operations at all times.

A-3. For the incoming intelligence officer, reset begins with a basic orientation to the unit and next higher echelon mission. The goal is to quickly acquaint the intelligence officer and staff with an understanding of the battalion, brigade, and division roles within corps, possible missions, and deployment areas. The intelligence officer, the intelligence staff, and assisted by the MI commander will further develop their knowledge, insight, and assessments of intelligence and security within their unit focusing on the intelligence preparation of the battlefield (IPB) process, intelligence production and dissemination, intelligence, surveillance, and reconnaissance (ISR) operations, and security.

Table A-1. Intelligence factors for reset

S-2 section (may be modified for intelligence officers and their sections at any echelon)
Mission/Unit orientation
Coordinate with and receive briefing from outgoing S-2 counterpart.
Receive unit commander, in brief.
• Communicate with unit commander. • Inquire about the required intelligence and intelligence products. • Tailor intelligence to the needs of the commander.
Study division, brigade, and battalion OPLANs.
Determine country and area study requirements from open and classified sources based on contingency and assigned OPLANs.
• Inspect unit maps, terrain, and weather products. • Identify shortages. • Request authority from the NGA (unclassified or at the lowest classification) to— ▪ Declassify products locally. ▪ Download digitized products (map sheets for the All-source Analysis System, terrain data, and imagery), as required.
Begin country studies.
Be knowledgeable on threat equipment, electro-optical devices, doctrine, and tactics. Teach a class on the subject at least once during this phase.
Determine all organic or assigned intelligence assets that may support the ISR efforts.
Review unit's ISR synchronization tools.
Study the commander's current PIRs and information requirements as developed.
Meet with the next higher echelon G-2/S-2 to discuss the ISR synchronization process.
Brief the next lower units on division and corps intelligence specific ISR assets.
Review and update S-2 section SOPs.

Table A-1. Intelligence factors for reset (continued)

S-2 section (may be modified for intelligence officers and their sections at any echelon)
Mission/Unit orientation
• Review and evaluate intelligence annex to unit SOPs. (Use FM 2-0, FM 5-0, unit SOPs, and intelligence annex to the division SOPs.) • Provide the commander with an updated evaluation of the unit intelligence annexes. • Develop SOPs if one is missing or outdated.
Visit and receive briefings from G-2, deputy G-2, G-2 operations chief, G-2 plans chief, G-2 training chief, G-2X, IO officer, and EWO.
Meet with subordinate S-2 to gain an understanding of— • Commander's intelligence priorities. • Personnel and equipment status. • Training proficiencies and deficiencies. • Areas requiring echelon assistance.
Visit MI commander or BSB commander for unit and equipment briefings, displays, and demonstrations.
Meet and discuss intelligence missions and products, and coordinate a training plan with the— • S-2X. • MI company commander. • Scout platoon leader. • Local CI team. • Analysis section chief and ISR synchronization manager. • Terrain detachment team. • Other staff officers.
Coordinate with commanders. Inquire about required intelligence during field training exercises and OPORD briefings.
Visit unit staff sections and attached sections from other units (fires cell, air-and-missile defense, CBRN, special operations C2 element, and engineers).
Coordinate with the fires cell to develop and review unit targeting and BDA procedures.
Know the unit air liaison officer. Request BDA and in-flight reports that will bolster reporting.
Become familiar with capabilities, limitations, and vulnerabilities of unit's equipment (tanks, Bradley's, other assigned, attached systems, or OPCON warfighting function operating in the unit's AO; particularly the TA and information dissemination capabilities).
Visit and observe the division's primary weapon systems training.
Become knowledgeable of the unit's and next higher echelon field SOPs and deployment procedures.
Training—section
• Review mission and section METL and battle tasks. • Have section members give assessments of the current training level. • Begin coordination for the training plan.
If linguists are organic to the unit— • Review language proficiency requirements. • Assist S-3 in coordinating training. • Retain a list of the unit's linguist capabilities, including unpaid abilities.
Visit G-2 training for intelligence training products.
• Obtain recent CTC and applicable CALL documents. • Develop a plan to correct any deficiencies. • Incorporate plan into future exercises or CTC rotations.
Submit training requests (MTTs, new equipment training, Foundry Program, and language immersion program) through applicable higher S-2 to G-2 training, as required.
Attend or send Soldiers to appropriate training. (See discussion on training by section/intelligence discipline in this appendix.)
Visit nearest battle simulation center and become familiar with computer operations.
Design opposing force plan for training exercises.
Training—equipment
Use the section's automation equipment and programs.
Receive briefing and training from the unit signals officer on communications procedures and communications equipment, preventive maintenance, checks, and services.
Become familiar with S-2 section vehicles and generators, as necessary.
Learn the connectivity, reporting, and requesting procedures.

Table A-1. Intelligence factors for reset (continued)

S-2 section (may be modified for intelligence officers and their sections at any echelon)
Personnel security
Obtain SCI access through the special security officer and review SCI billets for unit.
Obtain access to the security clearance system, such as the JPAS, through the special security officer.
Review the unit's personnel security procedures. (See AR 380-67.)
Continually review clearance requirements, applications, and updates.
Physical security
Review and update the unit's arms room security SOPs.
Inventory all sensitive items per company.
Review and update key control program SOPs.
Review and update physical security and crime prevention SOPs. (See AR 190-13.)
Receive crime prevention and physical security program briefings from the MPs and directorate of security. Update the unit's crime-prevention program as necessary.
Test the arms room's Joint-Services Intrusion Detection System.
Conduct random, unannounced security checks. Report results and recommendations to the commander.
Information security
Understand additional duty responsibilities as required: • Top secret document custodian. • Information systems security officer.
Understand current division policy on CONUS and OCONUS transport of classified material.
• Conduct inventory of classified materials. • Learn destruction and verification methods. • Review destruction and transfer SOPs.
Develop and implement a detailed internal security inspection program that covers intelligence areas within the unit.

AO—area of operations	JPAS—Joint Personnel Adjudication System
AR—Army regulation	METL—mission-essential task list
BDA—battle damage assessment	MI—military intelligence
BSB—brigade support battalion	MP—military police
C2—command and control	MTT—mobile training team
CALL—Center for Army Lessons Learned	NGA—National Geospatial–Intelligence Agency
CBRN—chemical, biological, radiological, nuclear	OCONUS—outside the continental United States
CI—counterintelligence	OPLAN—operation plan
CONUS—continental United States	OPORD—operation order
CTC—combat training center	PIR—priority intelligence requirement
EWO—electronic warfare officer	SCI—sensitive compartmented information
IO—information operations	SOP—standing operating procedure
ISR—intelligence, surveillance, and reconnaissance	TA—target acquisition

TRAIN/READY

A-4. Units in the **train/ready** force pool continue mission-specific collective training and are eligible for sourcing, if necessary, to meet joint requirements. (See table A-2.) Their collective training focuses on its directed METL, such as intelligence support to stability operations.

A-5. For the S-2 section, train/ready expands on the knowledge gained during reset. It consists of the same basic intelligence functions, but in more detail and culminates with a rotation at a combat training center (CTC).

Table A-2. Intelligence factors for train/ready

S-2 section (may be modified for intelligence officers and their sections at any echelon)
Understand the S-2's functions at the unit's tactical operations center and how they drive other tactical operations centers' functions.
Review threat characteristics holdings and files. Update material as required.
Determine available intelligence databases and "work the system" to obtain data to support a contingency plan. Brief results to the commander.
Identify information gaps in battle books, threat characteristics holdings and files, and intelligence annexes. Submit RFIs to satisfy intelligence requirements. The S-2 can access numerous products developed at the national level through the DGCS-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 weapons acquisition strategies and the overall military power and potential of selected foreign military forces. • TECHINT and user bulletins. • CIA World Fact Book and the DIA country studies. • JIOC assessments. • Open-source studies and articles. • JIOC threat characteristics database. • DIA intelligence support plans. • DIA contingency support studies and contingency support packages. • Other services.
Evaluate intelligence training and provide written results to the unit and commander.
Evaluate the unit Soldiers' knowledge of intelligence training tasks and provide a written report to the commander.
Develop an internal S-2 section intelligence cross-training program. Have section Soldiers teach the classes.
Become familiar with and teach a class on doctrine, tactics, and equipment of a contingency-plan threat.
Act as threat commander during the wargaming process and rehearsals.
Successfully deploy section and perform S-2 operations during a combat training center rotation.
Accurately predict threat actions during CTC rotation using IPB and all intelligence assets.
Successfully integrate with higher echelon G-2/S-2 during combat training center rotation.
Continually review and update intelligence running estimate and products.
Determine if all automated data processing systems are accredited. Brief the commander on steps required to correct any problems.
Determine the unit's security posture during field training exercises and CTC rotations. Recommend corrective actions to the commander.
Continually review clearance requirements, applications, and updates.
CIA—Central Intelligence Agency CTC—combat training center DCGS-A—Distributed Common Ground System–Army DIA—Defense Intelligence Agency INTSUM—intelligence summary IPB—intelligence preparation of the battlefield JIOC—joint intelligence operations center RFI—request for information TECHINT—technical intelligence

AVAILABLE

A-6. Units in the **available** force pool are in their planned deployment windows and fully trained, equipped, and resourced to meet operational requirements and conduct full spectrum operations. (See table A-3.)

A-7. Available takes the S-2, who has mastered the intelligence fundamentals through the first year**,** at which time the unit participated in the full annual training program and deployment process.

Table A-3. Intelligence factors for available

S-2 section (may be modified for intelligence officers and their sections at any echelon)
Qualify on all unit weapon systems.
Continually review clearance requirements, applications, and updates.
Continually review and update intelligence running estimate and products.
Successfully integrate with higher echelon G-2/S-2.
Determine all theater provided equipment or assets that may support the unit's ISR effort.
Conduct theater-specific individual, leader, and collective training.
Conduct mission-specific predeployment training and operations.
Successfully deploy section and perform S-2 RIP/TOA.
TOA—transfer of authority

INTELLIGENCE TRAINING RESOURCES

A-8. Some of the primary training resources used for intelligence Soldiers and units include—

- Noncommissioned officer education system (NCOES).
- Officer education system (OES).
- MI functional courses.
- New Systems Training and Integration Office.
- Language training.
- Cultural awareness training.
- Soldiers training plans (STPs).
- Joint Intelligence Combat Training Center.
- Foundry Program.
- MI Gunnery.

NONCOMMISSIONED OFFICER EDUCATION SYSTEM AND OFFICER EDUCATION SYSTEM

A-9. NCOES and OES train individual basic and advanced tasks. Both are managed by the U.S. Army Intelligence Center of Excellence (USAICoE) at Fort Huachuca, AZ. For more information, log onto the Intelligence Knowledge Network (IKN) Web site at https://icon.army.mil/.

MILITARY INTELLIGENCE FUNCTIONAL COURSES

A-10. MI functional courses train individual basic and advanced tasks. The courses are managed by USAICoE. Courses available include—

- Tactical Electronic Warfare (EW) Operations.
- F121 Sun Server Workstation Maintenance.
- F123 Highcastle Maintenance.
- F28 U.S. Air Force (USAF) Tactical Receive.
- Foreign Disclosure Certification.
- Information Systems Security Monitoring.
- Intelligence Master Analyst.

- TROJAN SPIRIT II V3/TROJAN LITE V3.
- J1 Basic Foreign Instrumentation Signals Intelligence (FISINT).
- MI Precommand.
- T6 Tactical Exploitation System (TES) Analyst.

A-11. For more information on MI functional courses, visit the University of MI Web site at http://www.universityofmilitaryintelligence.us/functional_courses/default.asp.

NEW SYSTEMS TRAINING AND INTEGRATION OFFICE

A-12. The New Systems Training and Integration Office at Fort Huachuca, AZ manages training development for new and product improved intelligence systems and capabilities, and the development of systems and nonsystems training devices. For more information and points of contact, log onto the IKN Web site (https://icon.army.mil). Click "IKN Web sites."

LANGUAGE TRAINING

A-13. Language training involves training individual tasks. Funding for language training is available through the Total Army Language Program. Resources include—

- **The Defense Language Institute Foreign Language Center** (DLIFLC). As the proponent for the Defense Foreign Language Program, DLIFLC assists commanders in developing a unit command language program, as well as the maintenance and local evaluation of the program. Visit the DLIFLC Web site at http://fieldsupport.lingnet.org/.
- **G-2 Language team** (Training and Language Technology and Contracting). Visit the Language team Web site at https://www.us.army.mil/suite/page/179065.
- **Army e-Learning**—with access to Rosetta Stone® courses in the 30 languages listed in table A-4. Visit http://usarmy.rosettastone.com/index.htm to obtain information about the Rosetta Stone® language training tool.

Table A-4. Rosetta Stone® language courses

Military Arabic	German	Latin	Swedish
Chinese (Mandarin)	Greek	Pashto	Tagalog
Danish	Hebrew	Polish	Thai
Dutch	Hindi	Portuguese	Turkish
English (United Kingdom)	Indonesian	Russian	Vietnamese
	Italian	Spanish (Latin America)	Welsh
English (U.S.)	Japanese	Spanish (Spain)	
Farsi (Persian)	Korean	Swahili	
French			

CULTURAL AWARENESS TRAINING

A-14. Cultural awareness training. The Professional Military Education Cultural Awareness Training Support Package contains four levels of training—initial military training to a captain's career course. The package offers lessons in defining culture, discussions of American and personal culture to determine areas of conflict and biases, the cultures of Iraq and Afghanistan, and the affect of culture on military operations through multiple practical exercises and situational training exercises. Materials available include—

- Presentations, levels 1 through 4.
- Training support package, levels 1 through 4.
- Lane training, levels 1 through 4.

A-15. Visit http://www.universityofmilitaryintelligence.us/tcc/cultural/default.asp for more information on cultural awareness training.

SOLDIER TRAINING PLANS

A-16. Soldiers training plans (STPs) provide training materials and information on individual military occupational specialties (MOSs) and warrior tasks. STPs are listed on the Army Knowledge Online (AKO) Web site.

JOINT INTELLIGENCE COMBAT TRAINING CENTER

A-17. The Joint Intelligence Combat Training Center trains individual and collective tasks in a simulated AO. The center uses realistic scenarios based on real-world operations and applies recent lessons learned from Operation IRAQI FREEDOM (OIF) and Operation ENDURING FREEDOM (OEF). This two-week course can be modified for a unit's mission. USAICoE manages the course. For more information, visit the IKN Web site at https://icon.army.mil/.

FOUNDRY PROGRAM

A-18. The Foundry Program trains individual and collective tasks. Led by the Department of the Army (DA) G-2, the training is an advanced skill, live environment certification program. Ultimately, the program assists tactical commanders and G-2s with a single point of entry for intelligence training coordination and opportunities that are otherwise unavailable. The Foundry Program handbook and quarterly training request worksheets are available on AKO and Secure Internet Protocol Router Network (SIPRNET). Training offered under the Foundry Program includes—

- MTTs sponsored through the Army Intelligence and Security Command, (INSCOM), Training and Doctrine Command (TRADOC), the National Reconnaissance Office, the Defense Intelligence Agency (DIA), and other joint and national activities.
- Formal classroom training events.
- Live environment training—usually 30 to 60 days in length.
- Funding for travel and per diem to attend MI training events sponsored by other units.
- Sponsoring short-duration (30 to 60 days) dialect training events to support operational missions. For example, Foundry Opportunity #019 (a basic Iraqi dialect course) to support OIF and Foundry Opportunity # 75 (Intermediate Pashtu) to support OEF.

Note. The Foundry Program does not sustain foreign language skills. Total Army Language Program funds are used for this.

MILITARY INTELLIGENCE GUNNERY

A-19. MI Gunnery trains and certifies individual and collective tasks. The MI Gunnery tables enable MI and unit commanders determine whether the MI Soldier and unit are prepared for their wartime mission. MI Gunnery tables are roughly modeled after Tank Gunnery tables—as a "crawl, walk, run" methodology of training and certifying Soldiers, teams, sections, platoons, and the unit in individual and collective tasks necessary to accomplish the unit's primary mission. MI Gunnery tables are organized as follows:

- First section:
  - ***STP individual tasks.*** Unit leaders ensure Soldiers are trained and certified as proficient in these tasks, as a part of the unit's combat readiness.
  - ***Annual common tactical tasks.*** Training directed by Army Forces Command (FORSCOM) for units deploying to support OIF/OEF. Soldiers are proficient in the 40 warrior individual tasks before deploying to a theater of operations.
  - ***MI individual tasks (by section).*** To provide intelligence support to operations, Soldiers are proficient in these tasks.
  - A table of instructions and guidance for leaders to certify MI element Soldiers in the aforementioned individual tasks.

- Second section:
  - ***Collective tasks and drill tasks.*** Teams, sections, and platoons are proficient and certified in these tasks before proceeding to company level training events.
  - ***Nine collective warrior battle drills***. Teams, sections, and platoons are certified as proficient in these drills as a matter of tactical protection.
  - ***Collective tasks and crew drill tasks.*** MI teams, sections, and platoons are proficient in these tasks to perform their missions in a specific AO.
  - ***Company level collective tasks.*** The MI company performs these tasks, as a whole, to successfully conduct intelligence operations.
- Third section:
- ***Home-station training event or exercise.*** Conducted and used by parent units to externally evaluate and certify the MI unit as proficient in all individual and collective tasks before a CTC or mission readiness exercise and deployment to a theater of operations.
- ***Deployment to a CTC training exercise or mission readiness exercise.*** The entire brigade combat team (BCT) is externally evaluated based on the conduct of the training exercise. There is a robust opposing force designed to depict a tough, competent threat.

A-20. Information on MI Gunnery is available on AKO.

TRAINING BY SECTION INTELLIGENCE DISCIPLINE

A-21. Table A-5 is list of training opportunities available to intelligence Soldiers. These training opportunities, combined with tactical overwatch of the assigned area of interest (AOI), ensure intelligence Soldiers can provide the commander with the intelligence required to plan, prepare, execute, and assess operations.

Table A-5. Training by section/intelligence discipline

Intelligence warfighting function personnel
NCOES/OES (as required)—(managed by USAICoE).
New equipment fielding and training.
Individual language and cultural awareness training.
Tactical questioning—(USAICoE).
DCGS-A MTT—(DCGS-A Program Manager).
Intelligence in Combating Terrorism—(USAICoE).
Individual and collective training certified (based on METL and IAW standards).
MI Gunnery.
Weapons qualification.
Vehicle licensing program.
Convoy staff exercise and live fire exercise.
Leader training program.
CP exercise.
CTC preparation.
CTC deployment.
CTC recovery.
CIED training.
Counterinsurgency seminar—(FORSCOM/TRADOC).
Theater-specific individual readiness training—(FORSCOM).
Deployment preparations.
Deploy.
If assuming an ongoing mission from another U.S. or multinational force conduct— • Theater briefings. • Theater reception, staging, onward movement, and integration training. • RIP/TOA.

Table A-5. Training by section/intelligence discipline (continued)

S-2 section
BCT S-2 course—(USAICoE).
G-2X/S-2X course—(USAICoE).
Special Security Officer/Special Security Representative course—(coordinate with higher special security officer).
Foreign Disclosure Officer course—(USAICoE).
NGIC All-Source Briefing—(NGIC).
MI Gunnery—(evaluated by the S-2 or the S-2 NCOIC).
JICTC—(USAICoE).
Section collective training.
Conduct tactical overwatch—(Target folders).
Lessons Learned Conference—(USAICoE) (If assuming an ongoing mission from another U.S. or multinational force).
All-source analysts/ISR synchronization managers
Collection Management Officer course—(DIA)/ISR Synchronization MTT—(USAICoE).
Intelligence Master Analyst course—(USAICoE).
National Intelligence Familiarization course—(DIA).
Joint Targeting course—(U.S. Joint Forces Command).
Joint Analyst-Interrogator Collaboration course—(USAICoE).
Computer forensics training—(Defense Cyber Investigation Training Academy).
All-source MI Gunnery.
JICTC—(USAICoE).
TROJAN SPIRIT training—(USAICoE).
Biometrics MTT—(Battlefield Forensics Course).
NGIC visit/briefing—(NGIC).
CI
CI Special Agent course—(DIA, HT-JCOE at Fort Huachuca).
CI and HUMINT Operations Management (S-2X/G-2X) course—(USAICoE).
Source Operations course—(DIA, HT-JCOE at Fort Huachuca).
Advanced Source Operations course—(DIA, HT-JCOE at Fort Huachuca).
DOMEX MTT—(NGIC).
Special capability equipment MTT—(USAICoE).
Biometrics MTT—(Battlefield Forensics Course).
Tactical overwatch—(Target folders).
Language immersion training—(Army G-2 Language Team, DLIFLC).
DOD Strategic Debriefing course—(DIA, HT-JCOE at Fort Huachuca).
CI and HUMINT Operations Management (S-2X/G-2X) course—(USAICoE).
Source Operations course—(DIA, HT-JCOE at Fort Huachuca).
Joint Analyst-Interrogator Collaboration course—(USAICoE).
Advanced Source Operations course—(DIA, HT-JCOE at Fort Huachuca).
HCT MTT—(USAICoE).
DOMEX MTT—(NGIC).
Special capability equipment MTT—(USAICoE).
Biometrics MTT—(Battlefield Forensics Course).
Tactical overwatch—(Target folders).
Language immersion training—(Army G-2 Language Team, DLIFLC).
Intermediate IMINT Analysis course—(Foundry–NGA).
TES course—(USAICoE).
Shadow flight training—(USAICoE/Unit).
IMINT live environment training—(Foundry–3d MI Center).
Imagery workstation training—(Army Space Program Office/3d MI Center).
JSTARS MTT—(Foundry).
JSTARS sustainment training—(Foundry).
Advanced IMINT Analysis course—(Foundry–3d MI Center).
Global Broadcast System training—(Foundry–3d MI Center).
GEOINT training cell—(USAICoE).
JSTARS Outreach—(Foundry–3d MI Center).

Table A-5. Training by section/intelligence discipline (continued)

MASINT and advanced GEOINT
MASINT fundamentals and equipment—(Foundry).
MASINT MTT—(Foundry).
Advanced GEOINT Analysis course—(Foundry).
UGS MTT—(USAICoE, New Systems Training and Integration Office).
MASINT QRC sensor training—(Foundry).
MASINT operations/immersion—(Foundry).
OSINT
OSINT Research and Analysis course—(Fort Leavenworth).
Open-Source Academy—(USAICoE).
DAIIS—(Foundry and MTT).
Nonattributable Internet access—(JIVU).
Untangling the Web—(JIVU).
Advanced Googling—(JIVU).
SIGINT
SIGINT Leaders course—(ATCAE, Fort Meade, MD).
Reporting guidance—(ATCAE).
Prerequisite computer based training for Deployer 2000—(ATCAE).
Deployer 2000/U.S. SIGINT Directives 18/Annex P—(ATCAE).
PROPHET team training/special collection and exploitation capability equipment training—(ATCAE, Army Cryptologic Operations–USAICoE).
ONEROOF operations training—(ATCAE/Army Cryptologic Operations–USAICoE).
Analyst Notebook training—(ATCAE–USAICoE).
Security identifier on the NSA's secure network—(ATCAE).
ArcView/target package development—(ATCAE–USAICoE).
TES course—(USAICoE).
Tactical EW Operations course—(USAICoE).
TROJAN SPIRIT training—(USAICoE).
SIGINT MI Gunnery.
Combat Operations Support—(Foundry).
Analysis and reporting—(Foundry).
SIGINT Tactical Overwatch—(Foundry).
Target familiarization and packets.
Language immersion training—(Army G-2 Language Team, DLIFLC).

ATCAE—Army Technical Control and Analysis Element
BCT—brigade combat team
CI—counterintelligence
CIED—counterimprovised explosive device
CP—command post
CTC—combat training center
DAIIS—Department of the Army Intelligence Information Service
DCGS-A—Distributed Common Ground System-Army
DIA—Defense Intelligence Agency
DLIFLC—Defense Language Institute Foreign Language Center
DOD—Department of Defense
DOMEX—document and media exploitation
EW—electronic warfare
FORSCOM—U.S. Army Forces Command
GEOINT—geospatial intelligence
HCT—HUMINT collection team
HT-JCOE—HUMINT Team Joint Center of Excellence
HUMINT—human intelligence
IAW—in accordance with
JIVU—Joint Intelligence Virtual University
JSTARS—Joint Surveillance Target Attack Radar System
MASINT—measurement and signature intelligence
METL—mission-essential task list
MI—military intelligence
IMINT—imagery intelligence
JICTC—Joint Intelligence Combat Training Center
MTT—mobile training team
NCOES—noncommissioned officer education system
NCOIC—noncommissioned officer in charge
NGA—National Geospatial–Intelligence Agency
NGIC—National Ground Intelligence Center
NSA—National Security Agency
OES—officer education system
OSINT—open-source intelligence
QRC—quick reaction capability
RIP—relief in place
SIGINT—signals intelligence
TES—Tactical Exploitation System
TOA—transfer of authority
TRADOC—U.S. Army Training and Doctrine Command
USAICoE—U.S. Army Intelligence Center of Excellence
UGS—unattended ground sensor

This page intentionally left blank.

Appendix B

Intelligence, Surveillance, and Reconnaissance Synchronization

Intelligence, surveillance, and reconnaissance is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. For Army forces, this activity is a combined arms operation that focuses on priority intelligence requirements, while answering the commander's critical information requirements (FM 3-0).

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

B-1. Through intelligence, surveillance, and reconnaissance (ISR), commanders and staffs continually plan, task, and employ collection assets and forces. They collect, process, and disseminate timely and accurate combat information and intelligence to satisfy the commander's critical information requirements (CCIRs) and other intelligence requirements. When necessary, ISR assets may focus on special requirements, such as information required for personnel recovery operations.

B-2. ISR is fundamental to information superiority and the support of friendly operations through the four ISR tasks:

- ISR synchronization.
- ISR integration.
- Surveillance.
- Reconnaissance.

ISR SYNCHRONIZATION

B-3. *Intelligence, surveillance, and reconnaissance synchronization* is the task that accomplishes the following: analyzes information requirements and intelligence gaps; evaluates available assets internal and external to the organization; determines gaps in the use of those assets; recommends intelligence, surveillance, and reconnaissance assets controlled by the organization to collect on the commander's critical information requirements; and submits requests for information for adjacent and higher collection support (FM 3-0).

ISR INTEGRATION

B-4. *Intelligence, surveillance, and reconnaissance integration* is the task of assigning and controlling a unit's intelligence, surveillance, and reconnaissance assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans and orders (FM 3-0). Integrating ISR into an operation ensures assignment of the best ISR assets (internal and external, including joint assets) through a deliberate and coordinated effort of the entire staff across all warfighting functions.

SURVEILLANCE

B-5. *Surveillance* is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means (JP 3-0). Surveillance involves observing an area to collect information.

RECONNAISSANCE

B-6. *Reconnaissance* is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0).

RELATED MISSIONS AND OPERATIONS

B-7. Within the context of the intelligence warfighting function, ISR related missions and operations are the activities and tasks associated with support to the conduct of ISR operations or providing ISR support to specialized missions. This task has four subtasks:

- Establish a mission intelligence briefing and debriefing program.
- Conduct intelligence coordination.
- Support sensitive site exploitation.
- Intelligence support to personnel recovery.

B-8. Related missions and operations are described, in detail, in FM 2-0.

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

B-9. The commander decides what information is critical based on experience, the mission, input from the staff, the higher commander's intent, and the staff's estimate of the situation. CCIRs are based on events or activities linked directly to the current and future situation. CCIRs consist of priority intelligence requirements (PIRs) and friendly force information requirements (FFIRs), which assist the commander in controlling the flow of critical information.

B-10. Although essential elements of friendly information (EEFIs) are not part of the CCIRs, they may be a priority if the commander so deems. *Essential elements of friendly information* are the critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation, and therefore, must be protected from threat detection (FM 3-0).

B-11. Figure B-1 depicts the relationship of information requirements, including CCIR (PIR and FFIR) and EEFI.

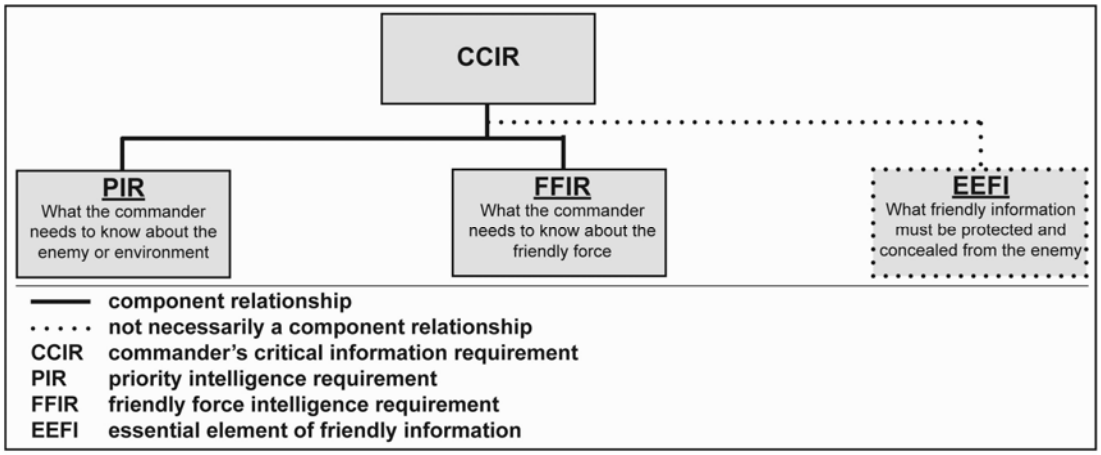


Figure B-1. Relationship of information requirements

THE ISR SYNCHRONIZATION PROCESS

B-12. The ISR synchronization process involves six continuous activities, as depicted in figure B-2. These activities and subordinate activities are not necessarily sequential and often overlap. The ISR synchronization process supports the staff planning and operations processes throughout the full spectrum

of operations. The process does not dramatically change with echelon, although organization, terminology, and tools may vary. For example, in the joint environment, there are differences in terminology and procedures that may require adjustments to unit standing operating procedures (SOPs).

