ST 2-50.4 (FM 34-8)

COMBAT COMMANDERS HANDBOOK ON INTELLIGENCE

US Army Intelligence Center and Fort Huachuca
Fort Huachuca, Arizona 85613-6000

SEPTEMBER 2001

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

PREFACE

Combat commanders need timely and accurate intelligence. In order to drive intelligence as a part of the intelligence operating system, commanders must understand what intelligence can do, how to focus it on specific requirements, and how you can integrate it with other operating systems.

This handbook addresses these requirements, expanding on the doctrine in FM 2-0 (FM 34-1), FM 3-0 (FM 100-5), FM 5-0 and FM 6-0 (FM 101-5), and FM 2-01.3 (FM 34-1 30).

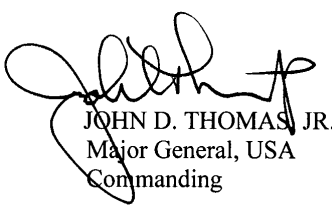
This handbook is written primarily for maneuver commanders and executive officers at brigade or regiment and battalion or squadron levels to include Active Components (AC) and Reserve Component (RC) commanders. It should also be useful to principal staff officers and combat support (CS) and combat service support (CSS) commanders.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men. Throughout the manual, “you” refers to the combat commander and also applies to the executive officer as he integrates and synchronizes the orders process and directs and supervises the staff.

The proponent of this publication is the US Army Intelligence Center and Fort Huachuca. We consider this a living manual and will dynamically revise this doctrine as frequently as necessary based on comments and suggestions from the field. Under normal circumstances appropriate revisions will be made within two weeks of receipt. While the initial (one time) distribution of this field manual will be made on CD-ROM, users should realize that to capture the dynamic changes/revisions of the manual as soon as they occur, they should check the Intelligence Center Homepage frequently for the most current version. We welcome your comments and recommended changes at any time. You may email them directly to the proponent at edd.goodmanc@hua.army.mil or mail them to: Commander, US Army Intelligence Center and Fort Huachuca (ATZS-FDRCD), Fort Huachuca, Arizona 85613-6000. You can also access the Doctrine Division Homepage at http://usaic.hua.army.mil/doctrine.htm and leave your comments or changes with the webmaster.

This handbook does not implement any international Standardization Agreements (STANAG5). It complies with all applicable STANAGs and Quadripartite Standardization Agreements. This document contains copyrighted material.

This manual incorporates the emerging intelligence and operational doctrine and terminology from FM 3-0, Operations, dated 14 June 2001. It uses the new manual numbers with the old manual numbers in parentheses. Although not all manuals have been updated to the new numbering system, this was done to transition the force to the new numbering system.



JOHN D. THOMAS, JR.
Major General, USA
Commanding

SPECIAL TEXT
No. 2-50.4 (FM 34-8)

USAIC&FH
Fort Huachuca, AZ 86513-6000
6 September 2001

TABLE OF CONTENTS

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

*FM 34-8, 28 September 1992, is rescinded. This Special Text reflects the latest doctrine on this subject approved by the Commanding General, United States Army Intelligence Center & Fort Huachuca.

Chapter 1

The Intelligence Challenge for Commanders

Intelligence is your tool; it is the foundation for synchronizing operations, massing combat power and effects, and protecting the force. There is no such thing as perfect intelligence but, when properly focused and planned and executed, intelligence operations are invaluable. To effectively use intelligence, you must understand—

- The capabilities and limitations of the intelligence operating system.
- The intelligence architecture (which includes command and control (C^2); processing; collaborative and distributed analysis; intelligence, surveillance, and reconnaissance [ISR] operations; and intelligence networks and communications).
- How you focus ISR operations.
- How you and your staff synchronize ISR with other operations.