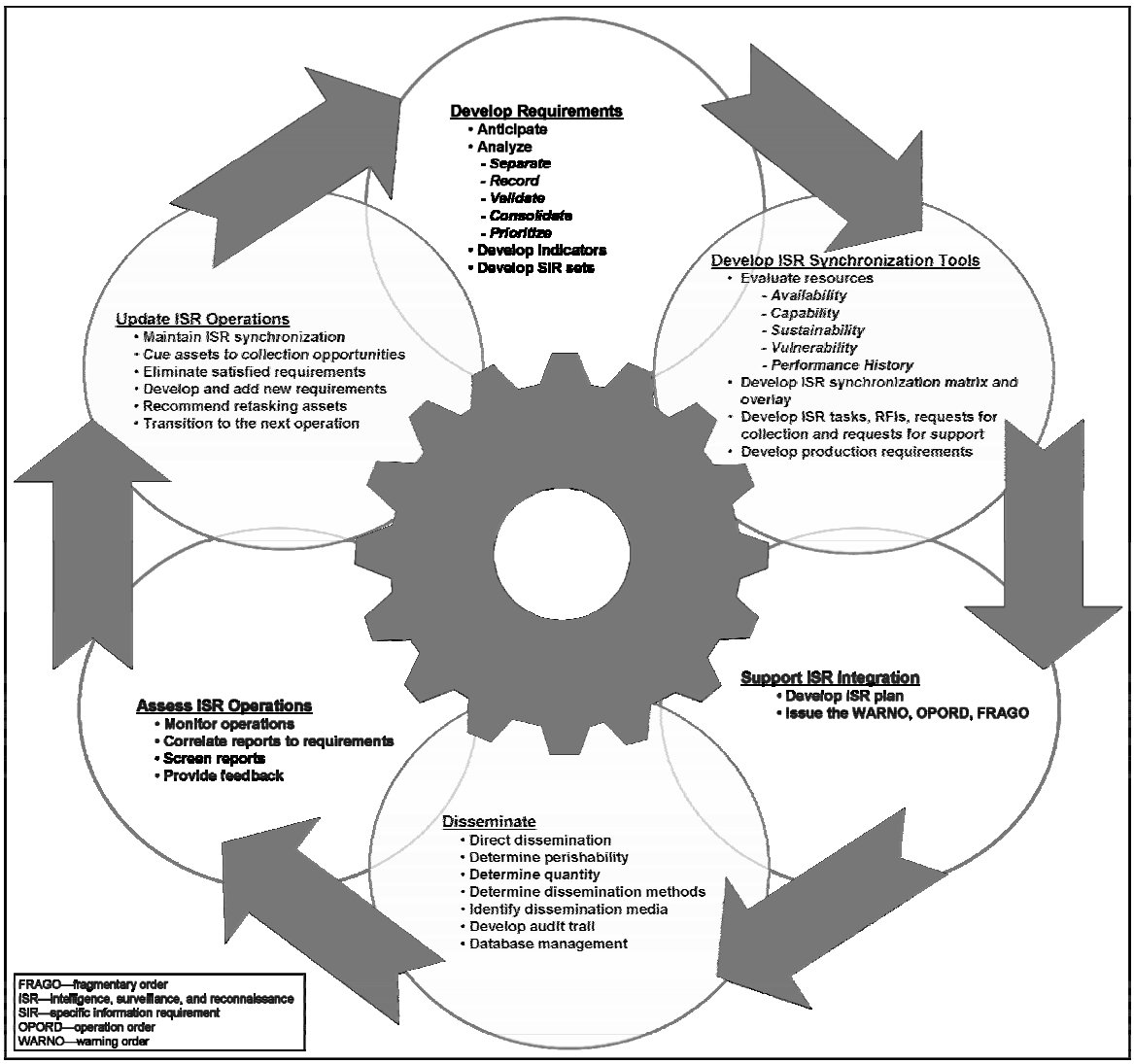


Figure B-2. ISR synchronization activities

DEVELOP REQUIREMENTS

B-13. Developing requirements refers to identifying, prioritizing, and refining gaps in data, relevant information, and knowledge concerning the operational environment requiring resolution, so the commander achieves situational understanding. Table B-1 (page B-4) describes the subordinate "Develop Requirements" activities and lists the G-2/S-2's responsibilities and products.

Table B-1. Develop requirements

Anticipate
• Identify new or refine existing requirements and present them to commanders for approval. • Recognize when and where to recommend a collection shift to the G-3/S-3.
Analyze
Separate. Categorize intelligence gaps answered through— • **Organic asset** collection. • **Intelligence reach**. Although not as responsive as a unit's own assets, intelligence reach may be the only way to answer a PIR. • **RFIs** for collection to higher and lateral echelons.
Record. • Record requirements from higher, adjacent, and subordinate units along with the requirements produced during mission planning. • Track each requirement from its receipt to its eventual satisfaction, merger, or elimination. • Record using a spreadsheet, database, or other mechanism prescribed by unit SOPs.
Validate. Consider the following: • **Necessity.** Is this requirement necessary or valid? If yes, has it been satisfied? Check databases to determine whether the intelligence was produced or the information was collected. If a product that satisfies the requirement already exists, refer the requestor to the producing agency. If the requestor does not have access to that agency's database, obtain and provide the product to the requestor. Refer requests for production to the appropriate agency. ***Note.*** In some cases, the intelligence already exists, but not in the format requested. One example is a unit that requests a demographics map put together from existing data. • **Feasibility.** Does the unit have the assets with the capabilities to execute the mission on time and with the detail required to support a decision? If not, can the unit submit an RFI to the echelon owning the ISR capability, with a reasonable expectation of receiving a timely response? • **Completeness.** All requirements should specify— ▪ ***Who*** (needs the results). ▪ ***When*** (time that the indicator is expected to occur and the LTIOV). ▪ ***What*** (activity or indicator). ▪ ***Where*** (geolocation, NAI, or TAI). ▪ ***Why*** (justification). ▪ ***Other*** (specific instructions or information).
Consolidate. Simplify the collection effort by merging similar requirements. Exercise caution when merging requirements to ensure— • The intent of the original requirements is not lost. • The accountability is maintained through accurate recordkeeping. • Dissemination is made to every requesting headquarters whenever a requirement is satisfied or eliminated.
Prioritize. Prioritize each intelligence requirement based on its importance to support the commander's intent and decisions. Consider the importance of the requirement above its generating echelon. Throughout the operation, intelligence officers prioritizing requirements should consider the ability to meet the requirement as well as justification, specificity, significance, and time phasing of the requirements. • **Justification.** Requirements are justified by their linkage to decisions. • **Specificity.** Requirements are narrowed and refined to the most specific *what, when*, and *where* questions possible. The *why* is the justification. • **Significance.** The relative significance of the activity to the commander's intent. • **Time phasing.** Time phasing influences prioritization. Time phasing of intelligence requirements, such as synchronization, is a continuous process. The operation may progress slower or faster during staff wargaming. Monitor the conduct of the operation and remain alert to changes in the LTIOV, based on shifts in the operational timeline.
Develop indicators
Indicator is an item of information that reflects the intention or capability of an adversary to adopt or reject a COA (JP 2-0). In Army intelligence, indicators— • May result from previous actions or from threat failure to take action. • Are the bases for situation development. • Are positive or negative evidence of threat, other activity, or AO characteristic that points toward capabilities, vulnerabilities, or intentions. • Show the adoption or rejection by the threat of a particular COA that may influence the commander's COA.

Table B-1. Develop requirements (continued)

Develop SIRs
SIRs describe the information required and should include the location and the time the information can be collected. • Develop SIR sets while the operations officers develop the collection strategy for each requirement and the general scheme of maneuver. • Make each indicator more specific by identifying the collection location—tying it to a point in the AO, such as a specific NAI. • Specify the collection time. Use the situation templates depicting the enemy COA and the graphics depicting the friendly scheme of maneuver to establish collection timelines for the NAI. • Identify the specific (detailed) information that supports the indicator. For example, specific information that supports the indicator "artillery deployed in NAI 12" might include the— ▪ Presence of M-1978 (KOKSAN) self-propelled gun. ▪ Presence of fire direction control equipment or vehicles. ▪ Presence of the digital data signal equipment. ▪ Presence of artillery ammunition carriers. • Label each SIR with an identifier to trace it back to the original intelligence requirement. • A final SIR might be written as, "Are there digital data signals active in NAI 12 between 041200 and 060200 March? LTIOV: 060400 March."

AO—area of operations	PIR—priority intelligence requirement
COA—course of action	RFI—request for information
ISR—intelligence, surveillance, and reconnaissance	SIR—specific information requirement
LTIOV—latest time information is of value	SOP—standing operating procedure
NAI—named area of interest	TAI—target area of interest

DEVELOP INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION TOOLS

B-14. Intelligence officers use ISR synchronization tools with staff input to synchronize the entire collection effort, including all assets the commander controls, assets of lateral units and higher echelon units and organizations, and intelligence reach to answer CCIRs. Table B-2 describes the subordinate "Develop ISR Synchronization Tools" activities and lists the G-2/S-2's responsibilities and products. Figure B-3 (page B-8) is an example of an ISR synchronization matrix.

Table B-2. Develop ISR synchronization tools

Evaluate resources
Note. See MIHB 2-50 for asset capabilities and limitations. The intelligence officer and staff take the prioritized requirements and match them with suitable ISR assets using the following criteria.
Availability. • Know the collectors and processors available at the unit's echelon, at echelons above and below, and know how to access the ISR assets. • Determine higher echelon and other Service asset availability by reviewing various scheduling and tracking mechanisms. • HUMINT assets are not linked to traditional schedules; their availability is linked to geographic access, support relationships, and workload.
Capability. Capability includes— • **Range.** What is the asset's ability to move and maneuver, including travel and support times? If the best asset is a UAS, what are its transit and dwell times? • **Day and night effectiveness.** Consider factors such as available optics and thermal crossover. • **Technical characteristics.** Can the system see through fog or smoke? Can it continue despite hostile EW? Each asset has time factors for task accomplishment to be considered. • **Reporting timeliness.** • **Geolocation accuracy.** • **Durability.** Can the aircraft launch in high winds or limited visibility? Can the prime mover go across restricted terrain?
Evaluate resources
Sustainability. • Consider the collection asset's sustainability for extended duration operations. • The longer the collection period on the ISR synchronization matrix, the more difficult it is to find assets for continuous activity. • Weather can significantly affect sustainability of certain ISR assets. • Redundancy is one solution to the sustainability problem.
Vulnerability. • Evaluate the threat's ability to locate, identify, and destroy ISR assets. • Evaluate the collector's vulnerability to threat forces in the target area and along the entire travel route.
Performance history. • Which ISR assets are relied on to meet the commander's intelligence requirements? • Consider readiness rates, responsiveness, and accuracy over time.
Develop ISR synchronization matrix and overlay (See figure B-3 [page B-8].)
Consider the following factors: **Redundancy.** • Use of same type assets to cover the same NAI. • Use of redundant tasking when the probability of success by any one system is low. • Use of redundancy improves the chance of accurate geolocation. **Mix.** • Complementary coverage by a combination of assets from multiple units. • Sensor mix increases the probability of collection, reduces the risk of successful threat deception, facilitates cueing, and provides more complete reporting. **Cue.** • Use of one or more sensor systems to provide data that directs collection by other systems. • Cueing maximizes the efficient use of finite ISR assets to support multiple, often competing, intelligence collection priorities.

Table B-2. Develop ISR synchronization tools (continued)

Develop ISR tasks, RFIs, and requests for collection or support
ISR task. • Intelligence and operations officers work to convert the SIRs into ISR tasks using organic ISR assets—these tasks are published in Annex L of the OPORD or FRAGO. • Tailor the reporting criteria to the capabilities of the tasked ISR asset. For example— ▪ **SIR:** Will more than 20 insurgents, subordinate to the Mahdi Army or Muqtada Al-Sadr, pass through NAI 8 between 041800 and 052000 March? ▪ **ISR task:** Report the presence of Mahdi Army personnel in NAI 8 between 041800 and 052000 March. Specify direction of movement, numbers, and types of vehicles. LTIOV: 060400 March. ▪ **SIR:** Is there normal activity in the city of Fallujah, NAI 10 on 21 June? ▪ **ISR task:** Report the presence of threat counterreconnaissance activity in NAI 10 between 210900 and 211800 June. LTIOV: 211800 June.
Develop ISR tasks, RFIs, and requests for collection or support
• Prioritize ISR tasks for the ISR assets. Be specific. However, avoid overly restrictive reporting guidelines. • Include instructions for direct dissemination of combat or targeting information to the original requestor. • Tailor the ISR task to the selected collection system or organization. For example— ▪ Some imaging systems require a basic encyclopedia number rather than a geographic or universal transverse Mercator coordinate for target location. ▪ USAF airborne collection platforms recognize geographic coordinates only. ▪ HUMINT collectors require specific timeliness, reporting, and dissemination guidance.
RFI. • Used when unable to satisfy a collection requirement through organic assets. • Submitted to the next higher echelon (or lateral units) for integration within that unit's ISR plan. • At each echelon, the requirement is validated and a determination made as to whether or not that echelon can satisfy the requirement. If no, the requirement is passed to the next higher echelon. This process continues until the requirement is satisfied, the intelligence is no longer needed, or it is determined that the requirement cannot be satisfied. • Alert the submitting organization of the RFI's status—accepted for action, passed to another organization for action, returned without action (invalid or infeasible request), or closed (satisfied). • Track all production requirements, particularly those transmitted to higher echelons. • When a requirement is satisfied or overcome by events, notify the higher headquarters that the requirement is closed.
Develop and synchronize production requirements
• G-2/S-2 coordinates and plans intelligence analysis and production activities to provide timely and relevant intelligence products to commanders, staff, and subordinate forces. • Use the ISR synchronization matrix to plan production activities and timelines to answer CCIRs. • Intelligence production involves analyzing information and intelligence and presenting intelligence products, assessments, conclusions, or projections regarding the AO and threat forces in a format that assists the commander in achieving situational understanding. • Continuously evaluate the success of production based on commanders' and staffs' satisfaction.

AO—area of operations
CCIR—commander's critical information requirement
EW—electronic warfare
FRAGO—fragmentary order
HUMINT—human intelligence
ISR—intelligence, surveillance, and reconnaissance
LTIOV—latest time information is of value
MIHB—military intelligence handbook
NAI—named area of interest
OPORD—operation order
RFI—request for information
USAF—U.S. Air Force
UAS—unmanned aircraft system

	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		UAS PLT4																									
14	**BCT ASSETS**	COLT PLT																									
15		**CAB 1**																									
16		**CAB 2**																									
17		**FA**																									
18																											
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		**ELINT**																									
32	**EAB ASSETS**	**CI**																									
33		**HUMINT**																									
34		**SF/LRS**																									
35		*LOCAL*																									*LOCAL*

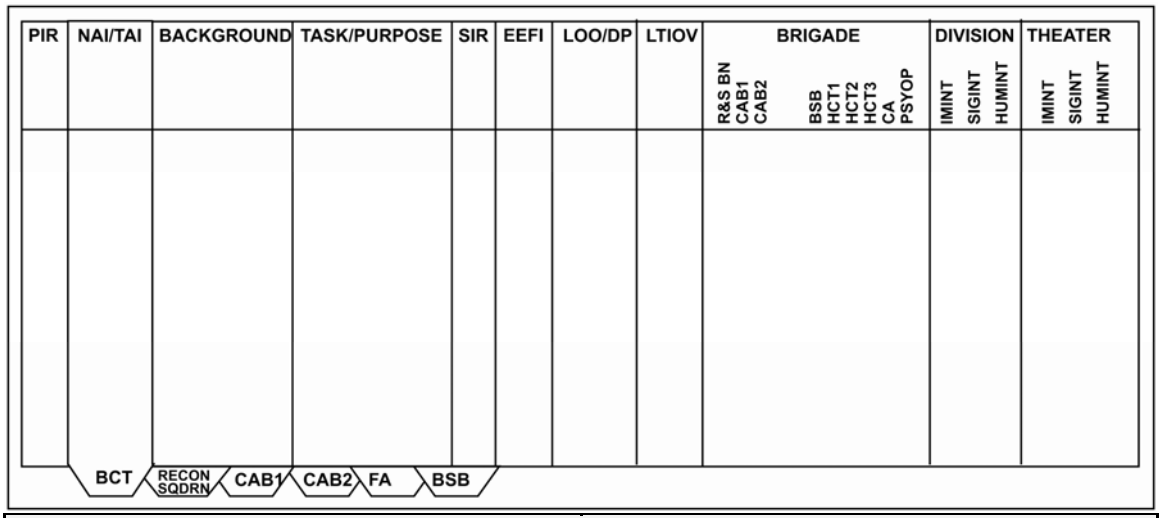
BCT—brigade combat team
BSB—brigade support battalion
CAB—combat aviation brigade
CI—counterintelligence
CO—company
COLT—combat observation and lasing team
COMINT—communications intelligence
DTG—date-time group
EAB—echelons above brigade
ELINT—electronic intelligence
EQ—equipment
FA—field artillery
FLT—flight
HCT—HUMINT collection team
HUMINT—human intelligence
IMINT—imagery intelligence
ISR—intelligence, surveillance, and reconnaissance
LRS—long-range surveillance
MI—military intelligence
MTI—moving target indicator
PLT—platoon
RECON—reconnaissance
SF—Special Forces
SQDRN—squadron
SURV—surveillance
TRP—troop
UAS—unmanned aircraft system

Figure B-3. Example ISR synchronization matrix

B-15. The ISR synchronization matrix does not provide details regarding technical channels of the ISR effort. In OIF, S-2s use a working matrix to assist in managing this effort and to help analysts. Figure B-4 is an example of a working matrix. As a tool, the working matrix—

- Links PIRs to the commander's 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 formatted as a spreadsheet and comprised of individual worksheets for the brigade and the subordinate battalions.
- Is posted to the unit's Web page and updated as needed by the G-2/S-2 at each echelon.

- Is not a tasking document and is not published as part of the base order.
- Is a working aid that assists the intelligence staff in synchronizing internal operations across echelons.



BCT—brigade combat team
BN—battalion
BSB—brigade support battalion
CA—civil affairs
CAB—combat aviation brigade
DP—decision point
EEFI—essential element of friendly information
FA—field artillery
HCT—HUMINT collection team
HUMINT—human intelligence
IMINT—imagery intelligence
LTIOV—latest time information is of value
NAI—named area of interest
PIR—priority intelligence requirement
PSYOP—psychological operations
R&S—reconnaissance and surveillance
RECON—reconnaissance
SIGINT—signals intelligence
SIR—specific information requirement
SQDRN—squadron
TAI—target area of interest

Figure B-4. Example working matrix

SUPPORT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION

B-16. During ISR integration, responsibility for ISR planning transitions from the G-2/S-2 to the G-3/S-3. ISR synchronization and ISR integration result in a fused effort focused on answering the commander's requirements through ISR tasks translated into orders. (See table B-3 [page B-10].)

B-17. The key to successful reconnaissance and surveillance is an ISR plan that—

- Is developed from well-reasoned enemy situation overlays, course of action (COA) statements, and event templates and matrices.
- Is driven by the CCIRs and focused on command directed tasks.
- Is linked to the commander's decisions points.
- Facilitates the commander's visualization of the AO.
- Is prepared jointly by the G-3/S-3, G-2/S-2, and their staff.
- Remains synchronized with the scheme of maneuver.
- Is issued and updated as part of the orders process.
- Assigns appropriate collection tasks to subordinate units.
- Requests intelligence support as needed from higher and adjacent units.

Table B-3. Support ISR integration

Develop the ISR plan
• The G-3/S-3 assigns tasks based on LTIOV and limitations of available ISR assets. • The G-2/S-2 assists the G-3/S-3 in ensuring intelligence requirements are identified, prioritized, and validated. • The G-2/S-2 also assists the G-3/S-3 in ensuring an ISR plan is developed and synchronized with the overall operation. • The G-2/S-2 coordinates with the staff and the ISR assets' commander. For example, the MI company commander coordinates sustainment of ISR assets on the battlefield.
Issue the WARNO, OPORD, FRAGO
The basis of all R&S missions is the ISR plan published in Annex L of the OPORD and continually modified through FRAGOs. There are many supporting documents developed by the G-3/S-3 and G-2/S-2 then submitted to the commander for approval: **Base OPORD** • Paragraph 3a(3), R&S (Commander's Intent). • Paragraph 3a(4), Intelligence (Commander's Intent). • Paragraph 3b, Tasks to Maneuver Units (Collection Tasks). • Paragraph 3c, Tasks to Subordinate Units (Collection Tasks). • Paragraph 3d(2), CCIR (PIR/FFIR). • Paragraph 3d(7), Limit of Reconnaissance. • Paragraph 3d(8), AOs (for the intelligence warfighting function). **Annex B (Intelligence)** • Paragraph 2, Mission. • Paragraph 3a, Scheme of Intelligence. • Paragraph 3b, Tasks to Subordinate Units. • Paragraph 3d(2), RFIs. • Paragraph 3d(5), Distribution of Intelligence Products. • Appendix 2, ISR Synchronization Matrix. • Appendix 2: Tab A, ISR Overlay. **Annex L (ISR)**
AO—area of operations CCIR—commander's critical information requirement FFIR—friendly force information requirement FRAGO—fragmentary order ISR—intelligence, surveillance, and reconnaissance LTIOV—latest time information is of value MI—military intelligence OPORD—operation order PIR—priority intelligence requirement R&S—reconnaissance and surveillance RFI—request for information WARNO—warning order

DISSEMINATE INFORMATION AND INTELLIGENCE

B-18. Dissemination includes intelligence sharing and granting access to databases, information, or intelligence for others to conduct intelligence reach. It also encompasses posting information to unit Web pages and the intelligence and ISR data required to update the common operational picture (COP). Table B-4 describes the subordinate "Disseminate" activities and lists the G-2/S-2's responsibilities.

B-19. There are three channels through which commanders and their staffs communicate:

- **Command channel.** The command channel is the direct chain-of-command link that commanders, or authorized staff officers, use for command-related activities. Command channels include command radio nets, video teleconferences, and the Maneuver Control System.
- **Staff channel.** The staff channel is the staff-to-staff link within and between headquarters. The staff uses the staff channel for control-related activities. Through the staff channel, the staff coordinates and transmits intelligence, controlling instructions, planning information, and provides early warning information and other information to support command and control (C2). Examples of staff channels include the operations and intelligence radio net, telephone, the staff huddle, video teleconference, and the warfighting function-specific components of DCGS-A to provide information and intelligence to the rest of the intelligence architecture.
- **Technical channel.** Staffs typically use technical channels to control specific activities. These activities include fire direction and the technical support and SCI reporting channels of intelligence and ISR operations. The SIGINT tasking and reporting radio net, intelligence

broadcast communications, and the wide area networks supporting single intelligence discipline collection, processing, and production are examples of technical channels.

Table B-4. Disseminate

Arrange for direct dissemination
• Have ISR assets report directly to the unit requiring the information for decisions. • This dissemination method is written into the ISR task or RFI if the G-2/S-2, with the commander's approval, requires the unit to execute it. Include the required coordinating information, such as call signs, frequencies, and routing addresses. • If the G-2/S-2 allows the asset to report directly to the requesting unit, the intelligence staff provides the G-2/S-2 with a copy of the information to update the ISR synchronization tools. • Direct dissemination is commonly used for fires and air defense units, and the target nomination process.
Determine perishability
• Determine what information will bypass intelligence processing functions and delivered directly to the commander for decisionmaking based on LTIOV. • Set alarms for critical intelligence using DCGS-A tools to alert analysts of the information's arrival.
Determine quantity
• Provide precise amounts of information to commanders and staffs to support their decisionmaking while avoiding overwhelming them with unnecessary detail or compromising security techniques, means, and sources. • Evaluate each element of reported information against the decisions, requirements, and supporting SIRs and ISR tasks for the identified consumer. • Ensure that SCI is not disseminated to unauthorized users. • Legal restrictions may prohibit information dissemination to multinational forces.
Determine dissemination methods
Dissemination methods are unique to each unit and usually specified by SOPs. • At a minimum, plan for primary and alternate dissemination methods (redundant means and pathways) for intelligence or reporting that supports CCIRs and decisionmaking. • Coordinate with operations and signals staff to determine the available dissemination methods. • Continuously monitor the status of the dissemination means.
Identify dissemination media
Choose the correct dissemination media to ensure timely delivery of mission-critical and time-sensitive information: • **Voice.** Most useful when speed in the transmission of small amounts of information is critical. • **Graphics and text dissemination.** Use graphics for information on disposition, composition, and strength; use text for the other threat characteristics. • **Messenger with a hardcopy.** Least desirable; however, if the messenger is well briefed, this technique is effective for user understanding.
Identify dissemination media
When disseminating information, the intelligence officers ensure the staff— • Uses the precedence coding system (FLASH, PRIORITY)—careful not to deflate the value of the highest precedence codes. • Is proficient at operating automated systems and familiar with message formats. • Answers questions about accuracy, source, and completeness. • Disseminates essential information to all appropriate commanders and staff sections and informs them of what is available. ***Note.*** The act of posting intelligence reports on a Web page or uploading a new database is not dissemination.
Develop audit trail
Coordinate with the signals officer to develop audit trails to ensure all appropriate commanders and staff sections receive each report only once. Audit trail techniques include— • Providing columns on the ISR plan to record messages received that satisfy an ISR task and where messages were sent. • Developing a matrix separate from the ISR plan, with "time received" and "sent to" on one axis and "ISR tasks" on the other axis. • Annotating the dissemination list directly into a message's remarks section. ***Note.*** A collection and dissemination journal is a simple method for tracking *who* sent *what* messages. Automation is especially useful—relational databases and automated journals allow complete and thorough cross-indexing, which solves many of the problems intelligence officers usually experience when relating requirements to reports and tracking dissemination.

Table B-4. Disseminate (continued)

Database management
Database managers address database development, management, and maintenance; data sources; information redundancy; import and export standards; data management; update and backup procedures; and data mining, query, and search protocols. • **Establishing new databases.** Have SOPs for establishing new databases to ensure all unit databases conform to minimum standards established by unit automation personnel. Establishing new databases prevents storage duplicate data and mixing of information to be stored at different classification levels and with different security or access requirements. • **Data entry.** Have SOPs for data entry standards that include specific formats and standardized naming conventions and fields (based on the category of information entered into the database). For example, standardizing data entry on an IED with a primary field of "IED" and a secondary field specifying IED "type" (such as VBIED, remote-controlled IED, or explosively formed projectile) allows the analyst to conduct an organized search for information and intelligence. • **Security protocols.** Establish protocols: ▪ Ensure authorized personnel can access the network, system, or database. ▪ Prevent the import or export of data, based on accesses or classification levels, to unauthorized networks, systems, or databases. • **Associated applications.** Ensure the appropriate software applications are legally installed on their systems so that relevant databases can be created and accessed and that the data can be appropriately manipulated in order to support the unit's mission. • **Data sources.** ▪ As early as possible, identify data sources required during the mission to ensure required communications and security authorizations are appropriately coordinated. ▪ May require different computer systems to access all the necessary data sources required for the mission. • **Database normalization.** Have SOPs for database normalization to minimize data redundancy in a database. • **Import and export standards.** A standardization of import and export protocols ensures transferred databases are accessible immediately upon transfer. The DCGS-A enterprise open architecture should assist in importing and exporting databases. • **Update and backup procedures.** Have a plan for updating software on networks and systems. Have procedures in place to backup the data on networks and systems to prevent a loss if hardware or software fails. Establish a system of archiving data.

CCIR—commander's critical information requirement	PIR—priority intelligence requirement
DCGS-A—Distributed Common Ground System–Army	RFI—request for information
ISR—intelligence, surveillance, and reconnaissance	SCI—sensitive compartmented information
LTIOV—latest time information is of value	SIR—specific information requirement
MI—military intelligence	SOP—standing operating procedure
OPORD—operation order	VIED–vehicle-borne improvised explosive device

ASSESS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE OPERATIONS

B-20. Assessment of ISR operations allows the staff to determine if the system is satisfying all requirements. Table B-5 describes the subordinate "Assess ISR Operations" activities and lists considerations.

Table B-5. Assess ISR operations

Monitor operations
Through coordination with the G-2/S-2, the staff knows *when* and *what* critical information is 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. DST is the staff's other critical tool for the staff, which has a complete copy of the DST to ensure the ISR synchronization matrix does not miss collection requirements. The intelligence officer— • Tracks the flow of the operation against the requirements and ISR synchronization matrices. • As necessary, prompts subordinate commanders and collectors to keep their reporting synchronized with the operation and the commander's needs. • Establishes a system to evaluate all reports, including reports going directly from the collector to the user. • Establishes a system that allows the intelligence section to monitor synchronization and evaluates if the intelligence system meets requirements without delaying intelligence dissemination.
Correlate reports to requirements
• The staff tracks ISR tasks and the PIRs from which they originate to ensure the collected information was provided to the original requester. • The tracking allows the staff to determine quickly which asset is available for retasking.
Screen reports
The G-2/S-2 staff screens each report received for the following criteria: • **Relevance.** Does the information actually address the tasked ISR task? If not, can the information satisfy other requirements? • **Completeness.** Is essential information missing? (Refer to the original ISR task.) • **Timeliness.** Has the collector reported by the LTIOV established in the original ISR task? • **Opportunities for cueing.** Can this system or another system take advantage of the new information to increase the effectiveness and efficiency of the overall ISR effort? If the report suggests an opportunity to cue other assets, take immediate action to do so and record any new requirements into the ISR plan and audit trail. If the report satisfies the ISR task, make the appropriate entry in the tracking log or register of intelligence requirements and disseminate the final intelligence to the requestor. Coordinate with the requestor to ensure the requestor also considers the requirements satisfied. If the report only partially satisfies the ISR task, annotate in the audit trail or register what was accomplished and what remains to be done.
Provide feedback
The staff— • Provides essential feedback to all the ISR assets—usually provided through the unit's C2 element. • May provide additional information on its collection or analysis if the G-2/S-2 indicates what is needed.
C2—command and control DST—decision support template ISR—intelligence, surveillance, and reconnaissance LTIOV—latest time information is of value PIR—priority intelligence requirement

UPDATE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE OPERATIONS

B-21. Updating ISR operations is the adjustment of the overall ISR plan to maintain ISR synchronized, collection, and exploitation capabilities optimized as the current situation changes. As SIRs and, subsequently, PIRs are answered, the G-3/S-3, in coordination with the G-2/S-2 and staff, updates the ISR plan and refocuses assets to answer other or new ISR tasks within the constraints of the mission variables—mission, enemy, terrain and weather, troops and support available–time available and civil considerations (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 linked to the headquarters requirements process, and the staff updates the ISR plan in a dynamic environment. Table B-6 describes the subordinate "Update ISR Operations" activities and lists considerations.

Table B-6. Update ISR operations

Maintain ISR synchronization
The intelligence staff stays alert to changes in the ISR plan resulting from changes to the LTIOV or other changes. If the branches and sequels were considered in the original plan adjustments, minor variances can be adjusted automatically by the staff. Unanticipated situations—such as a friendly force aircraft crash or shoot down, loss of a UAS asset to enemy fire, mechanical failure, or loss of signal—may require dynamic or ad-hoc tasking of additional ISR assets.
Cue assets to other collection opportunities
Cueing opportunities, whether prompted through combat information or analysis, allow intelligence officers to satisfy requirements more efficiently than previously planned.
Eliminate satisfied requirements
Once a requirement is satisfied or irrelevant, it should be eliminated. Requirements require continuous coordination with the agency that generated the original requirement. When higher headquarters declares a requirement satisfied, the requirement should be eliminated from the ISR synchronization matrix and the ISR plan, and other logs and records should be updated.
Develop and add new requirements
As the operation unfolds and the threat situation develops, commanders generate new requirements that lead to— • Updating the ISR synchronization tools. • Prioritizing the new requirements against the remaining requirements. • Consolidating the new requirements with the existing requirements. • Reprioritizing the requirements. • Evaluating resources based on newly developed requirements and priorities. • Making appropriate recommendations to the commander and the operations officer.
Recommend redirecting assets to unsatisfied requirements
Retasking is assigning an ISR asset a new task and purpose to ensure intelligence and operational synchronization. After eliminating satisfied requirements from the ISR plan, reevaluate each ISR asset based on its capability. Operations officers with input from the intelligence officers redirect ISR assets and units within the AO. Focus the ISR asset on the most important unsatisfied requirements. Redirecting an ISR asset does not change the asset's mission; instead, it updates or corrects the focus of the collection that allows the asset to more effectively execute that mission. When redirecting assets, consider— • New requirements from higher headquarters received before the completion of redirected missions. • The priority of new requirements relative to the remaining unsatisfied requirements. • The command or support relationship. • The ability of available ISR assets to respond to new missions while working on redirected missions. • Necessary responses to second- and third-order effects (see appendix E for further discussion on second- and third-order effects), branches, and sequels.
Transition to next operation
A *transition* occurs when the commander decides to change focus from one type of military operation to another (FM 3-90). Updating ISR operations can result in focus change for several ISR assets. ISR assets, as with any other unit, may require rest and refit, or employment lead-time to effectively transition from one mission or operation to another.
AO—area of operations FM—field manual ISR—intelligence, surveillance, and reconnaissance LTIOV—latest time information is of value UAS—unmanned aircraft system

Appendix C

Briefing and Debriefing Program

The commander establishes, supports, and allocates appropriate resources for a premission briefing and debriefing program. Battle updates and after-action reviews are distinct and separate tasks from the premission briefing and debriefing program. The G-2/S-2 develops a premission intelligence briefing plan and complementary debriefing plan to support the commander's program. The intelligence premission briefing and debriefing generally follow the mission-briefing format, including a review of the patrol route, mission patrol collection objectives, and methods employed.

PREMISSION INTELLIGENCE BRIEFING

C-1. The purpose of the premission intelligence briefing is to ensure all personnel conducting tactical operations, tactical movements, nontactical movements, and operational liaisons are sensitized to specific information and reporting requirements, intelligence gaps, and unique mission requirements. (For more information on operational liaison, see FM 2-91.6.)

C-2. Premission intelligence briefings may be an updated intelligence assessment or a detailed intelligence brief, depending on the nature of the mission. Missions that occur routinely, like convoy operations or presence patrols, are preceded by an updated intelligence assessment, including indicators of activity related to the commander's critical information requirements (CCIRs). Tactical operations, such as planned raids, combat patrols, or patrols that can result in site exploitation, are preceded by a more detailed intelligence briefing specific to the mission. This briefing has indicators related to the CCIRs and instructions on handling captured enemy documents and materiel. Premission briefings include reporting guidance for observed information. See FM 3-90.15 for more information on site exploitation.

KEY PREMISSION INTELLIGENCE BRIEFING POINTS

C-3. Patrols, tactical movements, and nontactical movements receive a premission intelligence briefing containing—

- Terrain impact updates.
- Civil considerations (areas, structures, capabilities, organizations, people, events [ASCOPE]) updates.
- Weather effects update.
- Threat updates.
- Route updates.
- Focus areas for observation.
- Collection requirements.
- Reporting requirements for unusual activity or lack of activity by the local population.
- Requirements for handling and disposing collected documents.
- Requirements for the handling and disposition of enemy prisoners of war (EPWs), detainees, and captured enemy materiel.
- Requirements for digital photography use.

C-4. A premission intelligence briefing provides criteria for immediate reporting requirements and nonpriority reporting requirements.

MISSION RESPONSIBILITIES

C-5. Every mission entails personnel responsibilities for the mission's success. Table C-1 provides a list of mission personnel responsibilities.

Table C-1. Mission responsibilities

Battalion S-2 and S-3 sections—
• Provide tasking and guidance on topic areas for tactical questioning based on unit PIRs. • Provide unit-focused intelligence and information, including open-source information, to help Soldiers improve their cultural knowledge and awareness of the current situation to conduct tactical questioning. • Establish a program patrols, checkpoints or roadblocks, and convoys are debriefed. • Establish procedures for immediate information reporting of critical tactical value, for example, spot report in SALUTE format. • Establish procedures for proper handling of captured equipment or media, such as cell phones, documents, or computers. • Coordinate HUMINT collection teams and other intelligence support as appropriate.
Unit commanders—
• Provide tasking and guidance to subordinate leaders on topic areas for tactical questioning based on unit tasking and guidance. • Review IPB products and disseminate information to personnel within the G-2/S-2 section to improve their knowledge of the AO. • Support the unit G-2/S-2 debriefing program and ensure that all patrols, traffic control points or roadblocks, and convoy Soldiers participate in the debriefing. • Reinforce the importance of the procedures for immediate information reporting of critical tactical value. • Are cautious about information reported by patrols and HUMINT collection teams. ***Note.*** Single-source, unanalyzed information can be misleading. When used, it should be fused with all-source analyzed intelligence or other corroborating information.
Platoon leaders—
• Provide tasking and guidance to squads, sections, patrols, checkpoints or roadblocks, and convoy leaders on topic areas for tactical questioning based on unit tasking and guidance. • Support the unit G-2/S-2 debriefing program and ensure all patrols, checkpoints or roadblocks, and convoy Soldiers participate in the debriefing. • Reinforce the importance of the procedures for immediate reporting of information of critical tactical value.
Squad/section/patrol/traffic control point/roadblock/convoy leaders—
• Train and integrate specific tactical questioning in the planning, preparation, and execution of patrols, checkpoints or roadblocks, and convoys based on unit tasking and guidance. • Prepare for and participate in the unit S-2's debriefing program (if necessary, demand the debriefing) after all patrols, traffic control points or roadblocks, and convoys. • Report information based on visual observations and tactical questioning in preparation for the debriefing or immediate reporting of information of critical tactical value. • Carefully carry out EPW/detainee and document handling during patrols, checkpoints or roadblocks, and convoys. • Conduct captured enemy materiel handling in accordance with local SOPs or OPORDs.
AO—area of operations EPW—enemy prisoner of war HUMINT—human intelligence IPB—intelligence preparation of the battlefield OPORD—operation order PIR—priority intelligence requirement SALUTE—size, activity, location, unit, time, equipment SOP—standing operating procedure

POSTMISSION DEBRIEFING

C-6. *Debriefing* is the systematic questioning of cooperating human sources to satisfy intelligence requirements consistent with applicable law. The source is usually not in custody and is usually willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments (FM 2-0). Friendly force debriefing operations are the systematic debriefing of U.S. forces to answer intelligence, surveillance, and reconnaissance (ISR) tasks. Predictive intelligence is enhanced by analyzing what is occurring within an area of operations (AO). Debriefing also facilitates situational understanding of the AO.

C-7. The purpose of debriefing is to identify and record data pertaining to assigned specific information requirements (SIRs) and ISR tasks, and any additional information and observations concerning the AO, and to collect any fliers, pamphlets, media, or pictures the patrol found or obtained.

C-8. Debriefing participants should include—

- All leaders returning from operational liaison or meetings.
- Returning patrols.
- Human intelligence (HUMINT) collection teams (HCTs).
- Helicopter pilots.
- Convoy personnel.
- Others who may have obtained information of intelligence value.

C-9. The intelligence section—

- Debriefs personnel.
- Writes and submits reports.
- Reports information verbally, as appropriate.

C-10. Table C-2 provides key debriefing points that assist the intelligence staff or command debriefing team in the debriefing process.

Table C-2. Key debriefing points

- The requirement for a debriefing by the intelligence section following each mission should be a part of the intelligence premission briefing.
- Leaders should not consider the mission complete or release mission personnel until reporting and debriefings are completed.
- Once the element (leader, patrol, convoy) returns from the mission, the intelligence staff or command debriefing team conducts a thorough debriefing.
- Debriefing should include all patrol members—the leader, unit members, and any attached personnel. In the event that the returning patrol splits into different locations, the intelligence staff should visit each location to debrief all patrol members.
- When company, platoon, or smaller elements deploy to remote locations, intelligence staff debriefings may be impossible. Platoon and company leaders conduct debriefings in accordance with standing operating procedures to ensure reports are available to the intelligence section and staff. Expeditious reporting ensures that patrol debriefing reports and additional notes are available for timely intelligence analysis.
- Like the mission briefing, the debriefing intelligence staff should review the route traveled, collection objectives of the patrol, and methods employed.
- After the debriefing, the intelligence staff should have received the patrol report, which will streamline the intelligence staff debriefing process. This allows the intelligence staff to concentrate on filling in gaps and following up on reported information.
- A practical method of debriefing is reviewing all patrol or mission actions chronologically.
- A detailed sketch provides a visual reference of debriefed patrol areas. Recalling and recording information is simplified when the information is divided into segments that flow logically. For example—
  - Use a map to determine segments of the route traveled.
  - Coordination points, checkpoints, phase lines, or significant events may divide segments.
  - Start at the beginning of the patrol route and let the patrol leader demonstrates—using the map—the route traveled.
  - Ask the patrol leader, “From Checkpoint 1 to Checkpoint 2, what did you observe?” The goal is to extract information of intelligence value.
  - Avoid requesting priority intelligence requirements only. This limits the patrol leader’s answers and increases the likelihood of missing significant information. Instead, let the patrol leader provide the information obtained while on that segment of the trip.
  - Use follow-up questions to obtain complete information. Always ask, “What else?” or “What other?” before closing a topic.
  - If the patrol used digital cameras, it is helpful to use their pictures during the debriefing.
- Once a travel segment has been fully exploited, continue to the next segment. Question the patrol leader from Checkpoint 2 to Checkpoint 3—continuing the process until the entire route has been exploited.

Table C-2. Key debriefing points (continued)

- Written report information should include—
  - Use a map to determine segments of the route traveled.
  - Size and composition of the unit conducting the patrol.
  - Mission (type, location, and purpose).
  - Departure and return date-time groups.
  - Routes. Use checkpoints and grid coordinates for each leg or include an overlay or detailed sketch.
  - Detailed description of identified terrain and threat positions.
  - Results of any contact with the local population or the threat (activities and demeanor or attitude).
  - Unit status at the conclusion of the mission, including the disposition of dead or wounded Soldiers.
  - Description of collected materiel, such as fliers, pamphlets, media, or pictures the patrol found or obtained.
- Conclusions or recommendations.

C-11. See table C-3 for more debriefing considerations.

Table C-3. Debriefing considerations

<table>
<tr><th>Sight</th><th>Hearing</th><th>Touch</th><th>Smell</th></tr>
<tr><td rowspan="2">Threat personnel, vehicles, and aircraft.
Sudden or unusual movement.
New local inhabitants.
Smoke or dust.
Unusual movement of farm or wild animals.
Unusual activity or lack of activity by local inhabitants, especially at times and places that are normally inactive or active.
Vehicle or personnel tracks.
Movement of local inhabitants along uncleared areas, routes, or paths.
Signs or evidence of threat occupation or threat trends.
Recently cut foliage or vegetation.
Muzzle flashes, lights, fires, or reflections.
Amount and type of trash.</td><td>Running engines or track sounds.
Voices.
Metallic sounds.
Gunfire (by weapon type).
Unusual calm or silence.
Dismounted movement.
Aircraft.</td><td>Warmth of coals and materials from fires.
Freshness of tracks.
Age of food or trash.</td><td>Vehicle exhaust.
Burning petroleum products.
Cooking food.
Age of food or trash.
Human waste.</td></tr>
<tr><td colspan="3">Other considerations
Armed elements: Location of factional forces, minefields, and potential threats.
Homes and buildings: Condition of the roofs, doors, windows, lights, power lines, water, sanitation, roads, bridges, crops, and livestock.
Infrastructure: Presence of functioning stores, service stations, other.
People: Numbers, sex, age, residence or status of dislocated civilians, visible health, clothing, daily activities, and leaders.
Contrast: Has anything changed? For example, are there new locks on buildings? Are windows boarded up or previously boarded-up windows now open, indicating a change of use of a building? Have buildings been defaced with graffiti?</td></tr>
</table>

Appendix D

Graphic Intelligence Reports

Intelligence personnel use a variety of formats to request, report, and disseminate information. (See TC 2-33.4.) The formats assimilate information into automated intelligence support systems, such as the Distributed Common Ground System–Army (DCGS-A). This appendix concentrates on the graphic intelligence summary (INTSUM) and the use of storyboards.

GRAPHIC INTELLIGENCE SUMMARY AND STORYBOARD

D-1. The graphic INTSUM is used by units at all echelons to convey threat situation dynamics. It is a current depiction of significant threat dispositions, activities, strengths, and weaknesses and an assessment of the most probable threat courses of action (COAs). A current, complete graphic INTSUM provides intelligence, surveillance, and reconnaissance (ISR) efficiency and enables the commander to exploit fleeting threat vulnerabilities.

D-2. A storyboard *tells a story* using bulleted points, charts, and graphs. However, it should be regarded as the story summary—containing only pertinent data. It should communicate the *who, what, where, when*, and *why/how*. Storyboards are typically used to convey significant actions to the commander.

D-3. There is not a specific format for a graphic INTSUM or storyboard. The formats for each are determined by the user of the information—namely, the commander.

GRAPHIC INTELLIGENCE SUMMARY—OFFENSIVE AND DEFENSIVE OPERATIONS

D-4. At a minimum the graphic INTSUM should contain the following information for offensive/ defensive operations. (See figure D-1 [page D-2].)

- Legend and margin information.
- Area orientation.
- Threat unit locations and mission activities.
- Threat mission capabilities assessment.
- Threat boundaries and front-line trace.
- Threat objectives.
- Threat air activity.
- Threat weaknesses and vulnerabilities.
- Threat strengths and capabilities.
- Threat intentions assessment.
- Friendly commander’s intent and priority intelligence requirements (PIRs).
- Predicted future threat activity.

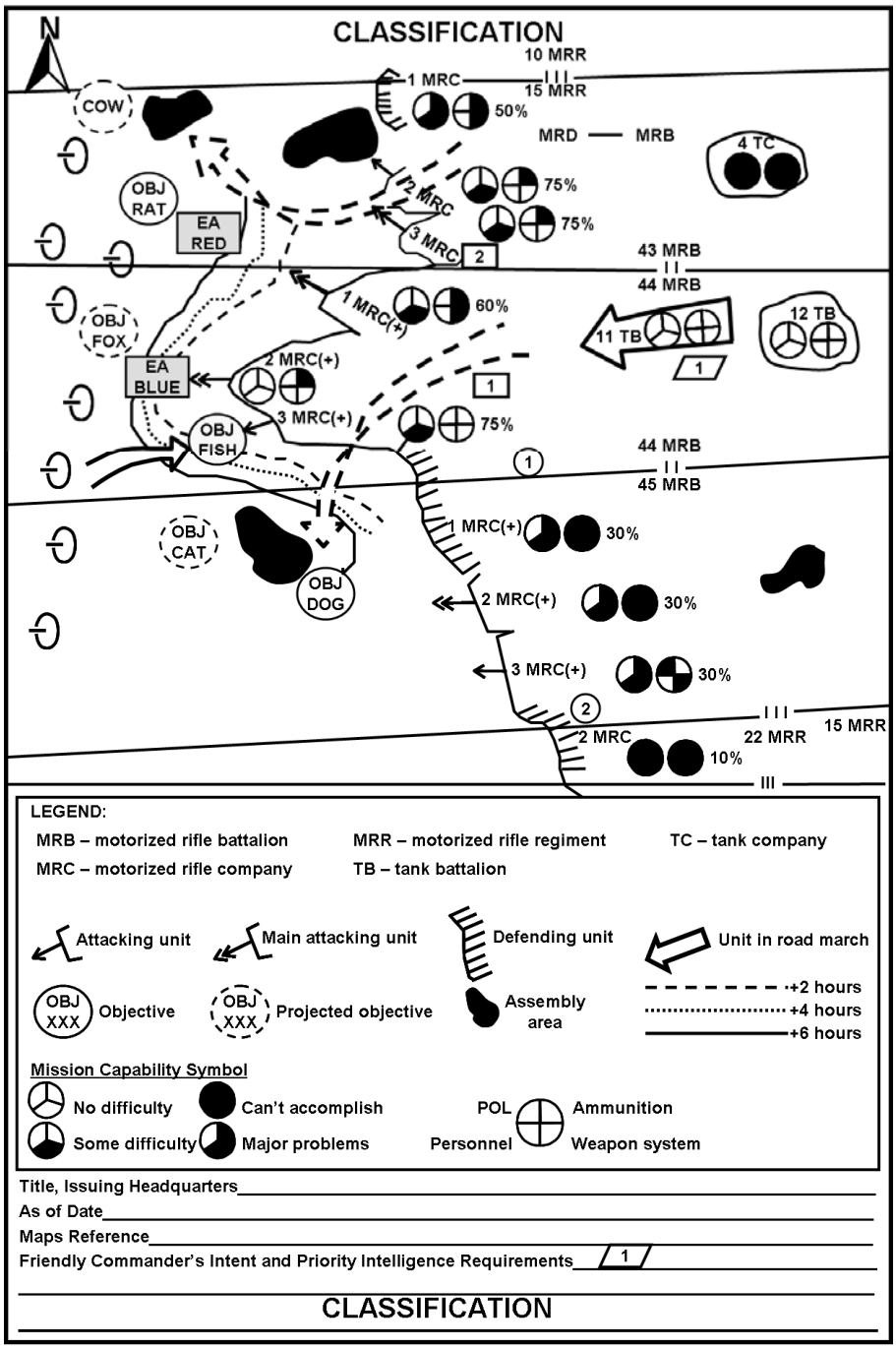


Figure D-1. One-page graphic intelligence summary example

LEGEND AND MARGIN INFORMATION

D-5. Legend and margin content information may include—

- **Classification** of the graphic INTSUM—posted on top and bottom—including a "Classified by" line and declassification instructions.
- **Title.**

- **Issuing headquarters.**
- **As of Date.** Use either local or Zulu time—this is critical since predicted threat activity is depicted based on the **As of Date** in addition to a **given number of hours**.

AREA ORIENTATION

D-6. Selected geographic features are highlighted on the overlay to orient the user to the displayed area. The features selected depend on the specific area of operations (AO) and the friendly unit's mission type.

D-7. Common features may include cities, rivers, and major relief features. Selected features for some stability operations are highlighted on a smaller scale. Highlighted features may include airports, fuel stations, housing areas, and other features that play prominently in the operation. A graphic INTSUM should provide only those features necessary for orientation.

THREAT UNIT LOCATIONS AND MISSION ACTIVITIES

D-8. Depict **committed** threat unit locations with a bracket followed by the identification. The bracket size indicates the frontage occupied by the unit. The unit's mission is depicted graphically. (See figure D-2.)

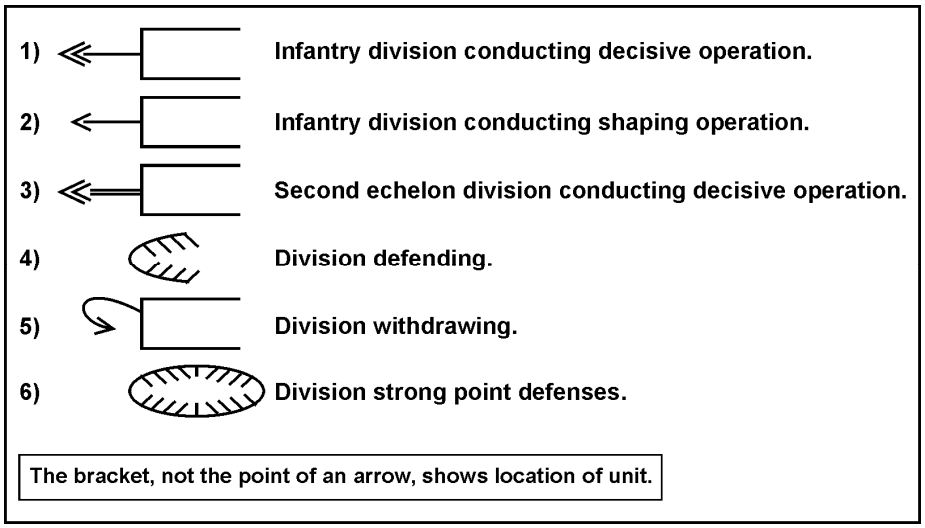


Figure D-2. Threat unit locations and mission activities (committed)

D-9. Depict **uncommitted** threat units with the symbology shown in figure D-3.

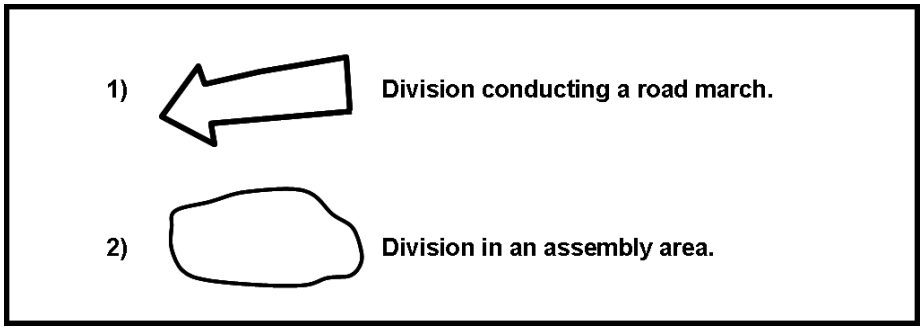


Figure D-3. Threat unit locations and mission activities (uncommitted)

THREAT MISSION CAPABILITIES ASSESSMENT

D-10. Use combat effectiveness graphics to assess and display a threat unit's capability to perform its mission. Consider all factors, tangible and intangible, in making the assessment. Include unit strength, sustainment status, maintenance and readiness status, morale, mission, terrain, and weather. Place selected symbols in the vicinity of the identified unit. (See figure D-4.)

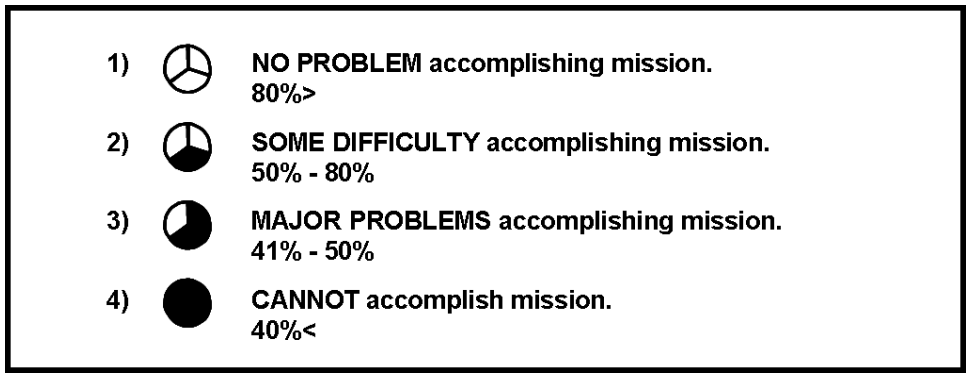


Figure D-4. Threat mission capabilities assessment

D-11. A diminished threat mission capability is usually due to one or more specific problem areas—damaged or destroyed weapons systems, a lack of ammunition, petroleum, oils, and lubricants (POL), or replacement personnel. Graphically depict the problem areas for each unit adjacent to the threat mission capabilities assessment symbol. The friendly commander can then exploit what is possibly crucial, but fleeting threat vulnerability.

D-12. Indicate specific problem areas by blackening the appropriate quadrant of the circle. The problem area categories are not static; other problem areas can be displayed on the symbol if the selection is clearly explained in the graphic. Figure D-5 shows a sample problem area symbol and an example of a problem area symbol used in conjunction with the threat mission capabilities assessment symbol.

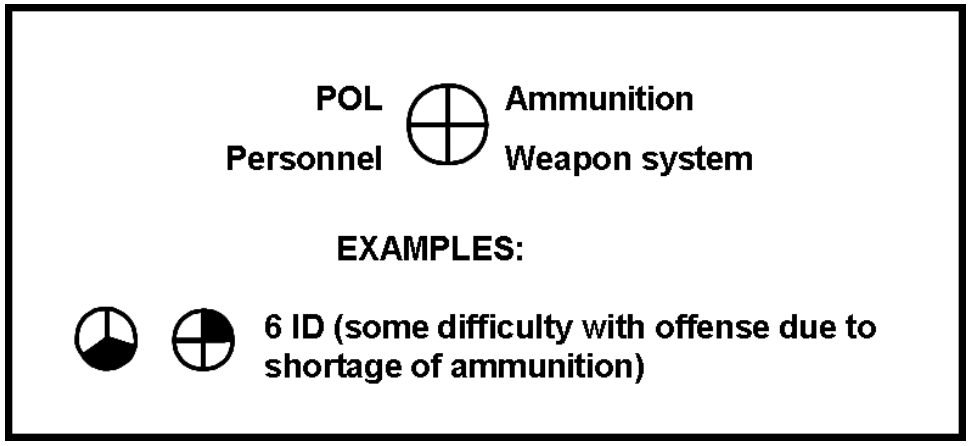


Figure D-5. Threat problem area symbology

THREAT BOUNDARIES AND FRONT-LINE TRACE

D-13. In conventional military operations, threat boundaries are depicted two echelons below the friendly unit. For example, at the brigade combat team (BCT) level, boundary lines for the threat battalion and company elements are depicted. Depicting threat boundaries beyond two echelons lower is difficult to delineate and clutters the graphic INTSUM. In some irregular warfare operations, such as support to insurgency and counterinsurgency, smaller units are the rule and constantly accounted for on the graphic INTSUM.

D-14. The front-line trace is not shown on the graphic INTSUM. The brackets depicting the threat unit, in contact, frontages is sufficient for an effective front-line trace. Addition of a front-line trace is easily confused with depicting predicted threat activity.

THREAT OBJECTIVES

D-15. If threat objectives are discernable, they will be placed on the graphic INTSUM.

THREAT AIR ACTIVITY

D-16. Depict threat air activity on the graphic INTSUM. Use an aircraft symbol with the direction of travel and total number of sorties in parentheses. Some units may opt to break down the sortie count by category, such as fighter (F), bomber (B), and reconnaissance (R). For example, a total sortie count of 12 could be depicted as (12). The same sortie count could also be depicted as (4F/6B/2R). The sortie breakdown should be used only if it does not clutter the graphic INTSUM. Include sortie breakdown symbols, such as F, B, and R. (See figure D-6.)

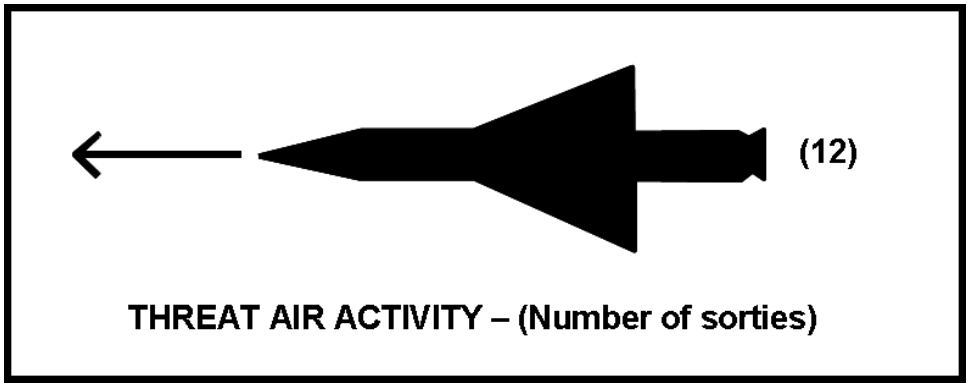


Figure D-6. Threat air activity symbology

THREAT WEAKNESSES AND VULNERABILITIES

D-17. Show specific weaknesses or vulnerabilities by using a numbered circle on the graphic INTSUM. (See figure D-1 [page D-2].) A supporting message could list threat weaknesses and vulnerabilities in narrative form.

THREAT STRENGTHS AND CAPABILITIES

D-18. Show threat strengths and capabilities by using numbered squares. (See figure D-1 [page D-2].)

THREAT INTENTIONS ASSESSMENT

D-19. Write an assessment of threat intentions and most probable COA in a concise narrative format; graphically key it to the graphic INTSUM when possible.

FRIENDLY COMMANDER'S INTENT AND PRIORITY INTELLIGENCE REQUIREMENTS

D-20. List the friendly commander's intent and PIRs in narrative format on the graphic INTSUM. Graphically key these statements to the overlay.

PREDICTED FUTURE THREAT ACTIVITY

D-21. Draw predicted lines of threat advance or withdrawal and link them to a timeline to convey information about possible future threat activity. (See figure D-7.) Predicted lines of advance or withdrawal are based on the "AS OF" time located in the legend and margin information.

Note. Predicted lines are only an aid to planners. Current threat situations must be continuously monitored to update the predictions.

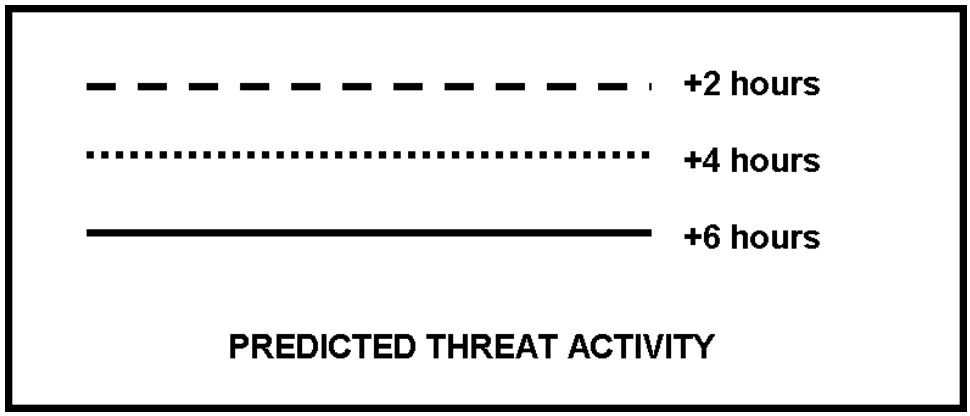


Figure D-7. Predicted threat activity timelines

GRAPHIC INTELLIGENCE SUMMARY—COUNTERINSURGENCY OPERATIONS

D-22. The graphic INTSUM may contain the following information for counterinsurgency operations:

- Legend and margin information.
- Weather.
- Significant activity (SIGACT) in the AO.
- AO executive summary.
- Indications and warning (I&W).
- Battle damage assessment (BDA) rollup.
- Special assessments, as required.
- Significant dates.
- Current threat situation template.
- Predicted threat activity—next 24 to 48-hours.
- Current commander's critical information requirements (CCIRs)/changes to CCIRs.
- High-payoff target list (HPTL).
- High-value target list (HVTL).
- Be on the look-out (BOLO) list.
- ISR plan.