INTELLIGENCE OPERATING SYSTEM

1-1. The mission of your intelligence operating system is to provide timely, relevant, accurate, and predictive intelligence support to you, your staff, and subordinates when planning, preparing, and executing decisive actions within the area of operations (AO). Implied within this mission, or associated with intelligence, are—

- Integrated ISR planning (focused through the S2 and S3 but thoroughly planned by the entire staff).
- Changes and adjustments to ISR collection.
- Analysis, production, and dissemination (to include presentation) of intelligence and combat information—the heart of the intelligence operating system.
- Electronic Warfare (EW), which is an integrated part of fires, targeting, and effects. EW should always be employed as an integrated and complementary capability.
- Counterintelligence (CI) is critical to your ability to protect the force in terms of supporting counterreconnaissance, analyzing the threat's multidiscipline ISR operations, and recommending countermeasures to those threat operations. There is a symbiotic relationship between counter-human intelligence (HUMINT) CI operations and human intelligence (HUMINT) collection. In the future, CI functionality will include analysis of threat information operations (IO) and other full-dimensional counter-ISR tasks.

ISR OPERATIONS

1-2. ISR planning and execution do not reflect a change to fundamental Army doctrine. Recent emphasis on ISR operations reflects the importance of a unified, integrated, and synchronized effort to—

- Plan and direct the ISR effort.
- Collect and process information.
- Produce intelligence.
- Disseminate intelligence and combat information to those who need it, when they need it.

1-3. Two concepts are imbedded in recent ISR doctrine:

- There are a finite number of "traditional intelligence collection" and "traditional reconnaissance and surveillance (R&S)" assets, but there are many potential ISR assets.
- There is a different "mindset" among each operating systems or proponent on how to plan, task, and control assets; how and where to report information; and how to use the information. However, ISR doctrine is designed to break the operating system or functional "stovepipes" for planning, reporting, processing, and analyzing information.

EMERGING DOCTRINE (IBCT)
(See Chapter 4)

In recognition of the importance of ISR operations and the unique challenges of small-scale contingencies, the initial brigade combat team (IBCT) is uniquely organized to facilitate ISR operations:

- The Military Intelligence (MI) Company (subordinate to the brigade) includes an ISR integration platoon, HUMINT platoon, more robust analytical capability, and organic control teams (specifically the operational management team [OMT] to help the commander control tactical HUMINT operations).
- The reconnaissance, surveillance, and target acquisition (RSTA) squadron S2 is supported by an ISR Integration Team (from the Surveillance Squadron).
- The surveillance troop (subordinate to the RSTA squadron) consists of soldiers and assets that execute nuclear, biological, and chemical (NBC) surveillance and other ISR operations (operations traditionally described as intelligence operations—from three disciplines). Another new characteristic is multi-sensor teams that employ sensors from more than one intelligence discipline.
- The reconnaissance troop (subordinate to the RSTA squadron) includes an organic HUMINT collection capability.

CRITICAL ELEMENTS OF ISR OPERATIONS

1-4. **Focus the ISR effort:**

- Clearly articulate your priority intelligence requirements (PIR) with a latest time intelligence is of value (LTIOV).

- Drive the IPB process throughout the military decision-making process (MDMP) (see Chapter 2).

1-5. **Carefully plan ISR operations.** You must ensure that intelligence preparation of the battlefield (IPB) drives the rest of the planning process and that all ISR operations are thoroughly planned (to include synchronized) and controlled as an integrated staff effort through the C^2 system. Although the G2 (S2) is the IPB and ISR integrator and the G3 (S3) plays a critical role in synchronizing ISR with the operation, every staff member plays an important role in both tasks. Your primary tool in accomplishing these integration tasks is the Chief of Staff (CofS) or executive officer (XO). The CofS (XO) is responsible to ensure all staff members participate in and provide their functional expertise into the IPB process and ISR planning and execution under the direction of the G2 (S2). There are a number of different techniques that the CofS (XO) can employ to facilitate interaction among the entire staff during the IPB process and ISR integration. However, the desired endstate is an efficient process that supports planning and helps facilitate the commander's visualization and understanding.