LEGEND AND MARGIN INFORMATION

D-23. Legend and margin content information may include—

- **Classification** of the graphic INTSUM—posted on top and bottom—including a "Classified by" line and declassification instructions.
- **Title** of document.
- **Issuing headquarters**.

Note. Appropriate classification markings must be on every slide or page (top and bottom).

WEATHER

D-24. Weather contents may include—

- A near term weather forecast and at least a 5-day forecast for the AO, as required.
- The effects of the weather on threat and friendly operations.
- A legend if using color-coding system.
- See appendix G, for an example.

SIGNIFICANT ACTIVITIES IN THE AREA OF OPERATIONS

D-25. SIGACTs content may include—

- Summary of SIGACTs for the AO—with analyst assessment. (See figure D-8 [page D-8].)
- **Storyboard** with a detailed summary of SIGACTs. (See figure D-9 [page D-9]):
  - Location—Zone/Neighborhood with grid *(Where)*.
  - Date-time group (DTG) of the activity *(When)*.
  - Unit reporting the SIGACT and the intelligence sources *(Who)*.
  - Description of the activity *(What)*.
  - Assessment—near term analysis of threat intent and activity *(Why)*.
- Summaries of SIGACTs over time, such as improvised explosive device (IED) incidents in the last 24 hours. (See figures D-10 [page D-10] and D-11 [page D-11].)
- Map or imagery with callouts or symbols that depict *where* the SIGACT occurred and the *type* of activity.
- Grouping by unit, activity, timeframe, or operation (situation dependent).

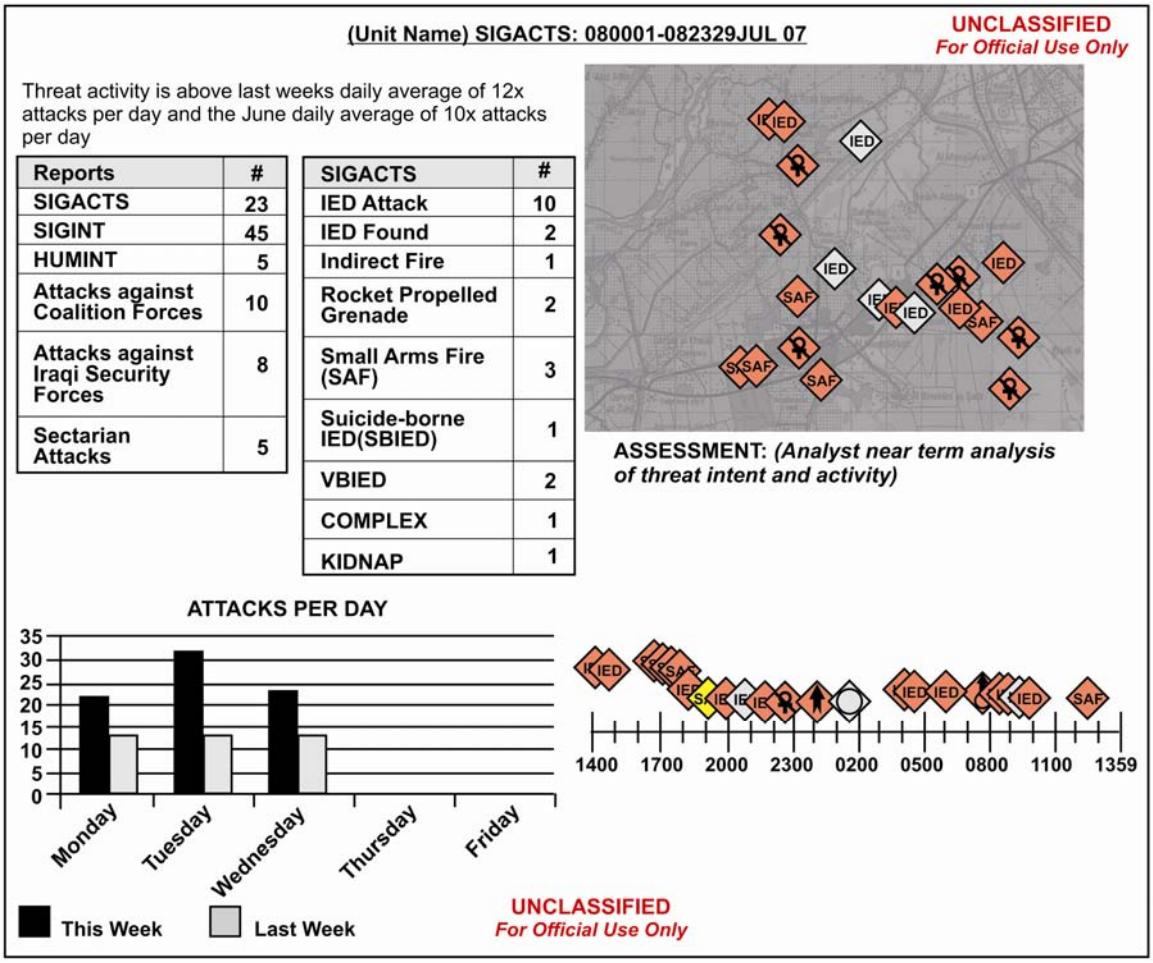


Figure D-8. Significant activities in the area of operations

UNCLASSIFIED
For Official Use Only

SAF, 1X Friendly WIA / A / 1-67 / Zone 25, Muhallah 832

Unit: A/1-67

Task: Conduct cordon and search Al Jabar

Purpose: Neutralize/destroy weapons cache site in order to deny threat use of weapons and munitions to conduct attacks in sectors.

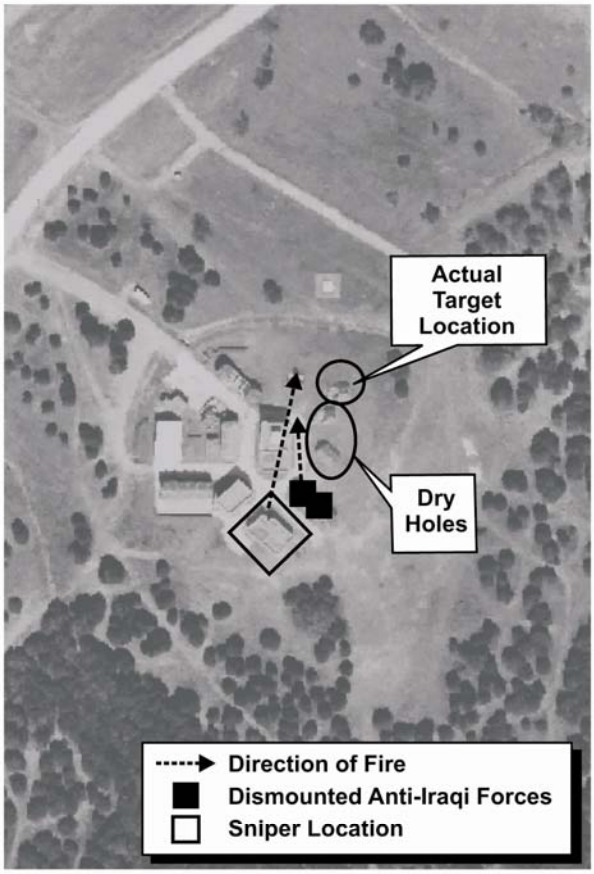
Grid: 38SMB4780070727

Category: SAF

Timeline: 081500-1525JUL 07:
At 081501JUL07, A/1-67 conducted a raid operation in the eastern section of Al Jabar (Zone 25, Muhallah [neighborhood] 832, Grid 38SMB4780070727) during the operation, they searched two locations that both resulted in dry holes. Upon receiving a tip from locals, Element-1 searched the house in the northeast corner of the village and discovered the primary target, Muhammad Al Wahabbi. Upon further search of the house, the patrol discovered 5x IEDs and 2x Rocket Propelled Grenades.

At 081510JUL07, while patrol was preparing to extract Wahabbi, they received SAF from 2x dismounted anti-Iraqi forces. The 2x dismounts escaped from the area. The attack resulted in 0x US/Iraqi Security Force casualties.

Shortly before exiting the site, at 081525JUL07, the patrol reported taking sniper fire from the southwest. The attack resulted in 1x US wounded in action (WIA). The sniper shot the soldier 1x in his shoulder.



UNCLASSIFIED
For Official Use Only

Figure D-9. Storyboard example

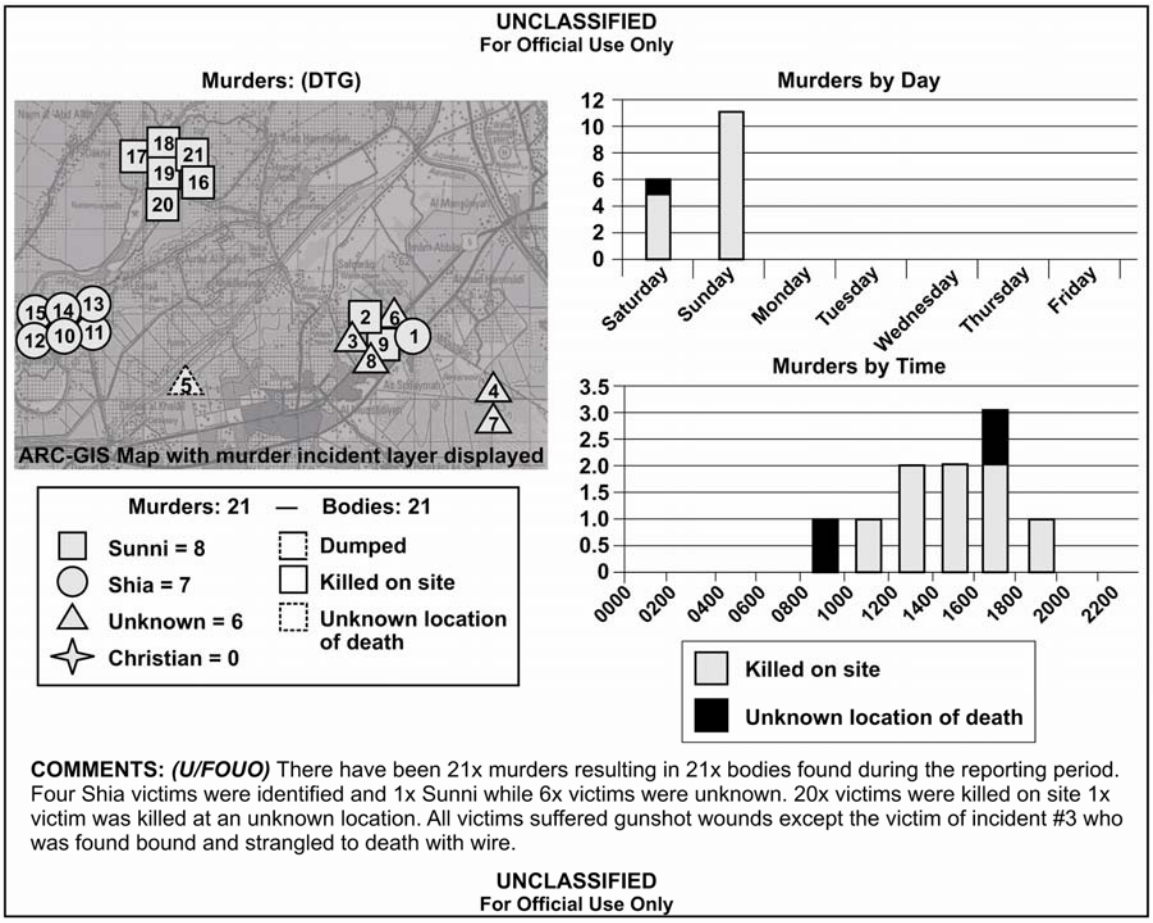


Figure D-10. Sample summary of weekly murders

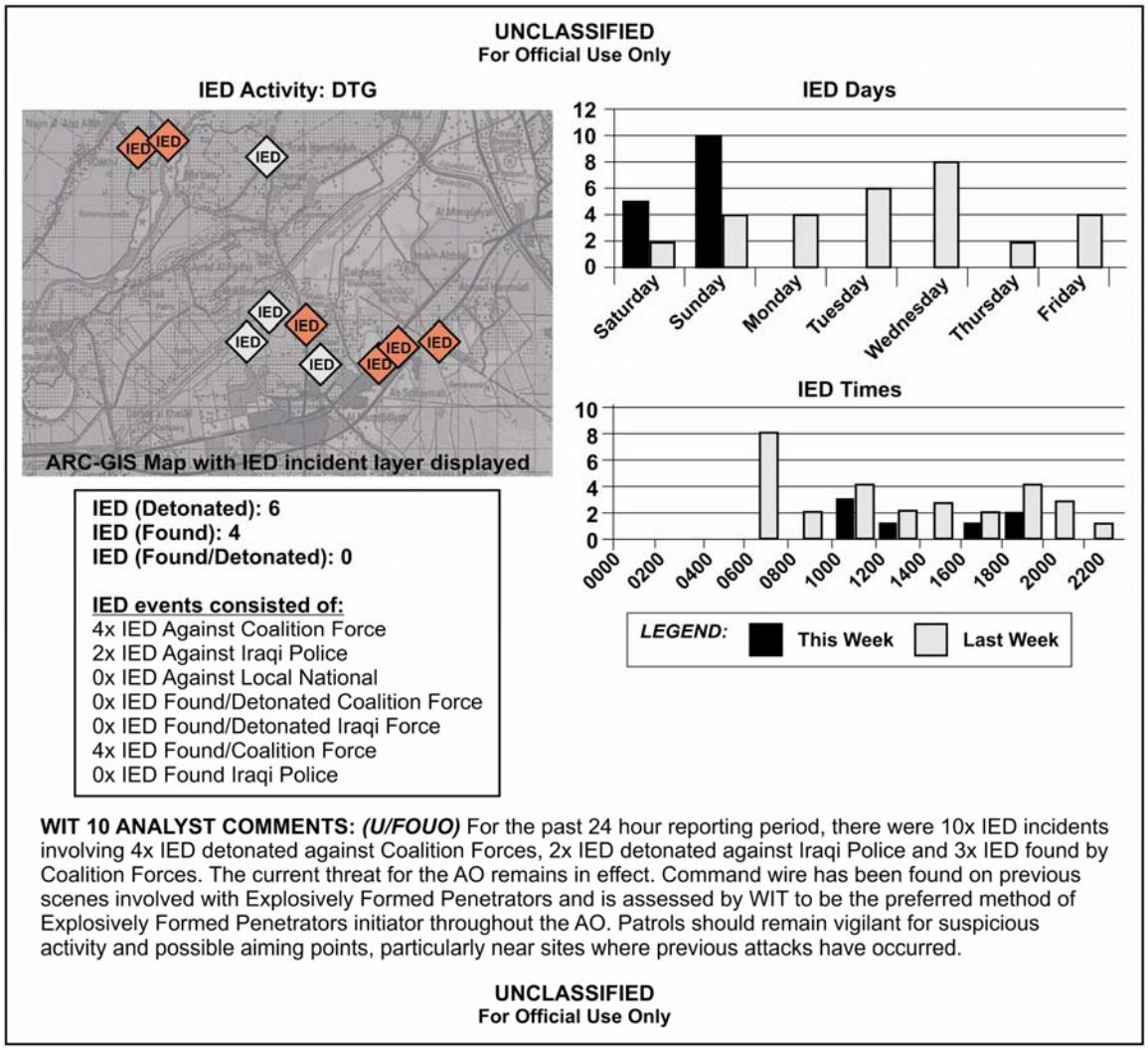


Figure D-11. Improvised explosive device activity summary

AREA OF OPERATIONS EXECUTIVE SUMMARY

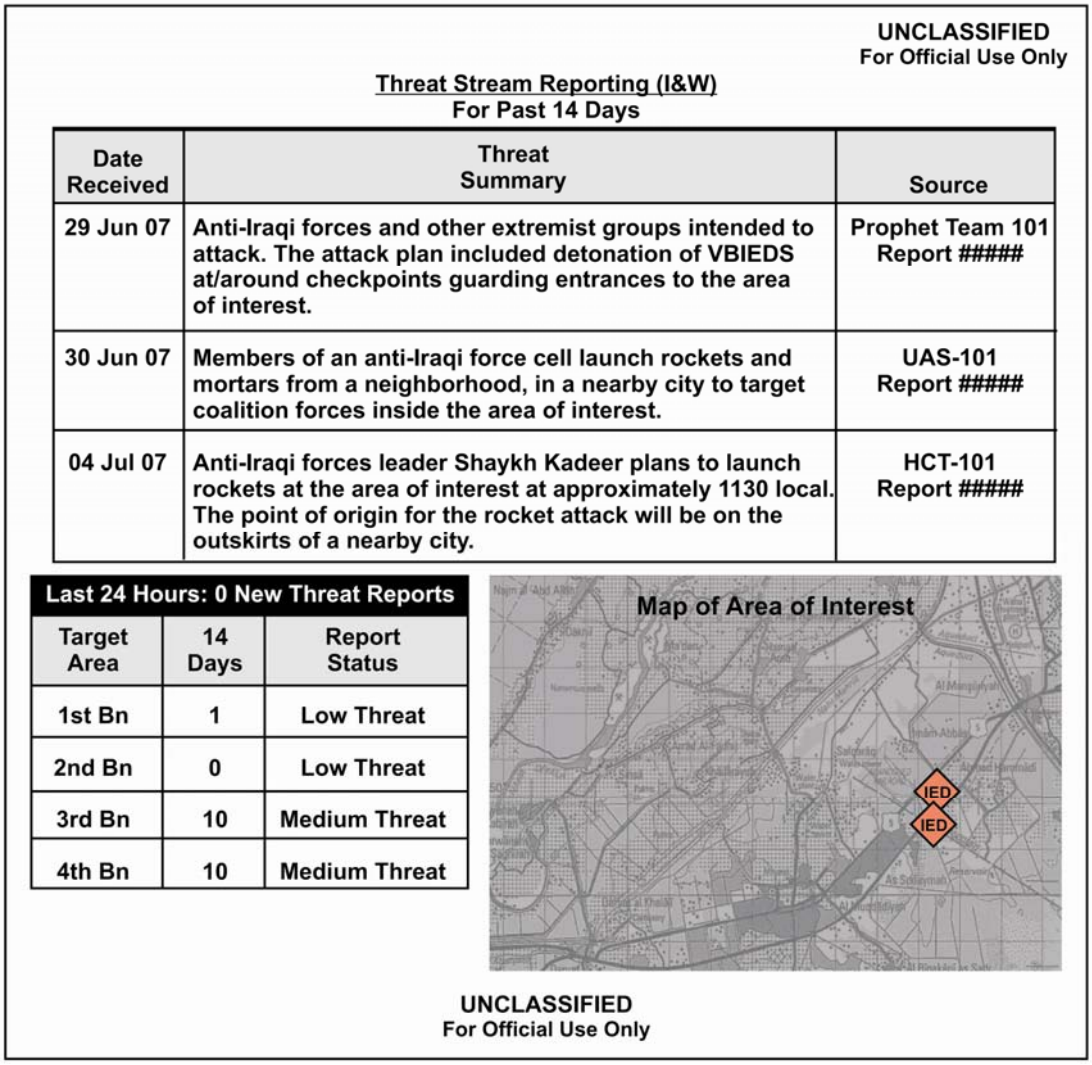
D-26. The AO executive summary contents may include—

- G-2/S-2 assessment of current threat activity within the AO and the effects on operations.
- Assessment of threat activity in each of the lower echelon S-2's AO.

INDICATIONS AND WARNING

D-27. I&W contents (see figure D-12) may include—

- Gist of the significant reports for the last two weeks.
- Map of the area of interest (AOI).
- Threat condition level.
- Grouping by intelligence source (human intelligence [HUMINT], signals intelligence [SIGINT]), or time period.



UNCLASSIFIED
For Official Use Only

Threat Stream Reporting (I&W)
For Past 14 Days

Date Received	Threat Summary	Source
29 Jun 07	Anti-Iraqi forces and other extremist groups intended to attack. The attack plan included detonation of VBIEDS at/around checkpoints guarding entrances to the area of interest.	Prophet Team 101 Report #####
30 Jun 07	Members of an anti-Iraqi force cell launch rockets and mortars from a neighborhood, in a nearby city to target coalition forces inside the area of interest.	UAS-101 Report #####
04 Jul 07	Anti-Iraqi forces leader Shaykh Kadeer plans to launch rockets at the area of interest at approximately 1130 local. The point of origin for the rocket attack will be on the outskirts of a nearby city.	HCT-101 Report #####

Last 24 Hours: 0 New Threat Reports

Target Area	14 Days	Report Status
1st Bn	1	Low Threat
2nd Bn	0	Low Threat
3rd Bn	10	Medium Threat
4th Bn	10	Medium Threat

UNCLASSIFIED
For Official Use Only

Figure D-12. Indications and warning reporting

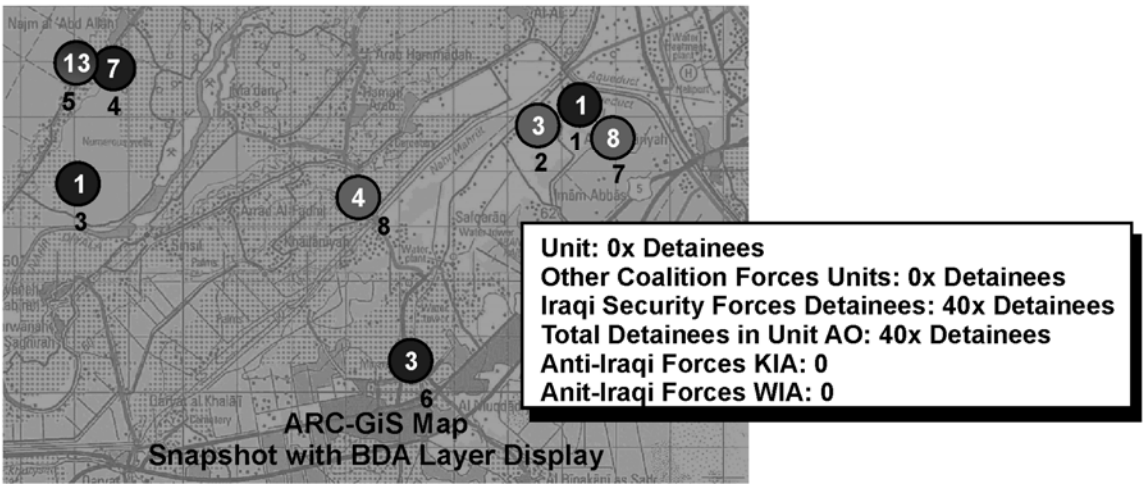
BATTLE DAMAGE ASSESSMENT ROLLUP

D-28. BDA rollup contents (see figure D-13) may include—

- Number of threat personnel wounded in action (WIA), killed in action (KIA), captured (detained) in the AO.
- Disposition of the detainees (in holding facility, released, transferred).

UNCLASSIFIED
For Official Use Only

Anti-Iraqi Forces BDA Roll Up
Past 7 Days
Day by day rollup of Anti-Iraqi Forces killed in action (KIA) / WIA / Captured in the Unit AO.



Unit	Detainees at TOA	Detainees at Holding Facitity	Detainees Released	Detainees Sent to Higher Headquarters	Detainees Transferred	Anti-Iraqi Forces Killed in Action	Cache(s)
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	32	25	0	7	0	0	0
	8	8	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
TOTAL	40	33	0	7	0	0	0

UNCLASSIFIED
For Official Use Only

Figure D-13. Sample detainee rollup

SPECIAL ASSESSMENT

D-29. The requirements for and the components of a special assessment are determined by the commander or the staff. Generally, special assessment components may include—

- Subject title.
- Synopsis of the incident or activity.
- Detailed reporting.

- Related PIRs.
- Map, imagery, or photograph.
- Analyst assessment or comments detailing the affect the incident or activity will have on future operations.

SIGNIFICANT DATES

D-30. Contents (see figure D-14) may include—

- Date.
- Event.
- Popular significance, such as special prayers, fasting, visiting holy shrines, processions.
- Level of impact on the AO—the "so what" factor.

UNCLASSIFIED
For Official Use Only

Upcoming Significant Dates

Date	*Event*	*Popular significance*	*Probable impact on the AO*
8 September	Laylat al-Bara'ah (Night of absolution)	Special prayers, fasting, larger processions around the shrines, chanting	No/Low Level of impact
8 September	Birth of the 12th Iman (Shia)	Visiting the holy shrines, processions, chanting	Low Level of impact
22 September	Iran-Iraq war begins (1980)		Low Level of impact

UNCLASSIFIED
For Official Use Only

Figure D-14. Significant dates

THREAT CURRENT SITUATION TEMPLATE

D-31. Threat current situation template contents may include—

- Threat locations.
- Threat task and purpose.
- Threat capabilities assessment.
- Threat AOs.
- Threat weaknesses and vulnerabilities.
- Threat strengths and capabilities.
- Threat intentions assessment.

PREDICTED THREAT ACTIVITY—NEXT 24 TO 48 HOURS

D-32. Contents (see figure D-15) may include—

- Continuous threats in the AOI.
- Threats expected in the next 24 to 48 hours.
- Description of activity expected.
- DTG or hours activity is expected.
- Map or imagery of AOI with threat activity depicted.

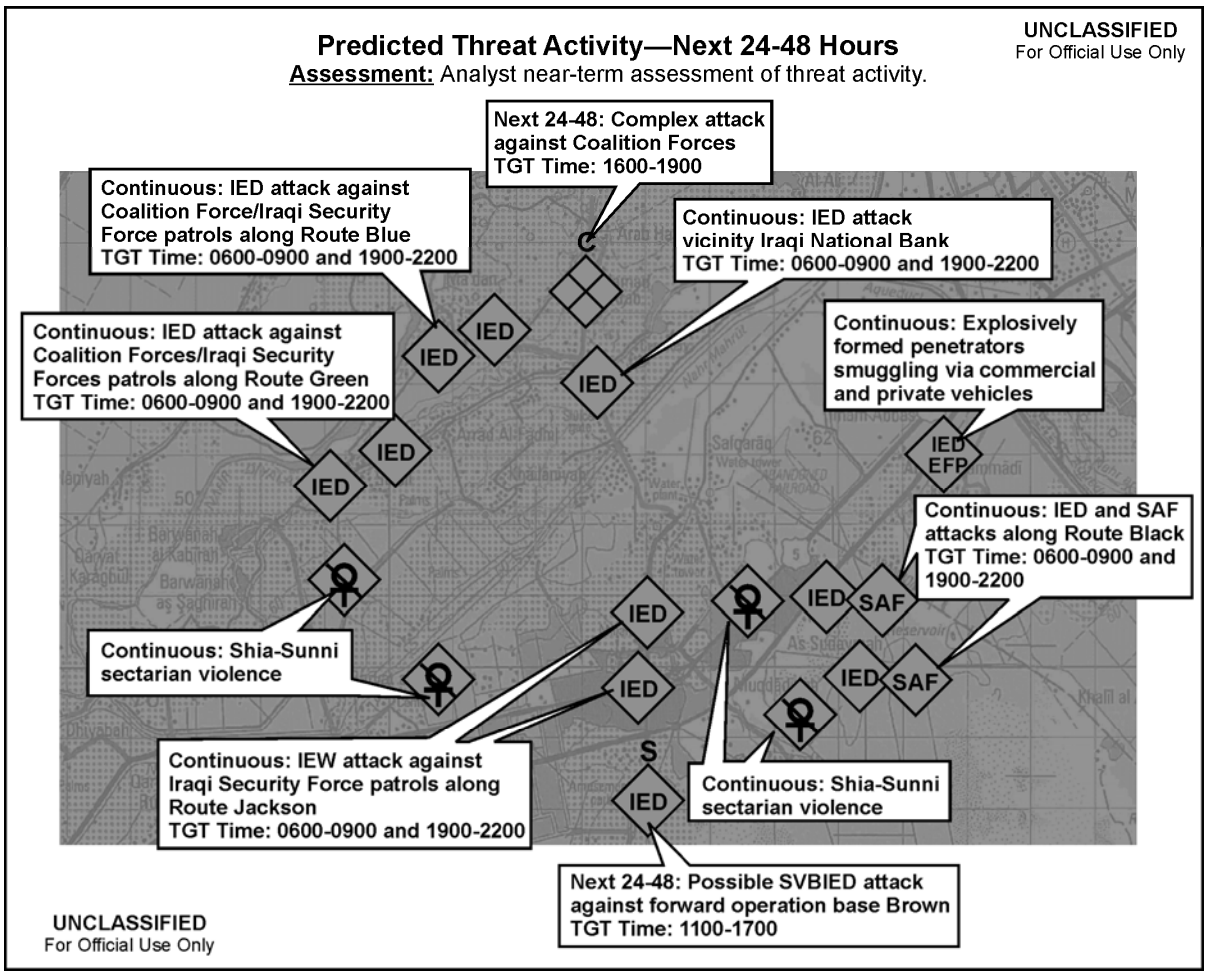


Figure D-15. Predicted threat activity—next 24-48 hours example

HIGH-PAYOFF TARGET LIST

D-33. HPTL contents may include—

- Current HPTL (prepared by targeting officer).
- Highlighted HPTL changes or new additions.

HIGH-VALUE TARGET LIST

D-34. HVTL contents (see figure D-16 [page D-16]) may include—

- Target number.
- Unit.
- Target value analysis (TVA).
- Individual's description (as detailed as possible).
- Execution criteria.
- Photo.

D-35. See appendix E for more information.

UNCLASSIFIED
For Official Use Only

High-Value Target List

Target # unit	*Version 045, 06Jul07*	*Execution criteria*	*Status/photo*
BCT ***(Cavalry)*** ***TVA #***	***Sheik Samee—*** • Is anti-Iraqi force cell leader and Imam of the neighborhood mosque. • Receives logistic support from Jeff regularly. • Is associated with Sheik Tamir (detained), Sabir (detained), and Sheik Sabir. • Used the mosque to screen, torture, and kill Sunni Muslims in the area. Use of mosque as a torture facility can be verified by several HUMINT reports and accounts of a kidnapped Iraqi released due to Shia status.	PID Source Location Trigger Evidence	No photo available
BCT ***(Infantry)*** ***TVA #***	***Kadeer (last name unknown)—*** • Is anti-Iraqi force cell leader and facilitator living in Muhallah ### in a city neighborhood. • Acquired possible IEDs (some are operational), as indicated by reports. • Has an extensive network of informants who warn of operations conducted against cell members. • Is involved in weapons trafficking, assassinations, IEDs, and kidnappings.	PID Source Location Trigger Evidence	No photo available
BCT ***(Cavalry)*** ***TVA #***	***Shayikh Walid—*** • Is anti-Iraqi force cell leader under Shayikh Mansur. • Is responsible for the protection of all personnel at the mosque. • Is in charge of cells responsible for various insurgent activities in the area. • Meets with Shayikh Merwan daily.	PID Source Location Trigger Evidence	No photo available
BCT ***TVA #***	***Shayikh Mustafa—*** • Is high-level anti-Iraqi force cell leader in the area. • Is quite involved with the detention and execution of dozens of Sunnis in surrounding areas. • Manages the mosque in the area. • Is associated with Hassaan, Haashim, Rami, and Malik.	PID Source Location Trigger Evidence	No photo available

BCT—brigade combat team
HUMINT—human intelligence
IED—improvised explosive device
PID—positive identification
TVA—target value analysis

UNCLASSIFIED
For Official Use Only

Figure D-16. Sample high-value target list

BE ON THE LOOK-OUT LIST

D-36. BOLO list contents (see figure D-17) may include—

- Date.
- Description of vehicle.
- Level of threat.

Date	*Vehicle*	*Threat*
5 July 2008	Acura Legend 1991 model, dark blue, Baghdad plate number 127557.	Anti-Iraqi force planned to detonate a VBIED at 0730 hours in a neighborhood targeting coalition forces.
3 July 2008	Dodge Ram 2004 model, black, Baghdad plate number 39341.	VBIED may be located in a city neighborhood—to be used against a target within the city.
3 July 2008	Toyota Matrix 2004 model, red, Baghdad plate number 39341.	An unspecified number of VBIEDs entered the city planning to attack police Army checkpoints.
2 July 2008	Vehicle description and license plate number, if possible.	The vehicle may be a VBIED.
2 July 2008	Vehicle description and license plate number, if possible.	Anti-Iraqi forces execute attacks against unspecified objectives in the AOI. The mentioned cell should be in possession of rockets.
2 July 2008		Extremist group elements supposedly planned hostile actions in the city in the direction of objectives not yet defined. The extremist cell should be in possession of three vehicles allegedly built as VBIEB.

AOI—area of interest
VBIED—vehicle-borne improvised explosive device

Figure D-17. Be on the look-out list example

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLAN

D-37. ISR plan contents may include—

- ISR overlay.
- PIRs—with changes highlighted.
- ISR synchronization matrix.

This page intentionally left blank.

Appendix E

Intelligence Support to Targeting

A *target* is an entity or object considered for possible engagement or action (JP 3-60). It may be an area, complex, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action to support the commander's objectives, guidance, and intent. Targets are categorized as planned and immediate.

TARGETING PROCESS

E-1. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting is based on the enemy's assets, which provide an advantage, friendly scheme of maneuver, and tactical plans. Therefore, its purpose is to disrupt, delay, or limit threat interference with friendly courses of action (COAs). Targeting options can be lethal or nonlethal. It requires coordinated interaction between the fires cell's operations, intelligence, information engagement, information operations (IO), and plans cells. Based on the commander's guidance and targeting objectives, the staff determines what targets to attack and how and where to attack them. Targets should be assigned to the best systems to achieve the desired effects, which can also be thought of as conditions that support achieving an associated objective.

E-2. **Direct effects** are immediate, **first-order** consequences of a military action, unaltered by intervening events or mechanisms. **Indirect effects** are the delayed and/or displaced **second-**, **third-**, and higher-order consequences of action, created through intermediate events or mechanisms. (See JP 3-60.)

E-3. In stability operations, target development and targeting are difficult because of the greater emphasis on the effects of combat operations on the local government, Army, police, and the civilian population—second- and third-order effects are considered.

E-4. For more information on targeting, see FM 6-20-10 and JP 3-60.

Second- and Third-Order Effects Example

In Iraq, separating anti-Iraqi forces from the Iraqi population avoids the possibility of further combat. For example, Friendly forces conduct a successful cordon and search by finding a room full of IEDs. They do not address and mitigate the civilians' concerns over the damage caused by the cordon and search (second-order effect). Consequently, the friendly forces will deal with civilian demonstrations or uprisings that will deplete combat power needed for other operations. If the population's security and facility needs are not addressed, the anti-Iraqi forces personnel and weapons will resume threat activities (third-order effects).

INTELLIGENCE SUPPORT TO TARGETING

E-5. Providing intelligence support to targeting is one of the four primary intelligence tasks on the Army Universal Task List (AUTL), which provides the commander information and intelligence support to targeting through lethal and nonlethal actions. It includes intelligence support to the planning (target development) and execution of direct and indirect fires, command and control (C2) engagement, and information engagement as well as assessing the effects of those operations. The intelligence officer also ensures the intelligence, surveillance, and reconnaissance (ISR) plan supports the finalized targeting plan. Table E-1 lists the functions of intelligence support to targeting.

Table E-1. Functions of intelligence support to targeting

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

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

METHODOLOGY

E-6. Decisions create the guidelines for the acquisition and engagement of targets. Target acquisition (TA) and attack are made through a decision cycle. (See figure E-1.) **Decide**, **detect**, **deliver**, and **assess** (D3A) together represent the decision cycle or methodology used to translate the commander's intent into a plan. Table E-2 (page E-4) shows the targeting methodology. Table E-3 (page E-4) lists factors to consider during targeting.

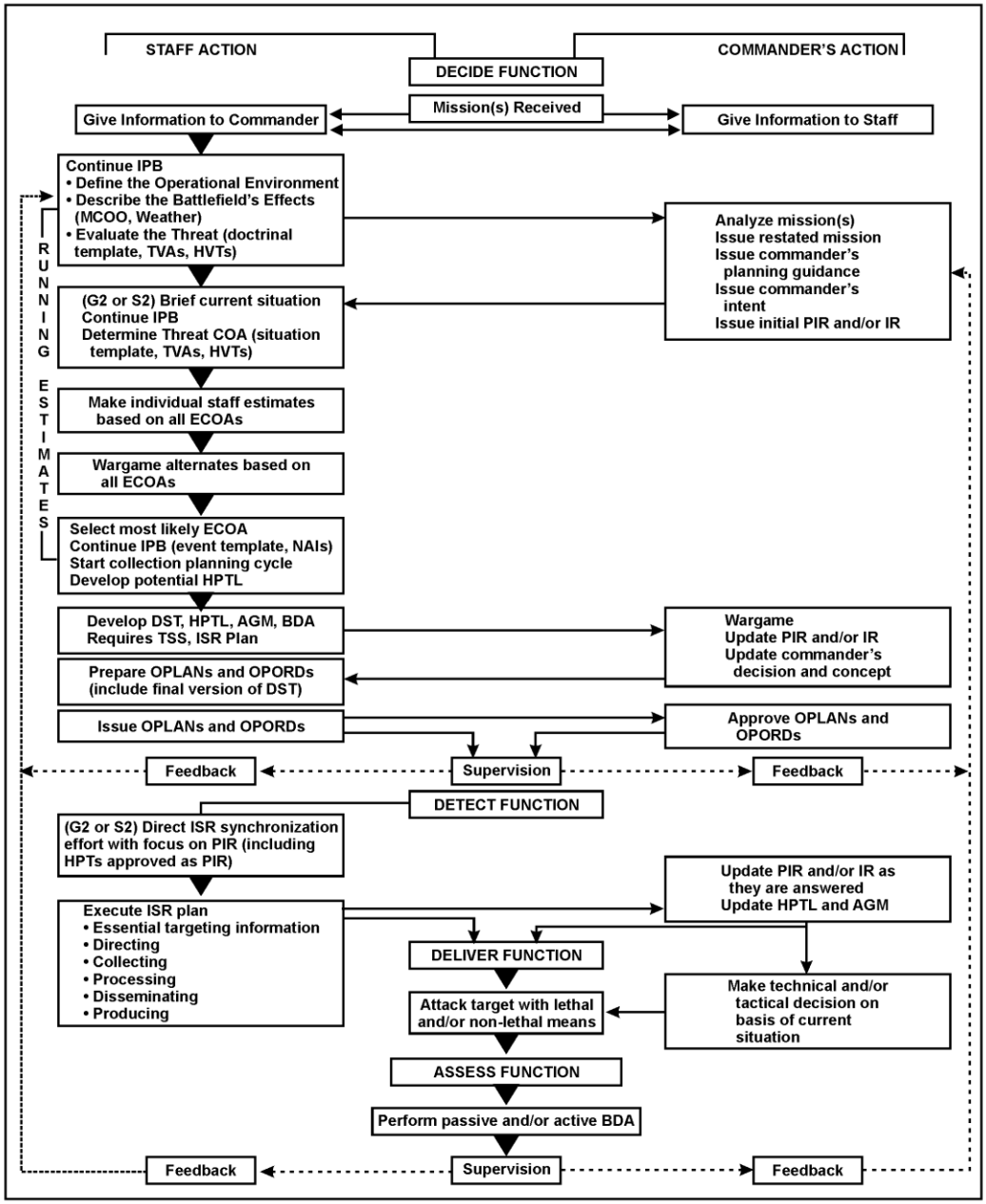


Figure E-1. D3A targeting process

Table E-2. Targeting methodology

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

Table E-3. Targeting considerations

Decide: *Conduct during the planning phase of the operation. Who or what to attack? Is the target worth engaging with available assets?*
Are the commander's planning guidance and intent detailed enough to enable the targeting team to determine— • HVTs to nominate as HPTs? • Desired effects on each HPT? • When to attack each HPT? • Any restrictions or constraints? • Which HPTs require BDA?
What targeting assets (organic, attached, or supporting) are available to detect and attack HPTs?
What detect, deliver, and assess support is needed from higher headquarters?
When are requests to higher headquarters submitted to obtain the support when required?
Have target-tracking responsibilities been established?
Are systems in place to handoff the detected targets to assets that are capable of tracking them?
What detect, deliver, and assess support is required from subordinate units, and when is it required?
What detect, deliver, and assess support requests were received from subordinate units, and what was done with them?
Has the AGM been synchronized with the decision support matrix and the maneuver and fire support plans?
Are all commands using a common datum for locations? If not, are there procedures to correct differences in data?
Detect: *Conduct mainly during the preparation and execution phases of the operation. How to acquire the*
Do ISR synchronization tools focus on the appropriate PIRs?
What accuracy, timeliness, and validity standards, such as, TSSs, are in effect for detection and delivery systems?
Are all target acquisition systems fully employed?
Have backup target acquisition systems been identified for HPTs?
Have responsibilities been assigned to the appropriate unit or agency for detecting each HPT?
Are HPTs being tracked?
Have verification procedures using backup systems been established where necessary?
Are target acquisition and BDA requirements distributed properly among systems that can accomplish both?

Table E-3. Targeting considerations (continued)

Deliver: *Execute the mission to achieve the desired results. Execute attacks on selected targets IAW the FRAGO and the target synchronization matrix. This includes lethal and nonlethal operations.*
Have communications links been established between detection systems, the decisionmaker, and delivery systems?
Have responsibilities been assigned to the appropriate unit or agency for attacking each HPT?
Has a backup attack system been identified for each critical HPT? (The primary system may not be available when the HPT is verified.)
Have fire support coordination measures or AGM and clearance procedures been established to facilitate target engagement?
Have on-order fire support coordination measures or AGMs been established to facilitate future and transition operations?
Have potential fratricide situations been identified? Have procedures been established to positively control each situation?
Have responsibilities been assigned to the appropriate unit or agency for tracking specific HPTs and providing BDA on specified HPTs?
What are the procedures to update the HPTL and synchronize the AGM and decision support template if it becomes necessary to change the maneuver scheme and fire support as the situation changes?
Assess: *Occurs mostly during the execution phase of the operations, but also occurs in all phases. How to verify targeting effectiveness. Were desired effects achieved?*
Are the ISR assets linked to specific HPTs still available?
Have the ISR asset managers been notified of the attack to a target requiring assessment?
Have assessment asset managers been updated on the actual target's location?
Has all the coordination for the assessment mission, particularly airborne assets, been accomplished?
What is the status of BDA collection?
Has the information from the mission been delivered to the appropriate agency for evaluation?
AGM—attack guidance matrix BDA—battle damage assessment FRAGO—fragmentary order HPT—high-payoff target HPTL—high-payoff target list HVT—high-value target IAW—in accordance with ISR—intelligence, surveillance, and reconnaissance PIR—priority intelligence requirement TSS—target selection standard

DECIDE

E-7. **Decide** provides the overall focus and sets priorities for ISR and attack planning (figure E-1 [page E-3]). Targeting priorities are addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

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

Intelligence Support to Target Development

E-8. *Target development* is the systematic evaluation of potential target systems and their components. It is used to determine which elements of military action should, or could, be sued against the targets to achieve the stated objectives. (See FM 6-20-10.)

- A *high-value target* (HVT) is a target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest (AOI) (JP 3-09). (See figure E-2.)
- A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets that must be acquired and successfully attacked for the success of the friendly commander's mission (JP 3-60). High-payoff targets are developed from high-value targets when the various courses of action are wargamed.

Warfighting function	***Examples of HVTs for offense, defense, and stability operations***
Movement and maneuver	Maneuver. Terrorist cells, criminals, VBIED.
Intelligence	RSTA/ISR. Reconnaissance teams, surveillance personnel, informant.
Fires	Fires cell. Mortar systems (82, 60 mm), rockets.
Sustainment	Engineer. IEDs (preparation team, emplacer, executor, bomb maker).
	Bulk fuels (Class III POL). Gas station.
	Maintenance and repair units (Class IX maintenance). Garage.
	Ammunition storage sites and distribution points (Class V ammunition). Weapons black marketing, caches, smugglers.
	Lift. Enemy transport systems.
Protection	CBRN. Chemical IEDs.
	Air and missile defense. SA-7s, SA-16s.
C2	Command, control, communications Cell C2 node, financiers, planners, ideologues.
	Radio electronic combat. Radio communications, cell phones.
	Lines of communications. Couriers, meetings, dead drops.

C2—command and control
CBRN—chemical, biological, radiological, nuclear
HVT—high-value target
IED—improvised explosive device
ISR—intelligence, surveillance, and reconnaissance
mm—millimeter
POL—petroleum, oil, lubricants
RSTA—reconnaissance, surveillance, target acquisition
VBIED—vehicle-borne improvised explosive device

Figure E-2. Examples of high-value targets

Intelligence Preparation of the Battlefield and Mission Analysis

E-9. Intelligence preparation of the battlefield (IPB) is a continuous process and starts in the preparation phase. It provides updated and new products and supports the targeting process. The intelligence running estimate provides key support to target development. Modified combined obstacle overlay (MCOO), threat, situation, event, and decision support templates (DSTs) help identify threat COAs, named areas of interest (NAIs), target areas of interest (TAIs), and HVTs.

Target Value Analysis and Wargaming

E-10. Target value analysis (TVA) yields HVTs for a specific threat COA. Target spreadsheets identify the HVTs in relation to a type of operation, and target sheets offer detailed targeting information for each HVT. (See FM 6-20-10, appendix A.) This information is used during the IPB and the wargaming processes. Both tools are developed by the G-2/S-2 analysis section.

E-11. TVA, a detailed analysis of the threat in selected COAs, focuses on the following threat characteristics:

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

E-12. For more information about threat characteristics, see TC 2-33.4.

E-13. TVA methodology supports a relative ranking of target sets or categories. The methodology begins when target analysts in the G-2/S-2 assume the position of enemy commander. The target analyst, in coordination with other staff members, wargames the operation.

E-14. During the war game, alternate friendly COAs are analyzed based on their affect to enemy operations and likely responses. Attacked enemy battlefield functions that force the enemy response are identified. The commander and staff analyze the criticality of friendly battlefield functions on a specific COA. TAIs are considered the best locations to attack HPTs. Commanders and staff use decision points or time phase lines to ensure the decision to engage or not to engage occurs at the right time. The war game prioritizes identified HVTs that are critical for the enemy mission to succeed. It also identifies HVT subsets, which are HPTs acquired and attacked for the friendly mission to succeed. Selected HPTs are recorded on the DST, at which time the commander and staff analyze the second- and third-order effects.

E-15. ISR managers evaluate HVTs to determine asset detection capability. HPTs receive priority in the allocation of assets. The fires cell determines friendly weapons systems capable of attacking HVTs with lethal fires, and the electronic warfare officer (EWO) nominates and coordinates to provide nonlethal fires.

E-16. Using the capabilities of the system to attack the targets, the G-2/S-2 analyzes and synthesizes the threat's response to each attack. Targets should be assigned priorities based on description, signature, degradation, and graphic representation. If targets have the same relative importance, a targeting team prioritizes the targets by seeking advice from the fires cell's targeting analyst and the field artillery intelligence officer (FAIO).

High-Payoff Target List

E-17. Once prioritized, targets are placed on an HPTL. (See table E-4.) After the HPTL is approved, the G-2/S-2 uses the list to develop the ISR synchronization tools.

Table E-4. High-payoff target list example

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

Target Selection Standards

E-18. TSS are criteria, determined by the commander, applied to enemy activity (acquisitions and battlefield information) and used to decide whether the activity is a target. There are two TSS categories—targets that meet accuracy and timeliness requirements for attack, and suspected targets that require confirmation before any attack. TSS are comprised of the following essential elements:

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

E-19. Different TSS may exist for a given enemy activity based on different attack systems. For example, an enemy artillery battery may have a 150-meter TLE requirement for attack by cannon artillery and a 1-kilometer requirement for attack helicopters. TSS are developed by the fires cells in conjunction with the intelligence cell. Intelligence analysts use TSS to quickly determine targets from battlefield information and pass the targets to the fires cell.

E-20. Attack system managers, such as fires cell, fire control elements, or fire direction centers, use TSS to identify targets for attack. Commands can develop TSS based on anticipated threat characteristics and doctrine equivalent to the available attack systems.

E-21. The G-2/S-2 knows the accuracy of acquisition systems, associated TLE, and the expected enemy target dwell times. The G-2/S-2 can specify whether information reported to the attack system manager is a target or a suspected target. Certain situations require the system to identify friendly and neutral from enemy before approval to fire. HPTs that comply with the criteria are tracked until they are attacked in accordance with the AGM. Target locations that do not comply with TSS are confirmed before attacked. The TSS can be depicted in a TSS matrix. (See figures E-3 and E-4.)

E-22. The matrix lists each system that forwards targets directly to the fires cell or fire direction center. The effects of terrain and weather on the ISR assets and on enemy equipment are considered. TSS are keyed to the situation. However, the greatest emphasis is on the enemy situation considering deception and the reliability of the source or agency that is reporting.

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

Figure E-3. Example of target selection standards matrix

Execution criteria	Status	Definitions
Positive identification	***Green***	A picture identified by a source as the targeted individual or a source willing to identify the target on the objective.
	Amber	A picture that has not been identified by a source, a source willing to identify after the target has been removed from the object (in person or from a detainee photo), or a detailed description of the target.
	Red	No knowledge of target's description or a general description only.
Corroborate sources (source)	***Green***	Reporting from at least two different sources with at least three reports on the targeted individual.
	Amber	Single source with multiple reports or two sources with only two reports.
	Red	Single source, single report.
Location	***Green***	A 10-digit grid or muhalla (neighborhood), street, or house address with knowledge of when the target will be at the location; generally triggers action.
	Amber	A 10-digit grid or muhalla (neighborhood), street, house address with no knowledge of target movement patterns.
	Red	No known location for target.
Intelligence cost	***Green***	Capturing or killing the target minimally affects the ability to collect on the network.
	Amber	Capturing or killing the target degrades the ability to collect on the network.
	Red	Capturing or killing the target negates the ability to collect on the network.
Evidence (used for detention and legal conviction)	***Green***	At least two sworn statements from two different individuals or physical evidence.
	Amber	One sworn statement.
	Red	No sworn statements or evidence.

Figure E-4. Example of target selection standards matrix used in OIF

Attack Guidance Matrix

E-23. Knowledge of target vulnerabilities and the effect an attack will have on enemy operations allows a staff to propose the most efficient available attack option. Key guidance is whether the commander wishes to disrupt, delay, limit damage, or destroy the enemy. During wargaming, decision points linked to events, areas (NAIs and TAIs), or points on the battlefield are developed. These decision points cue command decisions and staff actions where tactical decisions are needed.

E-24. Based on the commander's guidance, the targeting team recommends target engagement in terms of the effects of fire and attack options. Effects of fire can be—**harass, suppress, neutralize,** or **destroy** the target. Subjectively, the commander ensures the targeting team understands the commander's use of these terms. Applying fires support automation system default values further complicates this understanding.

Harassing Fire

E-25. Harassing fire is designed to disturb enemy troops, to curtail movement, and—by threat of losses—lower morale. The decision to employ harassing fires requires careful consideration, since harassing fires have little real effect on the enemy, subject gun crews to an additional workload, and increase the threat of counterfire. Rules of engagement (ROE) or the potential for adverse public opinion may prohibit its use. However, harassing fires may be a combat multiplier in some situations. Consider using harassing fires in stability operations, delaying actions, and economy of force operations.

Suppressive Fire

E-26. Suppressive fire, on or about a weapon system degrades, the system's performance below the level required to fulfill its mission objectives. Suppression lasts as long as the fires continue—the duration is specified in the call for fire or established by standing operating procedures (SOPs). Suppression use prevents effective fire on friendly forces. Usually, suppression is used to support a specified movement of forces. The fire support coordinator (FSCOORD) asks or calculates the *when* and *how long* questions.

Neutralization Fire

E-27. Neutralization fire renders a target temporarily ineffective or unusable. It leaves enemy personnel or materiel incapable of interfering with an operation or COA. The FSCOORD asks *when* and for *how long* the commander wants a target to be neutralized. Most planned missions are neutralization fires.

Destruction Fire

E-28. Destruction fire's sole purpose is the destruction of materiel objects. It physically renders a target permanently combat-ineffective unless the target is restored, reconstituted, or rebuilt. Setting automated fire support default values, for 30-percent destruction, does not guarantee achievement of the commander's intent. The remaining 70 percent may still influence the operation. Destruction missions are expensive time and materiel wise, therefore, consider whether neutralization or suppression is more efficient.

Deciding on Attack Systems

E-29. Deciding on which attack system to use occurs simultaneously as deciding when to acquire and attack the target. When deciding to attack by two different means, such as electronic warfare (EW) and combat air operations, coordination is required. Coordination requirements are recorded during the wargaming process. In stability operations, the attack system may be using IO and civil affairs operations to engage and cause a division between the local populace and the insurgents.

E-30. Commanders approve AGMs, which detail—

- Prioritized HPTLs.
- *When*, *how*, and the *desired effects* of attack.
- Special instructions.
- HPTs requiring a battle damage assessment (BDA).

E-31. This information is developed during the war game. Attack guidance—

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

E-32. The AGM is updated during staff planning meetings and when the enemy situation changes. (See figure E-5.) Consider separate AGMs for each phase of an operation.

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

Figure E-5. Example attack guidance matrix

E-33. **High-payoff target list** shows the prioritized HPTs identified during wargaming. They have priority for engagement.

E-34. **When.** Timing the target attacks is critical to maximizing effects. During wargaming, the optimum time is identified and reflected in the *when* column:

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

E-35. **How** does the attack system link to the HPT? Identify a primary and backup attack system for HPT attacks.

E-36. **Effect** refers to the target attack criteria. The targeting team specifies attack criteria as per the commander's guidance. Target attack criteria should be quantifiable, for example, percentage of casualties or destroyed elements, time, ordnance, and allocation or application of assets. Effect can be viewed as the number of battery or battalion volleys.

E-37. **Remarks.** Note which targets should not be attacked in certain tactical situations, for example, if the enemy is withdrawing. Examples of how to use this column:

- Accuracy or time constraints.
- Coordination requirements.
- Amount or type of ammunition limitations.
- Requirement for BDA.

DETECT

E-38. The G-2/S-2 directs the effort to **detect** identified HPTs. To identify *who*, *what*, *when*, and *how* for TA, the G-2/S-2 coordinates with the—

- Intelligence all-source analysis section.
- FAIO.
- Targeting officer and fires cell analyst.
- IO officer.
- Higher, lower, and adjacent G-2s/S-2s.
- Special operations forces (as applicable).
- National agency support teams (as applicable).

E-39. This process determines accurate, identifiable, and timely requirements for ISR systems. The analysis section ensures ISR system managers understand these requirements.

E-40. Target detection and action requirements are expressed as PIRs and information requirements. Their priority depends on the importance of the target to the friendly COA and tracking requirements. PIRs and information requirements that support HPT detection are incorporated into the overall unit ISR plan.

E-41. The maximum use of all available ISR assets detects targets. The G-2/S-2 focuses the intelligence acquisition efforts on designated HPTs and PIRs. Situation development information, through detection and tracking, accumulates as ISR assets satisfy PIRs and information requirements. The ISR requirements manager—

- Considers ISR assets' capabilities and availability within the echelon, and those assets available to subordinate, higher, and adjacent units.
- Considers joint or combined force assets.
- Translates the PIRs and information requirements into specific information requirements (SIRs) and recommended ISR tasks and request for information (RFIs).
- Arranges direct dissemination of targeting information, from the ISR asset to the targeting cell or targeting intelligence, to the fires cell if possible.

Detection in Counterinsurgency Operations

E-42. Targeting in counterinsurgency operations requires a detailed understanding of social networks, insurgent networks, actions, and civil considerations. A target can be any aspect of the populace; a person, place, or thing considered vital to defeat or deny threat activities. The target can be successful civic initiatives or new businesses in the IO strategy. Therefore, in a counterinsurgency environment, the **detect** phase often precedes the **decide** phase because it is difficult to decide *who* to target without knowing *who* or *what* are the targets.

Detection Procedures

E-43. The following procedures assist in the target detection process:

- Use all TA assets effectively and efficiently.
- Avoid effort duplication among available ISR assets unless confirmation of target information is required. The intelligence officer ensures there are no gaps in planned coverage, which allows timely collection of combat information to answer the commander's intelligence and TA requirements.
- To detect HPTs, give clear and concise taskings to those TA systems capable of detecting a given target. This information allows analysts to develop the enemy situation and identify targets. (See table E-5.)

E-44. Fires cell personnel provide the G-2/S-2 with the degree of located accuracy:

- Accuracy requirements are matched to the TLE of the ISR asset, which allows the G-2/S-2 to develop more detailed TSS.
- Identified NAIs and TAIs are matched with the most capable detection system available. If the target type and its associated signatures—for example, electronic, visual, thermal—are known, the most capable ISR asset can be directed against the target. The asset can be positioned based on *when* and *where* estimations of the enemy target's location.

E-45. Information needed to detect targets is expressed in PIRs and information requirements, which are incorporated into the ISR synchronization tools. The ISR synchronization manager—

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

E-46. When a target is detected, the information is quickly delivered to FAIOs if they are located in the analysis and control element (ACE) and have communications with the fires cell. The FAIOs—

- Determine if the target is an HPT, its priority, and if it complies with the TSS.
- If the target is an HPT, coordinate with their respective G-2s/S-2s and deliver the target directly to the fires cell.
- If the commander approves the target, transfer it to a firing unit.

Note. Mobile HPTs are detected and tracked to maintain a current target location. Target tracking is inherent to detection.

Table E-5. Warfighting function detection capabilities

Warfighting function	***Target acquisition means***
Movement and maneuver	Engineer units, patrols, scouts, units in contact, air or ground cavalry or air units.
Intelligence	SIGINT, IMINT, TECHINT, MASINT systems; HUMINT and CI personnel.
Fires	TA battery, AN/TPQ-36/37 radars, forward observers, combat observation laser teams.
Sustainment	Truck drivers, base cluster reconnaissance and counterreconnaissance patrols.
C2	MIJI reports.
Protection	Air and missile defense scouts, air and missile defense system's acquisition radars, and CBRN reconnaissance.
Other Services	
USAF	JSTARS and the Airborne Warning and Control System.
U.S. Navy	EP-3.

C2—command and control
CBRN—chemical, biological, radiological, nuclear
CI—counterintelligence
HUMINT—human intelligence
IMINT—imagery intelligence
JSTARTS—Joint Surveillance Target Attack Radar System
MASINT—measurement and signature intelligence
MIJI—meaconing , interference, jamming, and intrusion
SIGINT—signals intelligence
TA—target acquisition
TECHINT—technical intelligence
USAF—United States Air Force

E-47. As the assets collect information for target development, the information is forwarded to the all-source intelligence analysts. The all-source intelligence analyst—

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

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

E-48. The FAIOs coordinate with the G-2/S-2 and fires cell to deliver HPTs and other targets directly to the fire control element at the fires brigade, or, if approved, through the maneuver commander directly to a firing unit. The results are efficient targets designated in advance for attack.

E-49. When the FAIOs obtain intelligence information that warrants attack, the fires cell is notified. This allows the FAIO to focus on intelligence analysis and the fires cell to manage the control of fires. The targeting officer, at the maneuver brigade, and the S-2, at the battalion, perform FAIO functions.

E-50. Tracking priorities are based on the commander's concept of the operation and targeting priorities. Tracking is executed through the ISR plan. Although every target is not tracked, critical targets move frequently, therefore, require tracking.

DELIVER

E-51. **Deliver** executes the target attack guidance and supports the commander's plan once the HPTs have been located and identified. (See table E-6 [page E-14].)

Table E-6. Deliver functions and responsibilities

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

Table E-6. Deliver functions and responsibilities (continued)

Desired effects: ***Disrupt*** ***Delay*** ***Limit***	• **Planned targets:** ▪ Verify threat activity as that planned to be attacked. ▪ Reaffirm decision to attack. ▪ Issue the fire mission request (through the fires cell) to appropriate executing units. • **Targets of opportunity:** ▪ Targeting team decides payoff and availability of attack systems and munitions.
Attack system	• **Planned targets:** ▪ Decision made during the **decide** function. ▪ Determine system availability and capability. ▪ Targeting team determines the best system available to attack target if system unavailable or capable.
Attack system	• **Targets of Opportunity:** ▪ Targeting team determines attack system, subject to maneuver commander's approval. ▪ Consider all available attack systems. ▪ Attacking targets should optimize capabilities of— o Light and heavy ground forces. o Attack helicopters. o Field artillery. o Mortars. o Naval gunfire. o Combat air operations (CAS and air interdiction). o Offensive EW. ▪ Consider availability and capabilities of each resource using— o Desired effects on the target. o Payoff of the target. o Degree of risk to use asset against target. o Impact on friendly operations. o Impact on populace (second and third order effects). ▪ Target attack should be coordinated among two or more attack systems. ▪ Engaging a target by lethal means, along with jamming or monitoring, may be more beneficial than simply firing at the target.

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

COMBAT ASSESSMENT

E-52. *Combat assessment* is the determination of the effectiveness of force employment during military operations (JP 3-60). It is composed of three elements:

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

E-53. Together, BDA and MEA inform the commander of effects against targets and target sets. The threat's ability to make and sustain war is estimated continually. During the effects review of the targets, restrike recommendations are proposed or executed. BDA pertains to the results of attacks on targets designated by the commander. Producing BDA is primarily an intelligence responsibility, but requires coordination with operational elements. BDA requirements are translated into PIRs. BDA—

- Is used, at the tactical level, by commanders to obtain a series of timely and accurate snapshots of their effect on the enemy. BDA provides commanders an estimate of the enemy's combat

effectiveness, capabilities, and intentions. From this information, commanders determine when or whether their targeting effort accomplishes their objectives.

- Helps determine if restrike is necessary. Commanders use BDA to allocate or redirect attack systems to make use of available combat power.

Munitions Effects Assessment

E-54. The G-3/S-3, through the targeting team, conducts MEA concurrently and interactively with BDA as a function of combat assessment. From the MEA, changes are recommended to increase effectiveness in—

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

E-55. Munitions effect on targets is calculated by obtaining rounds fired on specific targets divided by artillery assets. The targeting team may generate modified commander's guidance concerning—

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

Battle Damage Assessment

E-56. BDA for specific HPTs is determined during the **decide** function. BDA is recorded on the AGM and the ISR synchronization matrix. The resources used for BDA are the same resources used for target development and TA. An asset used for BDA may be unavailable for target development and TA. The ACE receives, processes, and disseminates, to the targeting team, attack results, analyzed in terms of desired effects.

E-57. The targeting team should consider the following BDA principles:

- BDA should measure what is important to commanders, not make important what is easily measurable.
- BDA should be objective. When a G-2/S-2 receives a BDA product from another echelon, the conclusions should be verified (time permitting). G-2s/S-2s at all echelons strive to identify and resolve discrepancies among the BDA analysts at different headquarters.
- The assessment's degree of reliability and credibility relies largely on ISR resources. The quantity and quality of ISR assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (an estimation). Effective BDAs use more than one intelligence discipline to verify each conclusion.

E-58. Each BDA has three assessment components. (See table E-7.) Each requires different sensors, analytical elements, and timeliness—not necessarily subcomponents of each BDA report. (See FM 6-20-10.)

E-59. BDA is more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information, such as—

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

E-60. BDA may simply be compiled information about a particular target or area, for example, the area's cessation of fires. If BDA is developed, the targeting team gives intelligence acquisition systems adequate warning to direct sensors at the target at the right time. BDA outcomes may result in changed plans and

earlier decisions. The targeting team periodically updates earlier decisions during the **decide** function concerning—

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

Table E-7. Battle damage assessment functions

Components	*Description*
Physical damage assessment	• Quantitative physical damage from munitions blast, fragmentation, or fire. • Based on observed or interpreted damage.
Functional damage assessment	• Estimates the effects on the target's capability to perform its mission. • Assessment based on all-source intelligence. • Includes a time estimate required to reconstitute or replace the target. • Temporary assessment—compared to a target system assessment—used for specific missions.
Target system assessment	• The overall affect of the full spectrum of operations on an entire target system's capability. • Applicable against an adversary's combat effectiveness. • May address significant subdivisions of a target. • A more permanent assessment.

E-61. From the BDA and MEA, the G-2/S-2 or G-3/S-3 considers the achievement of operational objectives and makes recommendations to the commander. Reattack and other recommendations address operational objectives relative to the—

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

E-62. BDA key players include the commander, operations officer, FSCOORD, Army aviation officer, air liaison officer (LNO), and G-2/S-2. The G-2/S-2 integrates intelligence and operational data. In coordination with the G-3/S-3, the G-2/S-2—

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

TARGETING IN STABILITY OPERATIONS

E-63. Although the principles of the targeting process apply, in stability operations consider the following:

- ROE are restrictive compared to conventional combat situations.
- Targeting personnel understand the targeting process and the ROE.
- Targeting personnel have a detailed understanding of social networks, insurgent networks, actions, and community atmospherics.
- A target is any aspect of the populace—a person, place, or thing deemed necessary or vital to defeat or deny threat activities—including successful civic initiatives, or new businesses in the IO strategy.
- The **detect** function often precedes the **decide** function because it is difficult to decide *who* to target without knowing *who* or *what* are the targets.
- HVT, threat intention, threat location, and weapons systems identification are slowly developed; therefore, targeting personnel may be unable to act on them when fully developed.
- The nature of a threat—such as a relatively small, unconventional enemy that constitutes a significant threat to U.S. forces—makes it difficult to ascertain an HVT—specifically, what constitutes an HVT—which makes it difficult to develop precise time, location, and march rates for a threat force.
- Targets that blend into the population, are often less visible than conventional targets.
- When targets are identified, reaction and decision times decrease.
- Host-nation population considerations require targeting precision and the correct weapons system selection.
- Interaction and coordination with nontraditional elements and agencies—such as the private sector, indigenous populations and institutions, intergovernmental organizations, nongovernmental organizations, interagency partners, multinational forces, and host-nation forces—may be required.
- An attack system can be using IO and civil affairs operations to engage and form a wedge between the local populace and the insurgents.

PERSONALITY TARGETING—FIND, FIX, FINISH, EXPLOIT, ANALYZE, AND DISSEMINATE

E-64. **Find**, **fix**, **finish**, **exploit**, **analyze**, and **disseminate** (F3EAD) is a subset of the D3A targeting process used to engage selected high-value individuals (HVIs)—sometimes referred to as personality targets. (See figure E-6.) F3EAD, an aggressive targeting model, features massed, persistent ISR cued to a powerful and decentralized all-source intelligence apparatus.

E-65. The goal of F3EAD is to find and fix an HVI's precise location amid civilian clutter. This precise location enables surgical finish operations (lethal or nonlethal) that emphasize the speedy capture of a fleeting target—which removes the target from the battlefield, and affords an opportunity to gain information on and from the target. The **exploit** and **analyze** steps are often the "main effort" of F3EAD because they provide insight into the threat's network and may offer new lines of operations. The information collected during the **exploit** and **analyze** steps restarts the cycle by providing leads to an observable and traceable network.

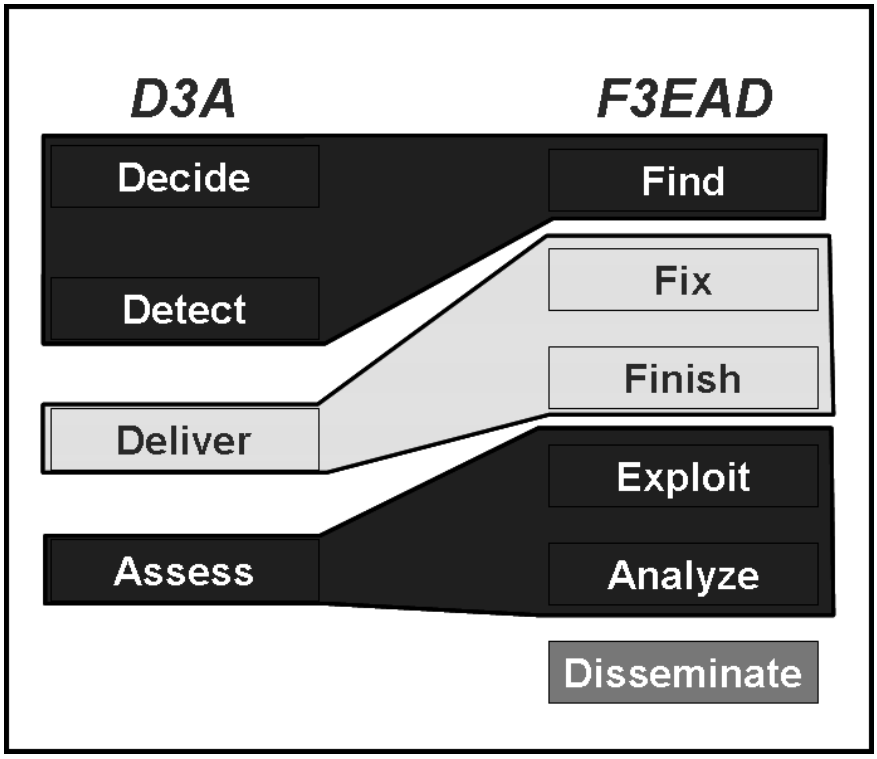


Figure E-6. D3A versus F3EAD

E-66. F3EAD is not a linear process with a start and end block. (See figure E-7.) Although adaptable, it is limited only by human ingenuity. F3EAD usually starts with a **find**.

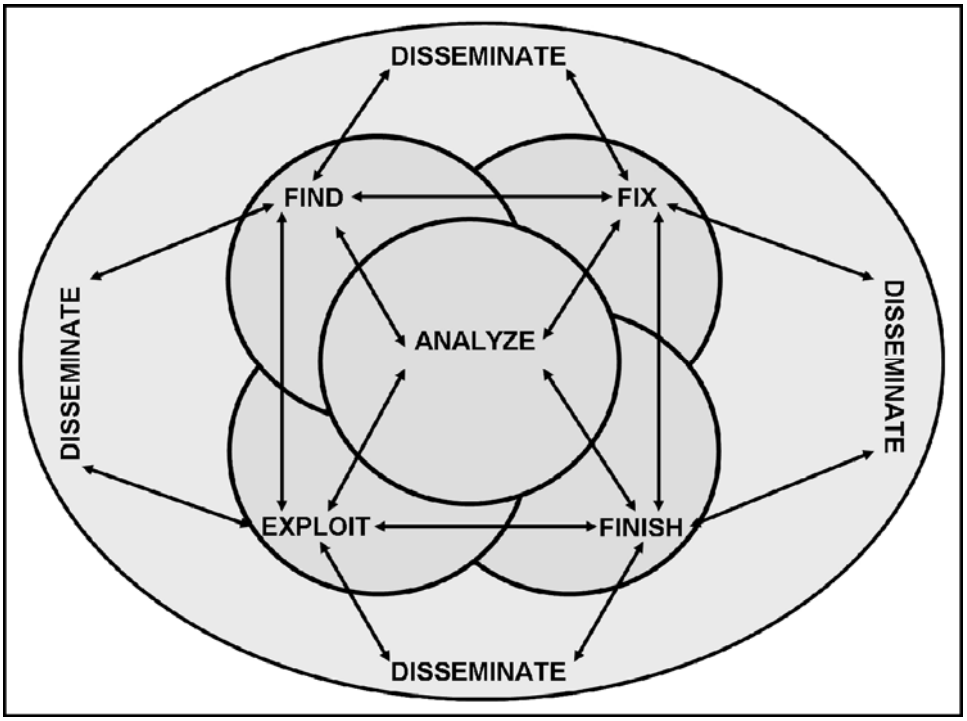


Figure E-7. F3EAD methodology

E-67. The following is a brief description of each of the elements of F3EAD:

- **Find.** Determine area of operations (AO) or AOI for target. Refine through ISR synchronization tools. Information can be derived from but are not limited to—
  - Analytical SIGINT.
  - Analyst driven interrogations.
  - Imagery intelligence (IMINT).
  - Human intelligence (HUMINT).
- **Fix.** Use NAI's and TAI's to *acquire information* to trigger decision points for action, ability to track targets in real time or near real time. Sources include—
  - SIGINT or EW assets to geolocate target.
  - ISR assets that provide an "unblinking eye" on objectives such as unmanned aircraft systems (UASs).
- **Finish.** Deliberate operations to kill, capture, or influence individuals. These operations may be—
  - Unilateral.
  - Bilateral.
  - Multinational.
  - Indigenous.
- **Exploit.** Exploit begins with tactical site assessment and transitions to people and objects exploitation. Thoroughly review all information pertaining to the objective received from HUMINT collection teams (HCTs).
  - Technical exploitation.
  - Document and media exploitation (DOMEX).
- **Analyze.** Analysis is ongoing throughout the F3EAD process. It assists in confirming assumptions, gaining awareness, identifying linkages and intelligence gaps. **Analyze** includes—
  - Assessing postdetention intelligence.
  - Expanding the network picture.
  - Developing future targets.
- **Disseminate.** The findings and results must be disseminated to adjacent, higher, and lower units and key communicators in the local AO.

E-68. Measurements of success with F3EAD include—

- Changes in local attitudes (friendliness towards U.S. and host-nation personnel).
- Changes in public perceptions.
- Changes in the quality or quantity of information provided by individuals or groups.
- Changes in the economic or political situation of an area.
- Changes in insurgent patterns.
- Captured and killed insurgents.
- Captured equipment and documents.

CARVER TECHNIQUE

E-69. Army special operations forces (SOF) use CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability) factors to assess mission, validity, and requirements. CARVER is also used in technical appreciation and target analysis. (See table E-8.)

E-70. The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are assigned a numerical value, which represents the desirability to attack the target. The values are recorded, in numerical order, on a decision matrix. After assigning CARVER values to each target or component, the sum of the values indicates the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

Table E-8. CARVER technique

C—Criticality			
Decision	***Factors***	***Criteria and values****	***Scale***
• Target value means. • Primary consideration in targeting. • Target is critical when its destruction or damage has impacted military, political, or economic operations. • Consider targets within a system relative to other elements of the target system. • Target value changes as situation develops. • Target requires time-sensitive methods that respond to changing situations. • **Example**: When there are few locomotives, railroad bridges may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces requiring use of such bridges. • High-value individuals—where does the target fit into the network (cell leader, financier)?	• Time—how rapidly will the target attack affect operations? • Quality—what percentage of output, production, or service will be curtailed by target damage? • Surrogates—what will be the affect on output, production, and service? • Relativity—how many targets? What are their positions? How is their relative value determined? What will be affected in the system or complex stream?	• Immediate halt; target cannot function without it.	9 to 10
		• Halt within one day, or 66 percent.	7 to 8
		• Halt within one week, or 33 percent.	5 to 6
		• Halt within 10 days, or 10 percent.	3 to 4
		• No significant affect.	1 to 2
		***Note.** ** Refers to time or percentage; curtailment in output, production, or service.	
A—Accessibility			
Decision	***Factors***	***Criteria and values****	***Scale***
• Target is accessible when operations element reaches the target with sufficient personnel and equipment to accomplish mission. • Identifying and studying critical paths by the operational element to achieve objectives and measuring what aids or impedes access. • Reach target AND remain stationary for extended periods. • Basic steps to identify accessibility: ▪ Infiltration from staging base to target. ▪ Movement from entry point to target or objective. ▪ Movement to target's critical element. ▪ Exfiltration. ▪ High-value individuals—what intelligence gives access to the target? ▪ HUMINT—expresses reliability, credibility, and degree of separation. ▪ SIGINT—reporting on the target's pattern of life.	• Active and passive early warning system. • Detection devices. • Air defense capabilities within target area. • Road and rail transportation systems. • Terrain type and its use. • Concealment and cover. • Population density. • Other natural or synthetic obstacles and barriers. • Current and climatic weather conditions. • Analysis, along each critical path to target, measures time for action element to bypass, neutralize, or penetrate barriers or obstacles. • Measured by ease or difficulty of movement of operational element and likelihood of detection. Consider using standoff weapons in such evaluations.	• Easily accessible, standoff weapons can be employed.	9 to 10
		• Inside a perimeter fence but outdoors.	7 to 8
		• Inside a building but on ground floor.	5 to 6
		• Inside a building but on second floor or in a basement; climbing or lowering is required.	3 to 4
		• Not accessible or inaccessible without extreme difficulty.	1 to 2

Table E-8. CARVER technique (continued)

R—Recuperability			
Decision	***Factors***	***Criteria and values***	***Scale***
• Measured in time—how long will it take to replace, repair, or bypass destruction of or damage to the target? • Varies with sources and type of targeted components and availability of spare parts availability. • High-value individuals—what is the ability of the cell or network associated with the target to rebound, reconstitute, or assign a replacement? ▪ What intelligence gives access to the target? ▪ Who is accessed to be the replacement?	• On-hand equipment, such as railroad cranes, dry docks, and cannibalization. • Restoration and substitution through redundancies. • On-hand spares. • Equivalent threat characteristics equipment sets that back up critical equipment or components; effects of economic embargoes and labor unrest.	Replacement, repair, or substitution requires—	
		• 1 month or more.	9 to 10
		• 1 week to 1 month.	7 to 8
		• 72 hours to 1 week.	5 to 6
		• 24 to 72 hours.	3 to 4
		• Same day replacement, repair, or substitution.	1 to 2
V—Vulnerability			
Decision	***Factors***	***Criteria and values***	***Scale***
• Target is vulnerable if operational element has means and expertise to attack the target successfully. • Scale of critical component should be compared to capability of attacking element to destroy or damage it. • Attacking element may— ▪ Choose special components. ▪ Do permanent damage. ▪ Maximize effects through use of on-site materials. ▪ Cause the target to self-destruct. • High-value individuals—what prosecutorial evidence can ensure long-term detention? ▪ If the evidence is lacking, who can be targeted to establish the necessary evidence to make the primary target vulnerable?	***Depends on—*** • Nature and construction of the target. • Amount of damage required. • Assets available, such as personnel, expertise, motivation, weapons, explosives, and equipment.	• Vulnerable to long-range laser target designation, small arms fire, or charges of 5 lbs or less.	9 to 10
		• Vulnerable to light antiarmor weapons fire or charges of 5 to 10 lbs.	7 to 8
		• Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 lbs, or very careful placement of smaller charges.	5 to 6
		• Vulnerable to heavy antiarmor fire, bulk charges of 30 to 50 lbs, or requires special weapons.	3 to 4
		• Not vulnerable to all but the most extreme targeting measures.	1 to 2
		lbs—pounds	

Table E-8. CARVER technique (continued)

E—Effect			
Decision	***Factors***	***Criteria and values***	***Scale***
• Measure of possible military, political, economic, psychological and sociological impacts at target and beyond. • Closely related to the measure of target criticality. • Type and magnitude of given effects desired will help planners select targets and target components. • Addresses all significant effects, whether desired or not, that may result once selected target component is attacked. • Traditionally, this element addressed effect on local population; now there are broader considerations. • Frequently neutral at tactical level. • High-value individuals—what are the anticipated effects associated with an operation against this target? • How are desired second- and third-order effects derived through various options lethal and nonlethal?	• Primary effect—of destruction of two adjacent long-range radar sites in early warning system—may be to open a hole in a system of sufficient size and duration to permit attacker to launch a successful air or missile nuclear strike against defender. • Can include— ▪ Countermeasures triggers. ▪ Supporting the negation of psychological operations themes. ▪ Unemployment. ▪ Reprisals against the civilian populace. ▪ Collateral damage to other targets. • Possible effects can be speculative, therefore, should be labeled. • Effects of same attack may be different at tactical, operational and strategic levels. • **Example**: Destruction of a substation may not affect local power but cuts off power to adjacent region.	• Overwhelmingly positive effects; no significant negative effects.	9 to 10
		• Moderately positive effects; few significant negative effects.	7 to 8
		• No significant effects; neutral.	5 to 6
		• Moderately negative effects; few significant positive effects.	3 to 4
		• Overwhelmingly negative effects; no significant positive effects.	1 to 2

Table E-8. CARVER technique (continued)

R—Recognizability			
Decision	***Factors***	***Criteria and values***	***Scale***
• Target's recognizability is the degree it can be recognized by an operational element or ISR assets under varying conditions. • Weather affects visibility. • Rain, snow, and ground fog may obscure observation. • Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. • Consider distance, light, and season. • High-value individuals—can the target be positively identified? • Is there a photograph of the target or are there any characteristics that will distinguish the target from other detainees?	• Site and complexity of target. • Existence of distinctive target signatures. • Presence of masking or camouflage. • Technical sophistication and training of attackers.	• Target is clearly recognizable under all conditions and from a distance; requires little or no training.	9 to 10
		• Target is easily recognizable at small-arms range and requires small amount of training.	7 to 8
		• Target is difficult to recognize at night or in bad weather, or might be confused with other targets or components; requires some training.	5 to 6
		• Target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components; requires extensive training.	3 to 4
		• Target cannot be recognized under any conditions, except by experts.	1 to 2

E-71. CARVER factors and their assigned values are used to construct a CARVER matrix. Table E-9 is a tool for rating the desirability of potential targets and allocating attack resources.

- List the potential targets in the left column.
- For strategic level analysis, list the enemy's systems or subsystems (electric power supply, rail system).
- For tactical level analysis, list the complexes or components of the subsystems or complexes selected for attack by higher headquarters.
- As each potential target is evaluated for each CARVER factor, enter the appropriate value into the matrix.
- Once all the potential targets are evaluated, add the values for each potential target.
- Each sum represents the relative desirability of each potential target; this constitutes a prioritized list of targets.
- Attack the targets with the highest totals first.
- If additional men or munitions are available as resources, allocate them to the remaining potential targets in descending numerical order.
- This allocation scheme maximizes the use of limited resources.

E-72. The G-2/S-2 can present the CARVER matrix, with a variety of attack options to operation planners, and discuss the strengths and weaknesses of each COA against the target. Because of this the rigorous evaluation process, the G-2/S-2 can comfortably defend conclusions.

Table E-9. Bulk electric power supply

Potential targets	*C*	*A*	*R*	*V*	*E*	*R*	*Total*
Fuel tanks	8	9	3	8	5	6	41
Fuel pumps	8	6	2	10	5	3	34
Boilers	6	2	10	4	5	4	31
Turbines	8	6	10	7	5	9	45
Generators	4	6	10	7	5	9	41
Condenser	8	8	5	2	5	4	34
Feed pumps	3	8	5	8	5	6	33
Water pumps	3	8	5	8	5	4	33
Generator step up transformer	10	10	10	9	5	9	53

E-73. Some OIF units have added three additional CARVER factors—CARVER***SHP***. Analyzing the ***s***ymbolism, ***h***istorical significance, and ***p***olitical significance of an HVI has proven effective while fighting in a counterinsurgency environment.

- **Symbolism.** How the population accepts relations with the counterinsurgents.
  - Will the general population be indifferent to, support, or oppose a relationship with the group?
  - If a relationship is generally accepted by the local population, will there be factions opposing the relationship? If yes, how will they disrupt the relationship?
- **Historical significance.** How long have relations with the counterinsurgents existed?
  - What other external groups, agencies, or ideologies have formed alliances with the counterinsurgents?
  - Did U.S. or other forces have established relationships with this group?
  - Did these relationships occur rarely or regularly?
  - Does this group establish relationships with others when there is a common interest?
  - Will relations with this group set a historical precedence?
- **Political significance.** How important are relations with the group on the international political scene?
  - What is the political advantage or disadvantage?
  - Will relations with the group have any political significance—locally, regionally, nationally, or internationally? If yes, what significance?

TARGETING MEETING

E-74. The targeting meeting allows the staff to—

- Focus and synchronize the unit's efforts based on the current enemy situation, current unit success, and fragmentary orders (FRAGOs) from higher echelons.
- Assess the current lethal and nonlethal effects to determine if a change to the current plan is needed.

E-75. The end state of a targeting meeting is a FRAGO to the subordinate staffs that decides *what* to target, *how* to detect it, *how* to deliver combat power against the target, and *how* to assess operation results. The FRAGO should address both lethal and nonlethal tasks.

PRETARGETING MEETING

E-76. The G-2/S-2 offers inputs during the pretargeting meeting:

- Light, weather forecast, and terrain data.
- BDA and TSM assessments.
- Proposed HVTL and link or pattern analysis (D, D+1/2/3).
- Current and proposed PIRs.
- Enemy COA and event template (D, D+1/2/3).
- Current ISR synchronization tools and proposed changes.

E-77. At the conclusion of the pretargeting meeting, the staff should have developed a TSM with baseline data sufficient to begin developing resources, synchronizing engagements, and other preparatory work necessary to conduct the targeting meeting. At a minimum, the decision column, and desired effect should be completed.

TARGETING MEETING

E-78. The G-2/S-2 offers input during the targeting meeting:

- Light, weather forecast, and terrain data.
- Current enemy situation template, incident overlay, pattern and link analysis.
- Status of ISR synchronization tools—NAIs tasked, gaps in coverage, significant reports, required synchronization.)
- Status of ISR assets available.
- BDA of attacked targets—in the past 12-24 hours—highlighting changes in enemy capabilities.
- Current or proposed PIRs and HVTs.
- Enemy COA for the targeting period.

THE HIGH-VALUE INDIVIDUAL TARGET PACKET

E-79. The target packet is a folder, hardcopy or electronic, that contains intelligence, operational, and related materials for the purpose of planning and executing action against a specific target. The G-2/S-2 produces a most of the target packet as an all-source product with vetted, validated information to support the designated desired effect. Table E-10 shows considerations used in OIF to build the intelligence portion of a target packet on an HVI.

Table E-10. Target packet intelligence considerations

Task
Name of HVI.
Suspected location of HVI.
Collection overview. Map with objective locations (grid coordinate) of target, target's known pattern of activity, intelligence sources (HUMINT detainee, SIGINT report, IMINT such as national imagery or UAS).
Photo of HVI.
Intelligence gaps—positive identification.
Physical description
• **Age.** Unless know accurately, should be bracketed.
• **Build.** Thin, medium, well built.
• **Clothes.** Dish dash or western style trousers and shirt.
• **Distinguishing features.** Scars, tattoos, missing limbs, small head.
• **Height/Weight.** xxx inches/xxx lbs.
• **Eyes.** Blue, green.

Table E-10. Target packet intelligence considerations (continued)

Physical description
• **Face.** Round, slim, gaunt, fat, jowls, double chin, big nose.
• **Gait.** The walk, upright, slouched, any limp.
• **Hair.** Color, length, and style. Does the individual wear a hat?
• **License plate numbers.** For all vehicles used by HVI.
• **Vehicles.** All vehicles used by HVI.
• **Aliases.** All known aliases for primary target.
Background. Key bullets on the individual's background—family, education, past events, or experiences known by the reviewer to determine the individual's character, leadership potential, or past roles.
• **Category.** To which major category does the individual belong (for example, Jihadist)?
• **Affiliation.** To which group is the individual affiliated (for example, 1920 Revolutionary Group)?
• **Connections** with government, military, or police?
• **Role.** List functions the individual provides (for example, leader, facilitator, enabler, financier).
• **AO.** Where does the individual operate (for example, Baghdad, Iraq, trans-national)?
• **Religious affiliation.** Sunni, Shia?
• **Province from.**
• **Civilian education.** Associate's, bachelor's, or master's degree or doctorate.
• **Military education.** MI, War College.
• **Known disabilities.** Uses a cane.
• **Health status.** Heart disease.
• **Travel.** Locations outside of country the HVI travels.
• **Previously detained.** *Where*, *when*, *why*, *by who*?
• **Military or insurgency experience.** IED maker, sniper, VBIED maker or combatant in Afghanistan.
• **Expected actions.** Will surrender. Will fight until captured or killed.
Responsibilities. List key events or actions for which the individual is responsible or involved. Summary of few specific key events that depict what the individual has done to support the insurgency.
HVI associates. List the top five associates (secondary targets) that might be on objective. Associates attitude and capabilities. Insert pictures and description if available.
• **Photo** of HVI associates.
• **Associates description.**
• **Connections** with government, military, or police.
• **Previously detained.** *Where*, *when*, *why*, *by who*?
• **Military or insurgency experience.** IED maker, sniper, VBIED maker, combatant in Afghanistan.
• **Expected actions.** Will surrender. Will fight until captured or killed.
• **Aliases.** List all known aliases for secondary targets.
HVI family. List all family members that might be on objective with HVI. Family attitude and capabilities. Insert pictures and description.
• **Photo** of HVI family.
• **Family background and descriptions.**
• **Family member's locations.** List locations with grid for each family members.
• **Connections** with government, military, or police.
• **Previously detained.** *Where*, *when*, *why*, *by who*?
• **Military or insurgency experience.** IED maker, sniper, VBIED maker, combatant in Afghanistan.
• **Expected actions.** Will surrender. Will fight until captured or killed.
• **Aliases.** List all known aliases for family members.
Intelligence products
• **HUMINT.**
▪ **Assessment of HUMINT source.** Assess the source as it applies to the suspected location of the target (report *type* and *number*). Develop this information for each objective—source description and rating, *who* vetted the source?
Note. Keep information at the NOFORN level.
▪ **Summary of HUMINT reports.** Gist of reports and how they tie the target to the objective.

Table E-10. Target packet intelligence considerations (continued)

Intelligence products
• **HUMINT.**
▪ **HUMINT RFIs** for source handler. Grid of HVI family or meeting location. Map with location of HVI. Map to HVI with routes. Sketch of HVI location. Photo of HVI location. Photo of HVI and family.
▪ **HUMINT—is source available to perform these tasks?** GPS—use waypoint to develop route to site or pattern of life. Drive by HVI location and give signal to UAS. Drive by HVI family location and give signal to UAS. Go to HVI location and leave a marker—infrared or beacon. Go to HVI family location and leave a marker—infrared or beacon. Drive by meeting place and give signal to UAS. Drive by meeting place and leave a marker—infrared or beacon. Pinpoint spider holes or weapons storage sites at HVI location. Pinpoint security positions or vehicles. Details of security forces weapons and emplacements. Ride to site with unit taking action.
• **IMINT.**
▪ **Imagery products pertaining to the objective. Example:** With a view from the cardinal—directions, security positions, vehicles, roads, trails, activity on objective, activity around objective **(national-level imagery, UAS)**.
▪ **IMINT PIRs example.** Trails around structure—to spider holes or weapons storage sites. Roads, alleys, or trails. Terrain, ditches, walls, fences, abandoned vehicles, makeshift barriers or any other obstacles that will stop or slow a vehicle. Utility access points—sewer manholes, ingress and egress points. Obstacles around structure—vegetation, antenna towers, power lines, or any other obstacles that will restrict the use of aircraft on objective. Structures that can be used as observation points next to site. All smaller structures on site—tool sheds, garages, boathouses, or dog houses. Security positions. Fighting positions including trails to fighting positions. Vehicles on objective. Pattern of life.
• **SIGINT.**
▪ **SIGINT products or PIRs.** Assessment of the objective, including communication devices, scanners or jammers at objective.
• **MASINT.**
▪ **MASINT products or RFIs.** Trails, spider holes, fighting positions directions, security positions, vehicles, roads, trails, activity on objective, activity around objective.
Objective summary
• Collective assessment of the intelligence.
• **Pattern of activity.** Dates and times at locations, lights on or off, meeting times, vehicle traffic.
• **Include details from collections.** Security element signature, posture and attitude, special weapons or equipment, numbers, enemy situation in area, possible booby traps.
• **Attitude and capabilities of surrounding population.** (Surrounding population support of insurgency, surrounding populations support for individual, is this a heavily populated area?)
• **Potential triggers.** Identify any recommended or available triggers for the operations, including source trigger, SIGINT trigger, or other intelligence trigger.
• **History of objective.** Previous missions conducted against objective, has objective been previously prosecuted?
• **Alternate locations.** Alternate locations, in vicinity of primary objective, to which target may flee or occupy as an alternate site.
• **All known persons that are part of security.** Neighbors acting as lookouts or other security forces.

Table E-10. Target packet intelligence considerations (continued)

Objective details
• **Provide tactical information on structure.** ▪ Construction type. ▪ New or old structure. ▪ Floor plan. ▪ Number of stories. ▪ Number of exits in building. ▪ Structure configuration. Walls or fences. ▪ Vegetation around structure. ▪ Details of roads or alleyways surrounding the structure. Condition or width. ▪ Openings in walls, fences. ▪ Window locations in structure. Type or direction of opening. Hardware. ▪ Door locations in structure. Type or direction of opening. Hardware. ▪ Possible routes of ingress and egress. ▪ External lights on and around structure. ▪ What utilities are connected? ▪ Electronic burglar alarm. ▪ Animals. ▪ Blind spots, dead spaces, tallest building providing view of structure in area. ▪ Details of electronic equipment at site. ▪ Special terrain features—roads (name or number for all major roads in area), rivers, major power lines, tunnels, mines. ▪ Overall lighting in area. ▪ Checkpoints, bottlenecks, bridges on roads to objective. ▪ Overall assessment of the surrounding terrain for traffic purposes.
• Personnel at objective. Details of personnel—groundskeepers, housekeepers—at structure. ▪ Gender. ▪ Age. ▪ Willingness to fight or surrender.
• **Route to objective.** Map with detailed annotations for best route to objective, the objective with grid.
• **Alternate objective summaries.** ▪ All known alternate locations with grids. ▪ Safe houses. ▪ Houses, offices, meeting places. ▪ Primary residence. ▪ Secondary residence. ***Note.*** Develop HUMINT and IMINT objective folders for each location.
• Provide intelligence to support the IO strategy as required.

AO—area of operations
GPS—Global Positioning System
HUMINT—human intelligence
HVI—high-value individual
IED—improvised explosive device
IMINT—imagery intelligence
IO—information operations
MASINT—measurement and signature intelligence
MI—military intelligence
NOFORN—not releasable to foreign nationals
PIR—priority intelligence requirement
RFI—request for information
SIGINT—signals intelligence
UAS—unmanned aircraft system
VBIED—vehicle-borne improvised explosive device

This page intentionally left blank.

Appendix F

Weather Elements and Support

Weather is critical to Army operations. The command's intelligence officer is responsible for providing information on enemy, terrain, weather, and civil considerations to the commander and staff. Weather information is a part of intelligence as are threat and terrain data. Weather affects every aspect of Army operations.

RESPONSIBILITIES

F-1. The intelligence officer is responsible for weather intelligence. The G-2/S-2 is supported by a U.S. Air Force staff weather officer (SWO), who provides a staff weather specialty team to support the unit. The intelligence officer, the terrain analysis technician of the topographic support team, and the SWO comprise "the integrated weather support team." (See table F-1.)

Table F-1. Weather intelligence officer responsibilities

The intelligence officer—
• Interprets, in coordination with the terrain analysis technician, weather effects on Army weapon systems and tactics.
• Interprets threat potential to exploit the use of weather and weather modification through tactics and operations.
• Knows where to obtain weather data or information and the types of weather products available.
• Coordinates with the staff weather officer to ensure correct analysis of weather information affecting intelligence.
• Coordinates and consolidates the commander's requirements for weather support.
• Coordinates with the staff weather officer and artillery commander to arrange for the timely exchange of meteorological information.
• Disseminates processed weather information and intelligence to appropriate command elements.
• Coordinates weather training requirements of Army personnel with the G-3/S-3 and the commander.
• Assists the staff weather officer in special or general staff relations.
• Informs subordinate Army units of weather observations requested by the staff weather officer. The G-2/S-2 instructs subordinate units on required information—*where* and *when* it is required, and *how* it will be forwarded.
• Receives required information from the staff weather officer and disseminates weather intelligence through electrical means, briefings, and written studies.
• Integrates weather intelligence into the advance planning to ensure the incorporation of weather into future operations.
• Receives from the chemical staff officer interpretations of fallout prediction and travel of fallout clouds based on data provided by artillery meteorological sections and the weather teams.
The staff weather officer—
• Coordinates, supervises, and oversees all weather support for the designated Army units.
• Incorporates and coordinates weather support services from higher echelons and centralized weather facilities into the overall weather support structure.
• Develops weather observation collection strategies, forecast support, and dissemination procedures for the supported unit, and, as required, any associated lower echelon units without dedicated direct or host support.
• Supervises weather activities, performs weather intelligence preparation of the battlefield (IPB), and uses automated weather data processing systems, as available.
• Evaluates, interprets, analyzes, coordinates, supervises, and oversees the production of all weather support products to support Department of Defense and combatant commanders' requirements.
• Advises the commander and subordinate units on weather considerations for operations.

INTEGRATED METEOROLOGICAL SYSTEM

F-2. The Integrated Meteorological System (IMETS) is a mobile, tactical automated weather data receiving, processing, and dissemination system designed to provide timely weather and decision aid information to multiple command elements and their subordinate commands. IMETS can be a vehicle-mounted system or a laptop. The laptop configuration is referred to as IMETS-Light. IMETS is deployed to Army Service component command (ASCC), corps, division, special operations, aviation brigades, and brigade combat team (BCT) units. (See table F-2.)

Note. The IMETS is a program of record and part of the Distributed Common Ground System-Army (DCGS-A) (see MIHB 2-50). Their capabilities will be replaced in a series of system fieldings, culminating in DCGS-A weather services.

Table F-2. Integrated meteorological system capabilities

• Receives weather data from USAF strategic and theater centers. (In DCGS-A the weather service *will* host the joint environmental toolkit that provides the same capability.) • Receives, processes, tailors, stores, and disseminates weather data. • Hosts the weather running estimate mesoscale weather forecast model. • Displays and loops, on client machines, geostationary weather satellite imagery. • Displays and processes local weather observations from the AN/TMQ-53 or the IMETS Meteorological Station Group. • Provides weather situation portion of the COP. • Provides weather and effects or impacts on Army missions, displayed on the COP. • Provides weather messages. • IMETS hosts a Web page that allows sharing weather graphics and text products to a variety of users, using Web-based technology. • Products are available by Army functional area. • Web-page generator graphical user interface assists the weather team in the production of Web-page graphics products.
COP—common operational picture DCGS-A—Distributed Common Ground System–Army IMETS—Integrated Meteorological System USAF—U.S. Air Force

WEATHER IMPACTS ON MILITARY OPERATIONS

F-3. Virtually all forces that comprise the military capability are influenced by the weather—warfighting more often adapts to the weather rather than surmounts it, as it adapts to terrain and sea conditions. Weather exerts a constant influence on the readiness, morale, and effectiveness of military forces, the choice of military strategy and tactics, and the performance and useful life of military weapons systems. Advanced, high-cost weapon systems are also affected by the aerospace environment. Therefore, accounting for weather conditions should be incorporated into every facet of military force planning, deployment, employment, and system design and evaluation.

F-4. Weather impacts military forces and subsequent operations. Each forces type responds differently to the impact—dictating the types of forces that can be employed effectively. Weather data is part of the intelligence information required by commanders and staffs to plan and conduct combat operations. The results—from analyzing weather data, identifying weather effects, and assessing the impact of weather on systems, tactics, and operations—provide vital information for commanders to optimally employ their forces.

WEATHER CONDITIONS EFFECT ON MILITARY OPERATIONS

F-5. Weather significantly impacts friendly and threat operations. The military aspects of weather include visibility, wind aloft, precipitation, cloud cover, and temperature and humidity. Weather factor overlays are integrated with terrain overlays to predict areas where maneuver is possible. Table F-3 provides a description of weather conditions that affect the successful deployment of a broad spectrum of U.S. weapons systems—from ships to tanks to fighter planes.

Table F-3. Effects of weather conditions on military operations

Temperature
High temperatures— • Reduce aircraft lift capability and decrease the time personnel can remain in armored vehicles. • Cause gun tube droop, shimmers, and mirages. • Make vehicle exteriors too hot to touch. • Increase water consumption by troops.
Humidity
• Coupled with high temperatures, humidity further decreases crew effectiveness in closed armored vehicles and aircraft lift. • Humidity reduces a Soldier's ability to work and fight. • High humidity occurs in several potential battlegrounds. Failure to consider the effects on Soldiers, machines, and the area of operations (AO) can cause costly military mistakes. • Low humidity can stress Soldiers, machines, and the AO, as does high humidity. Low humidity is difficult for some automated sensors to measure. One effect of low humidity is static electricity generation around sensitive electronic boards. Low humidity allows for efficient infrared energy transmission through the atmosphere, allowing for target detection at further distances by infrared sensors.
Barometric pressure
Barometric pressure affects gunnery computations and ballistic performance.
Density
The combination of the temperature, humidity, and barometric pressure determines the air density.
Wind
Strong winds, especially crosswinds and high crosswinds— • Affect aircraft control near the ground during take-offs and landings. • Affect ground speed for low-level flights. • Affect trajectory projections and first-round capabilities for armored vehicles. • In the desert, produce dust storms that can last for hours or days. ***Note.*** Wind speed and direction are critical when predicting the airborne speed of chemical, biological, radiological, and nuclear (CBRN) weapons.
Visibility
Bad visibility affects— • Landings and takeoffs. • Visual reconnaissance. • Target acquisition and designation. • Terminally guided munitions. • The ability to scatter mines.
Cloud coverage
Clouds are always a major consideration for air operations: • Low overcast clouds limit the effectiveness of aerial illumination devices. • Overcast skies tend to limit heating of inactive targets and lower target detection range for thermal sights. • Clouds blocking ambient light from the moon or the stars limit night vision devices. • Low clouds degrade combat air support and aerial resupply missions.
Precipitation
• Rain affects visibility and the safety of flight crews and aircrafts. • Precipitation can cause predetonation of munitions. • Water droplets in the air disrupt electro-optical transmissions. • In infrared systems, rain cools objects differently in imagery, causing objects to appear differently.
Aircraft icing
• Under certain atmospheric conditions, aircraft structural icing becomes a serious, even deadly problem: • It places added weight and drag on an aircraft and can change the aerodynamic shape of the wings, reducing lift and maneuverability. • Chunks of ice can break off the airfoil, get sucked in into the jet intake, and destroy the engine. • Ice seriously affects radar reflective measurements at frequencies of major interest to military equipment designers. • Ice crystals have different shapes, and with temperatures hovering around the freezing point, they change form as they melt and refreeze. This effect can cause poor performance of equipment, such as mine detectors.

Table F-3. Weather conditions effect on military operations (continued)

Thunderstorms and lightning
• Extreme weather that includes thunderstorms and lightning is hazardous to in-flight operations, refueling, and rearming operations. • Severe weather can affect Navy vessels. • Small vessels, in particular, are susceptible to bad weather, which impairs their ability to transit or conduct operations. • Because a typical lightning strike involves millions of volts and amperes, not only does it destroy by direct hit, lightning can also destroy by induced potentials on networks of wires nearby.
Turbulence
• Severe weather and clear air turbulence is a critical condition affecting all aviation assets and missions. • Turbulence can cause aircraft structural damage or crashes on takeoffs and landings. • Severe turbulence may cancel all operations.
Space weather
• Space weather affects military communications, especially in the high-frequency spectrum. • Space weather has become an important facet in the satellite communication age. Although it is impossible to prevent phenomena, produced by the sun, from affecting communications and navigation systems, learning new methods to predict weather-event occurrences can minimize their effects.

SOLAR ACTIVITY DISTURBANCES

F-6. Solar activity causes three main disturbances:

- **Radio blackout.** Solar flares disturb the ionosphere with X-ray transmission, which impedes high frequency radio and navigation systems, often causing total communication loss.
- **Geomagnetic storms.** Disturbances in the geomagnetic field due to gusts in the solar wind that blow by Earth. Coronal mass ejections, closely associated with solar flares, cause geomagnetic storms, which affect power systems, spacecraft operations, and radio propagation and navigation.
- **Solar radiation storms.** Solar flares greatly increase the radiation count, which creates a radiation hazard to astronauts, high-flying planes, satellite operations, and communications systems. (See figure F-1.)

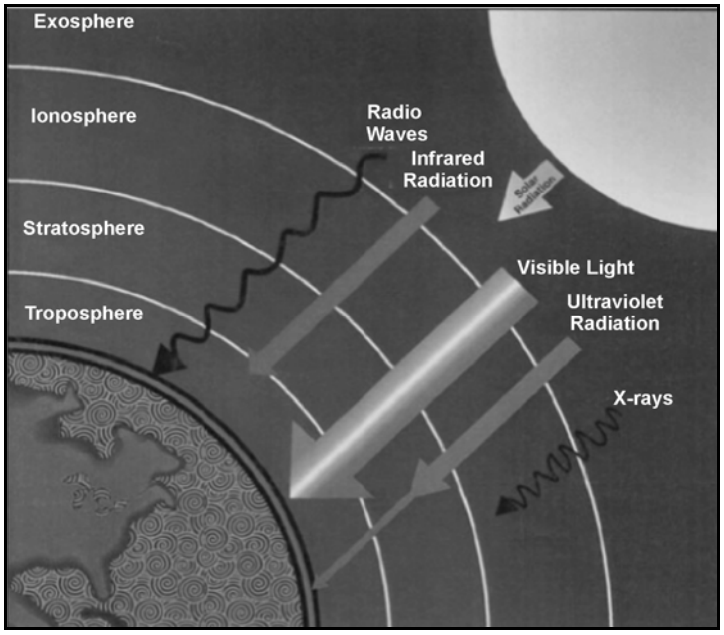


Figure F-1. Solar radiation

F-7. Because solar radiation increases the density of the ionosphere with energized particles, Global Positioning System (GPS) operations are adversely affected. GPS receivers depend on radio signals from several orbiting satellites. When these signals pass through the ionosphere, the various density changes affect the speed at which the signals travel, causing a "propagation delay" in the GPS signal resulting in range errors.

WEATHER EXPLOITATION

F-8. Weather exploitation is the deliberate use of knowledge about friendly and threat operations capabilities under given natural environmental conditions to set the terms of battle, resulting in optimal performance of the friendly force and reduced effectiveness of the threat force. Using this definition, one can examine and assess three aspects of weather exploitation:

- **Military force capability in terms of personnel, equipment, and doctrine—**as a whole, a nation's military capability is largely independent of the natural environment. However, individual engagements, missions, or even major operations can be significantly affected by the natural environment.
- **Effect of relevant observed weather on military operations—**requires the most improvement in terms of learning the vulnerabilities of both sides and incorporating that intelligence into the air and space strategy.
- **Prediction accuracy of relevant observed weather—**important in the planning phase because forces and weapons mixes and strategy decisions, such as target selection and route of attack, are determined. Modern air and space forces improve how to incorporate weather predictions into the planning cycle, especially with the advent of new and faster ways to access and visualize relevant, real-time weather information.

WEATHER EFFECTS ON STABILITY AND CIVIL SUPPORT OPERATIONS

F-9. Terrain and weather analysis occur simultaneously, in most instances. However, operations in an urban environment present some unique concerns. Inclement weather affects the availability of food supplies. Mass demonstrations use good weather for maximum turnout. Bad weather further degrades poor road networks. Rain and heavy winds disrupt or stop a PSYOP such as a leaflet drop. Common concerns include—

- Wind.
- Precipitation.
- Visibility.
- Cloud cover.
- Temperature and humidity.

WIND

F-10. Wind patterns and effects are important concerns in most environments; however, larger urban areas have unique challenges that, otherwise, usually occur in rugged mountain areas. Depending on weather conditions, when compared to unrestricted terrain, the wind may be blocked, reduced, or enhanced in areas surrounded by large structures, which can cause a buildup of smog (or lethal chemicals, if present), enhance the fire threat, restrict helicopter use (swirling winds), and other factors. These factors make downwind predictions for chemical, biological, radiological, nuclear (CBRN) difficult. Radical temperature changes associated with the combination of wind, precipitation, and structures, such as tunnels or high rises, significantly affect urban operations, especially during cold and wet periods, which affect the wind chill factor.

PRECIPITATION

F-11. City engineers and urban sanitation workers are aware of artificial changes to the topography caused by manmade structures. Rain or melting snow often floods basements, underpasses, tunnels, sewers, and subway systems; streets become impassable due to water, snow, or ice; and exposed or weathered electrical systems may short-circuit. Precipitation washes CBRN agents into underground systems. Some areas become impassable contaminated "hot spots" that affect drinking water supplies. As CBRN agents are absorbed by brick or unsealed concrete sewer walls, the effects are pronounced, and CBRN detection and decontamination crews will be required when operating in these areas.

VISIBILITY

F-12. Although visibility is critical at any given time, it is more so during operations in urban environments. Traditionally, night and periods of reduced visibility favor surprise, infiltration, detailed reconnaissance, attacks across open areas, seizure of defended strong points, and reduction of defended obstacles. Areas, regardless of size, with considerable amounts of artificial and background light, put unobserved movement at risk. The urban area's numerous structures, easily identified during the day, may not be so visible at night, which increases disorientation. Technology enhancements become a necessity (night vision devices or GPS) for Soldiers operating in the area.

F-13. Many urban areas are located along canals or rivers, which creates a potential for fog in low-lying areas. Industrial and transportation areas are the most affected by fog due to their usual proximity to waterways. In heavy industrial areas, smog can limit visibility regardless of light conditions. Fog and smog can ground operations by limiting illumination and reflective heating as well as by degrading many target acquisition (TA) systems and limiting the use of infrared-guided artillery rounds and general aviation.

CLOUD COVER

F-14. In an urban environment, cloud cover has significant tactical effects. In addition to visibility effects, cloud cover above an urban area can combine with building shadows to affect observation. Intermittent cloud cover may cause shadows on the ground, which could confuse observers. Low cloud cover over urban areas can restrict air operations due to the numerous vertical manmade obstructions in these areas.

TEMPERATURE AND HUMIDITY

F-15. Lower atmospheric inversions are common over cities, especially cities located in low-lying "bowls" or river valleys. Inversion layers may trap dust, pollutants, or chemical agents and reduce visibility. The atmospheric conditions that create inversions cause higher than normal air temperature. The heating of buildings during the winter and the reflection and absorption of summer heat make built-up areas warmer than surrounding open areas during both summer and winter. The temperature difference ranges from 10 to 20 degrees, which adds significantly to the problems faced in urban operations. Summer heat, combined with the physical requirement of urban combat, can cause severe heat exhaustion. In the winter, Soldiers fall victim to exposure in nominally protected areas such as tunnels or causeways.

F-16. Temperature variances, due to air inversions, also affect thermal sights during crossover periods of warm to cold and vice versa. Air inversions trap pollution, smoke from fires, or gases (such as tear gas) closer to the ground. This crossover period should be identified, since it may differ from urban area to urban area. Extremely cold temperatures and heavily constructed buildings affect target identification for thermal sights. For example, thick walls may make combat vehicle identification difficult by distorting hotspots, and increased use of heaters and warming fires may clutter thermal sights with numerous hotspots.

F-17. Before Soldiers are sent into an urban area, especially those comprised of numerous large structures, staff planners have a good understanding of the weather and the weather effects in the urban environment. The SWO provides the basic weather forecasts for planning purposes.

LIGHT DATA

F-18. Although light data is not weather data, like weather factors, it affects visibility. Light data describes astronomical event, such as—

- Sunrise and sunset.
- Associated twilight periods.
- Moonrise and moonset.
- Illumination amounts.

RISE, SET

F-19. Sunrise and sunset refer to the times when the upper edge of the Sun's disk is on the horizon—considered unobstructed relative to the location of interest. Moonrise and moonset times are computed for the same circumstances as for sunrise and sunset. However, moonrise and moonset occurs at any time during a 24-hour period.

TWILIGHT

F-20. Before sunrise and again after sunset, there are intervals of time—twilight—when there is natural light provided by the upper atmosphere, which does receive direct sunlight and reflects part of its light toward the Earth's surface. Some outdoor activities are conducted without artificial illumination during these intervals—it is useful to have means to set limits beyond which a certain activity should be assisted by artificial lighting. What mostly determines the amount of natural light during twilight are the state of the atmosphere and local weather conditions.

CIVIL TWILIGHT

F-21. Civil twilight begins in the morning and ends in the evening when the Sun's center is geometrically six degrees below the horizon. This is the limit at which twilight illumination is sufficient, in good weather conditions, for terrestrial objects to be distinguishable.

NAUTICAL TWILIGHT

F-22. Nautical twilight begins in the morning and ends in the evening when the Sun's center is geometrically 12 degrees below the horizon. At the beginning or end of nautical twilight, under good atmospheric conditions and in the absence of other illumination, general outlines of ground objects are distinguishable, but detailed outdoor operations are impossible, and the horizon is indistinct. (See table F-4.)

Table F-4. Light data visibility

Period of time	*Location of Sun's center in degrees below the horizon*
Beginning morning nautical twilight (BMNT)	12 degrees
Beginning morning civil twilight (BMCT)	6 degrees
End evening civil twilight (EECT)	6 degrees
End evening nautical twilight (EENT)	12 degrees

F-23. Under ideal conditions, the period when there is adequate visibility for large-scale operations is between beginning morning civil twilight (BMCT) and end evening civil twilight (EECT). Generally, visibility at beginning morning nautical twilight (BMNT) is about 400 meters—enough light for close coordination between personnel. Halfway between BMNT and BMCT (or EECT and end evening nautical twilight [EENT]), there is enough light for visual ground adjustment of close-in artillery fire and air strikes.

WEATHER PRODUCTS

F-24. The G-2/S-2 provides weather and weather effects information to the commander and supported or subordinate units. Methods may vary among units and echelons. Figure F-2 depicts how the weather elements and parameters in the forecast might be displayed.

Weather forecast valid for 121200Z to 131200Z Pungsan			
24-hour forecast			
Skies	Clear morning and night, partly cloudy in the afternoon, bases 3,000 feet.		
Visibility	Unlimited, occasionally 1 to 2 miles in blowing snow during afternoon.		
Winds	North to northwest, 10 to 15 knots, occasional gusts to 25 knots in afternoon.		
Temperatures	Maximum: 10°F Minimum: -20°F.		
72-hour outlook	Cloudy skies, snow flurries during afternoon hours lowering visibility to 2 to 4 miles. Temperatures: Maximum: 20°F Minimum: -5°F.		
Light data	BMNT: 1247Z BMCT: 2221Z Sunrise: 2251Z	Sunset: 0820Z EECT: 0851Z Moonrise: 1924Z	Moonset: 0819Z Night-vision goggles use
BMCT—beginning morning civil twilight BMNT—beginning morning nautical twilight	EECT—end evening civil twilight NVG—night-vision goggles		Z—Zulu time

Figure F-2. Example of a weather forecast chart

F-25. A weather effects forecast matrix uses color codes as one way to display potential weather impacts on operations, systems, and unit personnel. (See figure 3-4 [page 3-9].) The words “moderate” and “severe” can be used, also. Do not list all equipment or systems, but have the list available to answer commander or staff questions. Emphasize critical systems.

F-26. If weather conditions change significantly during the period covered by the SWO’s forecast, update the weather effects chart. Because a brigade or battalion’s area of interest (AOI) is small, the SWO’s forecast is likely to be uniform across the AOI.

WEATHER TOOLS

F-27. Figures F-3 and F-4 (page F-10) and tables F-5 through F-11 (pages F-10 though F-13) depict weather tools that assist in ascertaining conditions during military operations.

Mission	*Weather element*	*Favorable (unrestricted)*	*Marginal (restricted)*	*Unfavorable (severely restricted)*
Maneuver: mobility (track vehicles, day)	Visibility Rainfall Snow depth	>1.5 km <0.1 in per h <12 in	0.8 to 1.5 km 0.1 to 0.5 in per h 12 to 20 in	<0.8 km >0.5 in per h >20 in
Maneuver: mobility (track vehicles, night with PVS-5 NVG)	Visibility Rainfall Snow depth	>0.2 km <0.1 in per h >12 in	0.1 to 0.2 km 0.1 to 0.5 in per h 12 to 20 in	<0.1 km >0.5 in per h >20 in
Maneuver: mobility (dismounted infantry)	Visibility Rainfall Snow depth Temperature Wind chill temperature	>0.3 km <0.1 in per h <3 in <32 C >0 C	0.1 to 0.3 km 0.1 to 0.5 in per h 3 to 6 in >32 C 0 C to -30 C	<0.1 km >0.5 in per h >6 in ---------- <-30 C
Maneuver: weapons positioning (antiarmor direct fire)	Visibility Temperature	>3.0 km >18 C	0.5 to 3.0 km <-18 C	<0.5 km ----------
Fire support (155 mm)	Visibility Ceiling Surface wind Snow depth	>5.0 km >800 ft < 35 knots <4.0 in	1.5 to 5.0 km 500 to 800 ft 35 to 50 knots 4.0 to 6.0 in	<1.5 km <500 ft >50 knots >6 in
Fire support (CAS A-10)	Visibility Ceiling	>8.0 km >3,000 ft	5.0 to 8.0 km 500 to 3,000 ft	<5.0 km <500 ft
Intelligence (fixed-wing visual reconnaissance)	Visibility Ceiling	>5.0 km <3/8 clouds	3.0 to 5.0 km 3/8 to 5/8 clouds	<3.0 km >5/8 clouds
Air defense artillery (Vulcan, Chaparral, Stinger)	Visibility Ceiling Rainfall	>5.0 km >5,000 ft <0.5 in per h	3.0 to 5.0 km 3,000 to 5,000 ft 0.5 to 1.0 in per h	<3.0 km <3,000 ft >1.0 in per h
CBRN (chemical, artillery delivery)	Wind below 16 m Stability Temperature Humidity	<5 knots Stable >21 C >60 percent	5 to 7 knots Neutral 4 to 21 C 40 to 60 percent	<7 knots Unstable (lapse) <4 C <40 percent
Smoke	Precipitation	None	Light	Moderate or heavy
Airborne (C-130 to C-17)	Visibility Ceiling Surface wind Precipitation	>5.0 km >500 ft <10 knots None	1.0 to 5.0 km 300 to 500 ft 10 to 13 knots Light	<1.0 km <300 ft >13 knots Freezing rain or hail
Aviation (rotary wing)	Visibility Ceiling Surface wind Precipitation	>1.5 km > 500 ft <20 knots None	0.4 to 1.5 km 300 to 500 ft 20 to 30 knots Light	<0.4 km <300 ft >30 knots Freezing rain or hail

C—Celsius
CAS—close-air support
CBRN—chemical, biological, radiological, nuclear
ft—foot/feet
h—hour(s)
in—inch(es)
km—kilometer(s)
mm—millimeter(s)
m—meter
NVG—night vision goggles

Figure F-3. Sample weather effects critical values

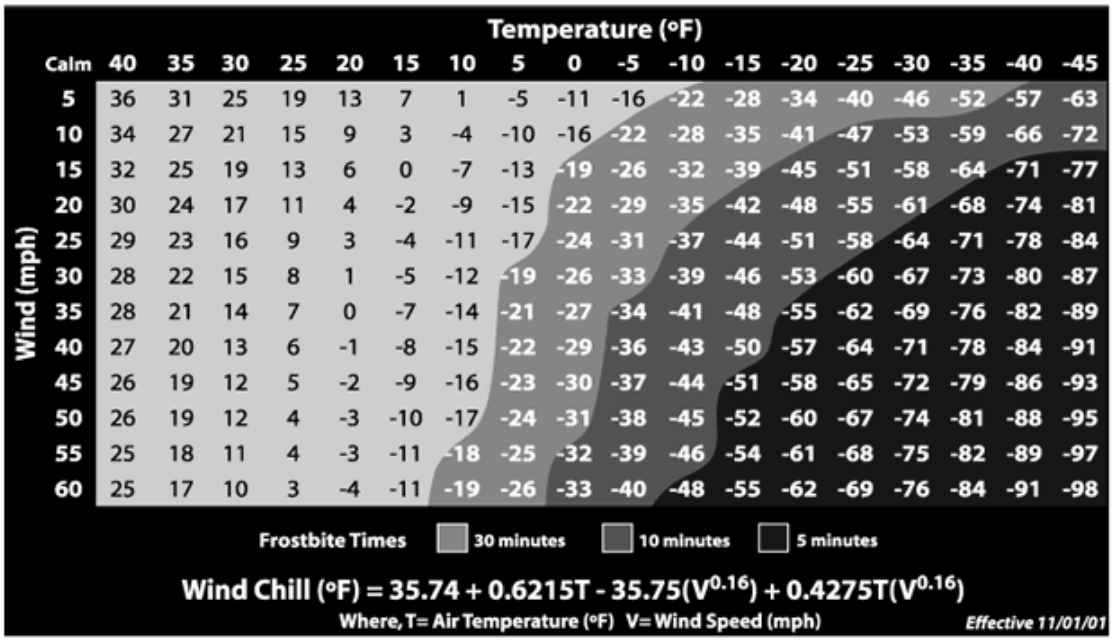


Figure F-4. National weather service wind chill chart

Table F-5. Extreme weather conditions

March rates in extreme cold		***Distance covered in one day of marching***	***Maximum snow depths***
Infantry (snow < 30 cm deep)	3 to 4 km/h	Infantry—12 to 24 km Ski unit—32 to 40 km Tracked vehicles—96 to 112 km	***Wet snow*** Personnel—12 to 18 in Wheeled vehicles (with chains)—18 in Tracked vehicles—30 in
Infantry (snow > 30 cm deep)	1 to 2 km/h	***Thickness of ice required for passage***	
Soldier on skis	6 to 8 km/h		
Tracked vehicles	10 to 24 km/h		
Tanks and APCs in— Snow < 50 cm—employed as usual Snow 50 to 75 cm—short moves Snow > 75 cm—restricted to roads or cleared routes		Infantry—10 cm Medium tanks—70 cm	***Dry snow*** Personnel—18 to 24 in Wheeled vehicles (with chains)—24 in Tracked vehicles—48 in
APC—armored personnel carrier cm—centimeter(s)	h—hour(s) in—inch(es)	km—kilometer(s) < —less than	> —more than

Table F-6. Estimating wind speed

Knots	***Observation***
1	Smoke, vapor from breath, or dust raised by vehicles or personnel—rises vertically. No leaf movement.
1 to 3	Direction of wind shown from smoke, vapor from breath, or dust raised by vehicles or personnel. Slight intermittent movement of leaves.
4 to 6	Wind slightly felt on face. Leaves rustle.
7 to 10	Leaves and small twigs in constant motion.
11 to 16	Wind raises dust from ground. Loose paper and small branches move.
17 to 21	Small trees with leaves sway. Coastal wavelets form on inland waters.
22 to 27	Large branches on trees in motion. Whistle heard in telephone or fence wires.
28 to 33	Whole trees in motion. Inconvenience felt walking against wind.
One knot = 1 to 15 miles per hour	

Table F-7. Load-bearing capacity on fresh water ice

Load	*Minimum ice thickness (cm)*	*Minimum distance between load (m)*
Soldier on foot	5	5
Soldier on skis or snowshoes	3	5
Vehicles		
¼–ton truck	20	15
¾–ton truck	25	20
1 ¼–ton truck	33	25
2 ¼–ton truck	40	25
2 ½–ton truck	40	25
5–ton truck	55	60
5–ton tanker	90	80
5–ton tractor with loaded trailer	90	80
M561 Cargo Carrier	25	20
Main battle tank	80	70
M88 Recovery Vehicle	85	70
M108 Howitzer, Self-propelled, 105 mm	50	40
M109 Howitzer, Self-propelled, 155 mm	50	40
M110 Howitzer, Self-propelled, 8 inch	55	50
M113 APC	45	25
M548 Cargo Carrier	45	25
M577 Command Post Carrier	45	25
M578 Recovery Vehicle	65	60
BV209 Small Unit Support Vehicle	35	15

APC—armored personnel carrier cm—centimeter(s) m—meter(s) mm—millimeter(s)

Table F-8. Weather effects on courses of action

	Temperature			*Humidity*		*Wind (knots)*			*Precipitation*		*Ceiling (feet)*			
	Cold	Med	Hot	Low	High	<13	13 to 30	>30	Rain	Snow	Fog	<1,5000	1,500 to 3,000	>3,000
Attack	+	0	-	0	-	0	+	-1	+	-1	+	0	0	0
Defend	-	0	-2	0	-2	0	-	-	-	-	-	0	0	0
Reinforce	+	0	-	0	-	0	0	-	+/-3	-	+	0	0	0
Withdraw	+	0	-	0	-	0	+	-	+/-3	-	+	0	0	0
Artillery	-	0	0	0	-	0	-	-	-	-	-	-	0	0
Airmobility	-	0	-	0	-	0	-	x	x	x	-	-	+	+
Airborne	-	0	-	0	-	0	-	x	-	-	-	-	0	+
CAS	0	0	-	0	-	0	-	x	x	x	x	-	-	+
Chemical	-	0	+	0	+	+	-	-	-	-	0	0	0	+
UW	-	0	0	0	0	+	+	-	0	-	+	+	0	-
Intel collect	-	0	-	0	-	0	-	-	-	-	-	-	-	-
EW/Commo	-	0	-	0	-	0	0	-	-	-	-	0	0	-
Smoke	0	0	0	-	+	+/-	-	-	+/-1	+	+	0	0	-

+	Favors.
-	Disfavors.
+/-	May favor or disfavor, depending on circumstances.
0	Neither favors or degrades.
X	Strongly disfavors.
1	Does not favor any military operations; favors attack relative to defense.
2	Does not favor most military operations; favors defense relative to attack.
3	Hinders mobility but increases concealment.

CAS—close-air support
collect—collection
commo—communication(s)
EW—electronic warfare
Intel—intelligence
UW—unconventional warfare
< —less than
> —more than

Note. Weather effects depend on tactical situations. Use chart as a general guide only. Effects on attack and defense are shown in isolation, rather than as relative to each other.

Table F-9. Precipitation terms

Term	*Specifications*	*Reduction in visibility*
Very light	Scattered drops or flakes that do not completely wet an exposed surface regardless of duration.	None
Light	A trace of 0.10 of an inch of precipitation per hour; maximum 0.01 of an inch in six minutes.	Visibility 5/8 statute mile or more.
Moderate	1.11 to 0.30 of an inch per hour; between 0.01 and 0.03 of an inch in six minutes.	Visibility less than 5/8 statute mile, but not less than 5/16 statute mile.
Heavy	More than 0.30 of an inch per hour; more than 0.03 inches in six minutes.	Visibility less than 5/16 statute mile.

Table F-10. Beaufort wind scale

No.	*Miles per hour*	*Knots*	*Description*	*Sea condition*	*Specifications*
0	0-1.7	0-1	Calm	Glassy-smooth, Mirror-like.	Calm; smoke rises vertically.
1	1.8-4.0	1-3	Light air	Scale-like ripples.	Direction of wind shown by smoke drift, but not by wind vanes.
2	4.1-7.4	4-6	Light breeze	Small, short wavelets with glassy crests.	Wind felt on face, leaves rustle, ordinary vane moved by wind.
3	7.5-12.0	7-10	Gentle breeze	Large wavelets, crests begin to break, occasional foam.	Leaves and small twigs in constant motion, wind extends light flag.
4	12.1-18.9	11-16	Moderate breeze	Small waves, some white caps, more frequent foam.	Raises dust and loose paper; small branches are moved.
5	19.0-24.7	17-21	Fresh breeze	Moderate longer waves, better formed, many white caps, much foam, some spray.	Small trees begin to sway; crested wavelets begin to form on inland waters.
6	24.8-31.6	22-27	Strong breeze	Large waves form, many whitecaps, foam everywhere, more spray.	Large branches in motion, whistling heard in telegraph wires, umbrellas used with difficulty.
7	31.7-38.5	28-33	Moderate	Sea heaps up; streaks of foam, spindrift begins.	Whole trees in motion, inconvenience felt in walking against wind.
8	28.6-46.6	34-40	Fresh gale	Moderately high, long waves, crests into spindrift, well-marked streaks of foam.	Breaks twigs off trees, generally impedes progress.
9	46.7-53.9	41-47	Strong gale	High waves, sea rolls, dense streaks, spray affects visibility.	Slight structural damage occurs (chimney pots and slates removed).
10	54-63	48-55	Whole gale		Trees uprooted, considerable structural damage occurs.
11	64-72	56-63	Storm		Widespread damage.
12	73-82	64-71	Hurricane		

Conversion:
Wind (knots) = 0.868391 wind (miles per hour)
Wind (miles per hour) = 1.15155 wind (knots)

Table F-11. Conversion factors

To convert	*To*	*Use*
	Temperature	
Degrees Fahrenheit (°F)	°C	°C = 5/9 (°F – 32)
Degrees Celsius (°C)	°F	°F = (9/5 °C) + 32)
	Distance	
Kilometers	Miles	0.62
Kilometers	Nautical miles	0.54
Kilometers	Feet	3,280.80
Miles	Kilometers	1.61
Miles	Nautical miles	0.87
Miles	Yards	1,760.00
Miles	Feet	5,280.00
Nautical miles	Kilometers	1.85
Nautical miles	Miles	1.15
Meters	Feet	3.28
Yards	Feet	3.00
	Speed	
Kilometers/hour	Miles/hour	0.62
Kilometers/hour	Knots (nautical miles/hour)	0.54
Miles/hour	Kilometers/hour	1.61
Miles/hour	Knots	0.87
Miles/hour	Feet/second	1.467
Knots	Kilometers/hour	1.85
Knots	Miles/hour	1.15
Meters/second	Feet/second	3.281
Meters/second	Miles/hour	2.237
	Pressure	
Inches of mercury (Hg)	Millibar	33.86395
Millibar (Mb)	Inches of mercury	0.295299
	Length	
Feet	Meters	0.3048
Feet	Centimeters	30.48
Inches	Meters	0.0254
Inches	Centimeters	2.54
Meters	Yards	1.094
Yards	Meters	0.9144

This page intentionally left blank.

Appendix G

Intelligence Resources

There are numerous resources available to the intelligence professional to assist in conducting intelligence operations. Knowing where to start when looking for specific information can be the biggest obstacle to overcome when conducting these operations. This appendix lists some starting points for obtaining information/intelligence and contains some of the most commonly used analyst aids. For a more comprehensive list of resources used for intelligence reach operations, see FM 2-33.5.

MILITARY PUBLICATIONS

G-1. The references mentioned in this manual can be found at the following Web sites:

- **Army publications.** Army Publication Directorate Web portal: http://www.apd.army.mil/.
- **Joint publications.** Joint Doctrine, Education, and Training Electronic Information System (JDEIS) Web portal: https://jdeis.js.mil/jdeis/index.jsp.

MILITARY INTELLIGENCE TRAINING PUBLICATIONS

G-2. Military intelligence (MI) approved and draft individual and collective training manuals (for example, Soldier training plans [STPs] and MI Gunnery) are also available for downloading and viewing on the **Intelligence Knowledge Network** (IKN), at https://icon.army.mil/.

PERSONNEL SECURITY RESOURCE

G-3. **Joint Personnel Adjudication System** (JPAS), at https://www.dss.mil/portal/ShowBinary/BEA%20Repository/new_dss_internet/diss/jpas/jpas.html, is the Department of Defense (DOD) personnel security migration system for—

- The virtual consolidation of the DOD central adjudication facilities.
- Use by nonsensitive compartmented information (non-SCI) security program managers and special security officers.
- Special access program managers.
- DOD contractor security officers.

G-4. JPAS automates both core and central adjudication facility-unique functionality and provides "real-time" information about clearance, access, and investigative status to authorized DOD security personnel and other interfacing organizations, such as Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, and U.S. Air Force Personnel Center.

MILITARY INTELLIGENCE OPEN-SOURCE RESOURCES

G-5. **Intelligence Knowledge Network** (IKN), at https://icon.army.mil/, is a knowledge management tool that enables intelligence Soldiers worldwide to communicate, collaborate, and investigate. IKN—

- Hosts discussion forums.
- Serves as a single point of entry to get to U.S. Army Intelligence Center of Excellence (USAICoE) and other intelligence community Web sites.

- Hosts a variety of public and private Web applications that support the intelligence community.

G-6. **University of Military Intelligence (UMI)**, at http://www.universityofmilitaryintelligence.us, is the distance learning arm of the MI Schoolhouse. From the UMI Web site, MI professionals can access—

- Self-paced and reachback training.
- The Cultural, Foreign Language Integration Center.
- MI training resources.
- The New Systems Training and Integration Office at Fort Huachuca, AZ.

G-7. **AKO intelligence**, at https://www.us.army.mil/suite/page/6, features—

- The Intelligence Collaboration Center.
- Knowledge Center (documents, FMs).
- Training, agencies, policy, doctrine, and links to other intelligence related sites.

G-8. **AKO Army Open-Source Program**, at https://www.us.army.mil/suite/page/115902, features open-source—

- Events.
- Discussion forum.
- Intelligence products.
- Handbooks.
- Links of interest.

G-9. **AKO Library Reference Center**, at https://www.us.army.mil/suite/page/51, includes many databases and excellent resources, such as—

- Military and Government Collection.
- Academic Search Premier—click on "Academic Resources." This database contains 4,700 publications with full text coverage in biology, chemistry, education, engineering, humanities, physics, psychology, religion and theology, sociology.

G-10. **Department of the Army Intelligence Information Service (DAIIS) Country Research** portal, at https://www.us.army.mil/suite/page/132281, has road-mapped and data-mined the Joint Worldwide Intelligence Communications System (JWICS), Secure Internet Protocol Router Network (SIPRNET), Combined Enterprise Regional Information Exchange System (CENTRIXS), and unclassified networks. This results in a "one stop shop" for intelligence information. Data is pushed across multiple networks to ensure the intelligence consumers have access to the data from the network on which they operate. For example, collateral data from JWICS is pushed down to SIPRNET, and unclassified data is pulled up to JWICS and SIPRNET. Some of the links on this site include—

- Open-source products (Early Bird, Terrorism Daily Update, Basra Bugle).
- Foundry Program—also available on SIPRNET at http://www.portal.inscom.army.smil.mil/g3/or/foundry/default.aspx.
- Intelligence community links (Federal Bureau of Investigation [FBI], Central Intelligence Agency [CIA], National Security Agency [NSA]).
- Combatant command links.
- Analyst references (CIA World Factbook).

G-11. **DAIIS** is available at—

- JWICS: http://dadpm.inscom.ic.gov.
- Intelligence Dominance Center Portal on JWICS: http://idcportal.inscom.ic.gov/.
- SIPRNET: http://dadpm.inscom.army.smil.mil.
- SIPRNET Portal: http://www.portal.inscom.army.smil.mil/.
- CENTRIXS: http://dadpm.inscom.mcfi.cmil.mil.
- AKO: https://www.us.army.mil/suite/page/132281.

G-12. **General weather** Web sites include—

- Climatology (14th Weather Squadron):
  - https://www.afccc.af.mil/SCIS.
  - SIPRNET: http://afccc.asheville.af.smil.mil.
  - JWICS: http://www.afccc.ic.gov.
- Joint Air Force and Army Weather Information Network (JAAWIN):
  - https://weather.afwa.af.mil.
  - SIPRNET: http://weather.offutt.af.smil.mil.
- Links to more specific forecasts created by regional operational weather squadrons are available through JAAWIN.

G-13. **Open-Source Information System**, now called Intelink, is a private Intranet connecting various networks for the exchange of unclassified U.S. Government and other open-source information in intelligence community agencies, military commands, and certain other organizations. No special software is needed. With a password, access Intelink at https://www.intelink.gov:

- **Intelink-SBU account.** Request an Army sponsored Intelink remote access account through a personal AKO e-mail to: accounts@intelink.gov. Upon receipt, scroll down to the end of the brochure for the form and send as an e-mail attachment to receive a password.
- **Intelink databases and sites.** Use the Open-Source Information System login and password. Request an Intelink password once connected to Intelink. Use this password for the first-time login and for accessing Jane's. The original interface is in the right frame under ***Favorites***. The following are a few of the topics accessible on Intelink:
  - *The National Ground Intelligence Center*, at https://www.intelink.gov/rims/organizationList.aspx, is the largest intelligence producer in the Army.
  - *Foreign Military Studies Office/World Basic Information Library*, at http://fmso.leavenworth.army.mil/index.htm, is a research and analysis center under the Army's Training and Doctrine Command, Intelligence Support Activity. The Foreign Military Studies Office manages and operates the Fort Leavenworth Joint Reserve Intelligence Center and conducts analytical programs focused on emerging and asymmetric threats, regional military and security developments, and other issues that define evolving operational environments worldwide.
  - *Pathfinder* (unclassified version), at https://pathfinder.intelink.gov, is a data-mining and visualization tool. Pathfinder has become a core enabling technology in overseas contingency operations.
  - *Jane's online*, at https://www.intelink.gov/Reference/janes/, is an excellent site for defense information, military systems, terrorism, and country studies.
  - *EbscoHost databases*, https://www.intelink.gov/osis/cgi-bin/rd?http://search.epnet.com, features databases to search for articles in newspapers, journals, and magazines. Included are the *Academic Search Premier*, *Military & Government Collection*, *Business Source Premier*, and *Environmental Issues and Policy Index*.
  - *Open-Source Center* (formerly the Foreign Broadcast Information Service), at http://opensource.gov, provides translation and exploitation of foreign media, including foreign language Web sites and multimedia. The center also hosts a variety of commercial databases, such as *Jane's*, *Oxford Analytica*, *Lexis-Nexis*, *Economist Intelligence Unit*, and others.
  - *Marine Corps Intelligence*, at https://www.intelink.gov/mcia/handbook.htm, accesses to *Smart Cards*, *Country Handbooks*, and others.
  - *Oxford Analytica*, at https://www.intelink.gov/references/references.aspx?pageType=Reference, is an international consulting firm that provides business and political leaders with timely analysis of worldwide political, economic, and social developments.

G-14. **Other open-source** sites:

- *Google Scholar*, at http://scholar.google.com/, searches academic sites on the deep Web.
- *Google Earth*, at http://earth.google.com/, is a three-dimensional interface to the planet and is a free download.
- *The Intelligent Road/Rail Information Server*, http://www.tea.army.mil/tools/irris.htm.
- *Defense Technical Information Center*, http://www.dtic.mil/.
- *Center for Army Lessons Learned*, http://call.army.mil/.
- *Strategic Studies Institute*, http://www.strategicstudiesinstitute.army.mil/.

MESSAGE TRAFFIC

G-15. **Intelligence tear line reporting:**

- A semiautomated process used to migrate tear line messages to JWICS, STONEGHOST, SIPRNET, CENTRIXS, and releasable servers.
- Through JWICS, at http://dadpm.inscom.ic.gov/reports/tearlines.asp, or SIPRNET, at http://dadpm.inscom.army.smil.mil/MPS, extract a collateral tear line message from limited access messages.

G-16. **SIPRNET message traffic** (DAIIS on SIPRNET):

- Access the Multimedia Message Manager (M3) on SIPRNET, at http://dadpm.inscom.army.smil.mil/m3/index.asp. M3 is the standard message handling system for the intelligence community and provides—
  - Real-time dissemination of message traffic.
  - Retrospective information searches.
  - Message composition, coordination, and release.
- SIPRNET M3 accounts provide access to Army G-2 collateral message traffic.
- Message traffic sources include—
  - CIA.
  - Open-Source Center.
  - Operations IRAQI FREEDOM (OIF)/Operation ENDURING FREEDOM (OEF) tactical reports.
  - FBI.

INTELLIGENCE PRODUCTION

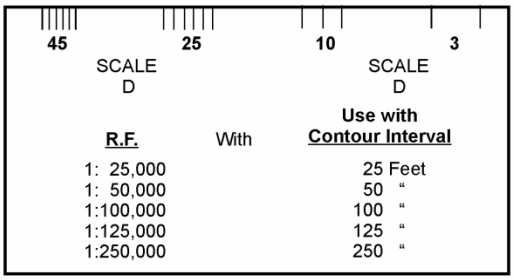
G-17. Community On-Line Intelligence System for End Users and Managers (COLISEUM)—

- Is accessed through JWICS, at http://coliseum.dia.ic.gov, or SIPRNET, at http://coliseum-s.dia.smil.mil.
- Executes DOD policy and procedures under the Defense Intelligence Analysis Program.
- Ensures Army customers obtain new intelligence production from the Defense Intelligence Agency (DIA), Service national production centers, and joint intelligence centers.
- Researches and validates Army intelligence production requirements.

ANALYST AIDS

G-18. Analysts use numerous techniques and tools to assist in providing intelligence support to operations. Figure G-1 and tables G-1 through G-4 (pages G-5 through G-6) depict some, but not all of the analyst aids used to determine terrain slope calculations, lane widths, route types, identification ranges of targets, and foot march factors.

Many slope calculators have been made by various terrain detachments. Calculators show different contour densities to be used on maps at these various scales with various contour intervals. They are usually reproduced on transparent plastic by photography laboratories.



To construct a slope calculator, you must know:

- The map scale, for example,1:100,000.
- The map contour interval, for example,10 meters.
- The percentage of slope you wish to calculate, for example, 20 percent.

To determine the amount of space between each line on your slope calculator, first determine the amount of ground distance by using the formula:

$$\frac{\text{Contour interval x 100}}{\text{\% slope}}$$

In our example, we get: $\frac{10 \times 100}{20} = \frac{1{,}000}{20} = 50$ meters

Next, convert the ground distance into map distance with the formula:

$$\frac{\text{Ground distance}}{\text{Map scale}}$$

In our example, we get: $\frac{50 \text{ meters}}{100{,}000} = 0.0005$ meters (or 0.5 mm)

This gives the amount of space between each line on the slope calculator. Use at least five lines. Place the slope calculator over the map section you are evaluating. If the contours on the map are more closely spaced than those on the calculator, the slope is greater than that depicted by the calculator. Conversely, if they are less closely spaced, the slope is less than that depicted on the calculator.

Figure G-1. Degree of slope calculator

Table G-1. Land widths shown on U.S. military maps

	Meters	***Feet***
Trail	Less than 1.5	Less than 5
Track	At least 1.5 but less than 2.5	At least 5 but less than 8
One lane	At least 2.5 but less than 5.5	At least 8 but less than 18
Two lanes	At least 5.5 but less than 8.2	At least 18 but less than 28
More than two lanes	At least 8.2	At least 28

Table G-2. Identification ranges

Targets	***Naked eye***	***Magnification 7.8 power***
Tank crewmembers, troops, machine gun, mortar, antitank gun, antitank missile launchers.	500 meters	2,000 meters
Tank, APC, truck (by model).	1,000 meters	4,000 meters
Tank, Howitzer, APC, truck.	1,500 meters	5,000 meters
Armored vehicle, wheeled vehicle.	2,000 meters	6,000 meters
APC—armored personnel carrier		

Table G-3. Route types and military load classifications

Route type	The route type is determined by its ability to withstand weather. It is determined by the worst section of road on the entire route and is categorized as follows:
Type X	An all-weather route that, with reasonable maintenance, is passable throughout the year to a volume of traffic never appreciable less than its maximum capacity. This type of route is normal, formed of roads having waterproof surfaces and being only slightly affected by rain, frost, thaw, or heat. This type of route is never closed because of weather effects other than snow or flood blockage.
Type Y	A limited, all-weather route that, with reasonable maintenance, is passable throughout the year, but at times having a volume of traffic considerably less than maximum capacity. This type of route is normally formed of roads that do not have waterproof surfaces and are considerably affected by rain, frost, thaw, or heat. This type of route is closed for short periods of time (up to one day at a time) by adverse weather conditions, during which heavy use of the road would probably lead to complete collapse.
Type Z	A fair-weather route passable only in fair weather. This type of route is so seriously affected by adverse weather conditions that it may remain closed for long periods of time. Improvement of such a route can only be achieved by construction or realignment.
Military load classification	A route's military load classification is a class number representing the safe load-carrying capacity and indicating the maximum vehicle class that can be accepted under normal conditions. Usually, the lowest bridge military load classification (regardless of the vehicle type or conditions of traffic flow) determines the route's military load classification. If there is not a bridge on the route, the worst section of road will determine the route's overall classification. The entire network's class is determined by the minimum load classification of a road or a bridge within the network. The broad categories are as follows:
Class 50	Average traffic route.
Class 80	Heavy traffic route.
Class 120	Very heavy traffic route.

Table G-4. Basic data foot march factors

	Visibility	***Rate of march* (km/h)***	***Normal march (8 hours) (km)***	***Forced march (12 hours) (km)***
Roads	Day	4	32	48
	Night	3	24	36
Cross-country	Day	2	16	24
	Night	1	8	12

*Computed on a 50-minute hour, allowing for a 10-minute halt each hour.

Length of a column. To determine the length of a column occupied by a dismounted unit, multiply the estimated or known number of personnel by the applicable factor.

Length of column, factor table, and foot marches

Formation*	**2 m/person distance**	**5 m/person distance**
Single file	2.4	5.4
Column of twos	1.2	2.7

*****Foot marches will vary with the tactical situation. Normal formation is a column of twos with a file on either side of the road and staggered, much like U.S. forces. However, columns of threes and fours may be employed where conditions permit.

Pass time. To determine the pass time in minutes for a dismounted unit, multiply the length of the column by the appropriate factor for the estimated or known rate of march.

Pass time factor, foot marches

Rate (km/h)	**Factors**
4	.015
3	.018
2	.020
1	.023

h—hour km—kilometer(s) m—meter

Glossary

AA	avenue of approach
ACE	analysis and control element
AGM	attack guidance matrix
AKO	Army Knowledge Online
AO	area of operations
AOI	area of interest
AR	Army regulation
ASCC	Army Service component command
ASCOPE	memory aid for civil considerations—areas, structures, capabilities, organizations, people, events
AUTL	Army Universal Task List
BCT	brigade combat team
BDA	battle damage assessment
BMCT	begin morning civil twilight
BMNT	begin morning nautical twilight
C2	command and control
CARVER	criticality, accessibility, recuperability, vulnerability, effect, recognizability
CARVERSHP	criticality, accessibility, recuperability, vulnerability, effect, recognizability, symbolism, historical, political
CBRN	chemical, biological, radiological, nuclear
CBRNE	chemical, biological, radiological, nuclear, high-yield explosives
CCIR	commander's critical information requirement
CENTRIXS	Combined Enterprise Regional Information Exchange System
CI	counterintelligence
COA	course of action
CONUS	continental United States
COP	common operational picture
CTC	combat training center
D3A	decide, detect, deliver, assess
DA	Department of the Army
DAIIS	Department of the Army Intelligence Information Service
DCGS-A	Distributed Common Ground System–Army
DIA	Defense Intelligence Agency
DLIFLC	Defense Language Institute Foreign Language Center
DOD	Department of Defense

DST	decision support template
DTG	date-time group
EECT	end evening civil twilight
EEFI	essential element of friendly information
EENT	end evening nautical twilight
EW	electronic warfare
F3EAD	find, fix, finish, exploit, analyze, disseminate
FAIO	field artillery intelligence officer
FFIR	friendly force information requirement
FM	field manual
FRAGO	fragmentary order
FSCOORD	fire support coordinator
G-1	assistant chief of staff, personnel
G-2	assistant chief of staff, intelligence
G-2X	human intelligence and counterintelligence staff officer (general staff)
G-3	assistant chief of staff, operations
GEOINT	geospatial intelligence
GMI	general military intelligence
GPS	Global Positioning System
HCT	HUMINT collection team
HPT	high-payoff target
HPTL	high-payoff target list
HUMINT	human intelligence
HVI	high-value individual
HVT	high-value target
HVTL	high-value target list
I&W	indications and warning
IED	improvised explosive device
IKN	Intelligence Knowledge Network
INSCOM	United States Army Intelligence and Security Command
INTSUM	intelligence summary
IO	information operations
IPB	intelligence preparation of the battlefield
IR	information requirement
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint force
JAAWIN	Joint Air Force and Army Weather Information Network
JP	joint publication
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communications System

LOC	line of communications
M3	Multimedia Message Manager
MCOO	modified combined obstacle overlay
MDMP	military decisionmaking process
MEA	munitions effects assessment
METL	mission-essential task list
METT-TC	memory aid for the mission variables—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MI	military intelligence
MIHB	military intelligence handbook
MP	military police
MTT	mobile training team
NAI	named area of interest
NCOES	noncommissioned officer education system
OEF	Operation ENDURING FREEDOM
OES	officer education system
OIF	Operation IRAQI FREEDOM
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSINT	open-source intelligence
PIR	priority intelligence requirement
POL	petroleum, oil, lubricants
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time
PSYOP	psychological operations
RDSP	rapid decisionmaking and synchronization process
RFI	request for information
RIP	relief in place
ROE	rules of engagement
S&TI	scientific and technical intelligence
S-1	personnel staff officer
S-2	intelligence staff officer
S-2X	human intelligence and counterintelligence staff officer
S-3	operations staff officer
SAF	small-arms fire
SCI	sensitive compartmented information
SEAD	suppression of enemy air defenses
SIGACT	significant activity
SIGINT	signals intelligence
SIPRNET	Secure Internet Protocol Router Network

SIR	specific information requirement
SOFA	status of forces agreement
SOP	standing operating procedure
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
STP	soldier training plan
SWO	staff weather officer
TA	target acquisition
TAI	target area of interest
TC	training circular
TECHINT	technical intelligence
TES	Tactical Exploitation System
TLE	target location error
TOA	transfer of authority
TRADOC	United States Army Training and Doctrine Command
TSS	target selection standards
TTP	tactics, techniques, and procedures
TVA	target value analysis
UAS	unmanned aircraft system
UMI	University of Military Intelligence
U.S.	United States
USAF	United States Air Force
USAICoE	United States Army Intelligence Center of Excellence

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

JOINT PUBLICATIONS

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001.

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

JP 3-0. *Joint Operations*. 17 September 2006.

ARMY PUBLICATIONS

FM 1-02. *Operational Terms and Graphics*. 21 September 2004.

FM 2-0. *Intelligence.* 17 May 2004.

FM 3-0. *Operations.* 27 February 2008.

RELATED PUBLICATIONS

These sources contain relevant supplemental information.

JOINT PUBLICATIONS

JP 3-09. *Joint Fire Support.* 13 November 2006.

JP 3-35. *Deployment and Redeployment Operations*. 7 May 2007.

JP 3-59. *Meteorological and Oceanic Operations*. 24 September 2008.

JP 3-60. *Joint Targeting*. 13 April 2007.

JP 4-0. *Joint Logistics.* 18 July 2008.

JP 5-0. *Joint Operation Planning*. 26 December 2006.

ARMY PUBLICATIONS

AR 190-13. *The Army Physical Security Program*. 30 September 1993.

AR 380-67. *The Department of the Army Personnel Security Program*. 9 September 1988.

AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009.

FM 2-19.4. *Brigade Combat Team Intelligence Operations*. 25 November 2008.

FM 2-22.2. *Counterintelligence*. 21 October 2009.

FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.

FM 2-91.6. *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection.* 10 October 2007.

FM 3-05.40. *Civil Affairs Operations*. 29 September 2006.

FM 3-06.11. *Combined Arms Operations in Urban Terrain*. 28 February 2002.

FM 3-90. *Tactics*. 4 July 2001.

FM 3-90.15. *Sensitive Site Operations*. 25 April 2007.

FM 4-0. *Sustainment*. 30 April 2009.

FM 4-01.011. *Unit Movement Operations*. 31 October 2002.

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. *U.S. Army Report and Message Formats*. 30 April 2007.

FM 7-15. *The Army Universal Task List*. 27 February 2009.

FMI 2-01. *Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization*. 11 November 2008.

FMI 2-01.301. *Specific Tactics, Techniques, and Procedures and Applications for Intelligence Preparation of the Battlefield*. 31 March 2009.

FMI 3-35. *Army Deployment and Redeployment*. 15 June 2007.

FMI 5-0.1. *The Operations Process*. March 2006.

TC 2-22.4. *Technical Intelligence*. 19 November 2009.

TC 2-33.4. *Intelligence Analysis.* 1 July 2009.

OTHER PUBLICATIONS

Lanicci, John M. "Integrating Weather Exploitation into Air and Space Power Doctrine." *Air Power* 12, No. 2. Summer 1998: 52–63.

Military Intelligence Handbook (MIHB) 2-50. *Intelligence Systems*. 22 July 2008.

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Forms are available on the Army Publishing Directorate web site (www.apd.army.mil).

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

DA Form 3964. *Classified Document Accountability Record*.

Index

This page intentionally left blank.

TC 2-50.5
6 January 2010

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
0935005

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Not to be distributed; electronic media only.

PIN: 086063-000