1-6. **Ensure ISR operations are continuous.** Your S2 (through the intelligence architecture) continuously performs intelligence tasks to meet your requirements before deploying and during operations. No echelon has enough time, ISR assets, and analytical tools to satisfy all of its requirements. Therefore, never keep your ISR assets in reserve.

1-7. **Use the C^2 system (as described in FM 5-0 and FM 6-0 (FM 101.5)).** Clear C^2 through centralized planning and decentralized execution is important. (This extends beyond collection management, as described in FM 2-33.4 (FM 34-2)). Command and support relationships for ISR units are developed by thorough staff planning (through mission, enemy, terrain and weather, troops, time available, and civilians [METT-TC] analysis). Use habitual relationships, when possible, to optimize effective operations as a combined arms team.

1-8. **Ensure ISR is a distributed operation.** Timely reporting to the right analytical element at the right echelon is critical to ISR operations. Intelligence Reach is a process by which deployed military forces rapidly access information from, receive support from, and conduct collaboration and information sharing with other units (deployed in theater and from outside the theater) unconstrained by geographic proximity, echelon, or command. G2s, S2s, and intelligence analytical elements (for example, the analysis and control element [ACE] and the analysis and control team [ACT] within the direct support [DS] MI company) utilize Intelligence Reach to collaborate, participate in distributed analysis, and share access to the intelligence between echelons and units. Every echelon must work together and tailor the intelligence architecture so that it is as close to seamless as possible—no barriers.

ISR TRAINING

1-9. **Integrate ISR training into garrison ("day-to-day") operations, exercises, and training events**. An increase in the importance of intelligence and the recent complexity of unique environments (urban operations and other complex terrain) and missions (stability operations and support operations) requires well-trained ISR commanders, leaders, soldiers, and organizations to produce superior results. You are responsible for training your portion of the intelligence operating system—the G2/S2. Your G2/S2 is

responsible for training his section and helping you train your unit on ISR issues. However, the G2/S2 (Senior Intelligence Officer) and intelligence commanders and leaders also train a significant portion of the intelligence operating system.

INTELLIGENCE TASKS

1-10. The intelligence battlefield operations system (BOS) is divided into the following four intelligence tasks. It is important that you understand the tasks that the S2 section performs during operations. Each task corresponds with a critical aspect of operations.

- **Facilitate commander's visualization and understanding of the threat and the environment.** This task provides information and intelligence to the commander to support his achievement of battlefield visualization. This task is comprised of three subtasks:

  — **Perform Intelligence Preparation of the Battlefield (IPB)** - IPB is the staff planning activity undertaken to understand the battlefield and the options it presents to friendly and threat forces. It is a systematic process of analyzing the threat and environment in a specific geographic area for a specific mission. By applying IPB, the commander gains the information necessary to selectively apply and maximize his combat power at critical points in time and space.

  — **Perform Indications and Warnings (I&W)** – I&W provide the commander with early warning and prevents surprise through anticipation of significant changes in threat activities. I&W provide the commander the ability to quickly reorient his forces on unexpected major contingencies and shape the battlefield.

  — **Perform Situation Development** – This subtask confirms or denies threat courses of action (COAs), explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness. Commanders use situation development to help understand the AO, thereby reducing risk and uncertainty. Situation development helps the commander make decisions and execute branches and sequels.

- **Counter the Threat** - This task provides the commander information and intelligence support for targeting of the threat's forces, threat organizations, units and systems through lethal and non-lethal fires to include electronic attack (EA) and information operations. It also includes the tactics, techniques, and procedures (TTPs) to deny or degrade the threat ISR capabilities to access and collect information and intelligence on friendly forces. This task is comprised of two subtasks:

  — **Support Targeting** - Targeting is supported by the staff to develop target systems, locate the targets, and perform battle damage assessment (BDA) on engaged targets. Included in this task is the use of EA against threat forces.

  — **Perform Counterintelligence** - CI is designed to defeat or degrade threat intelligence collection capabilities. The intelligence staff will provide CI to the commander outlining the capabilities and limitation of threat intelligence services and TTPs to limit or eliminate these capabilities.

- **Intelligence, Surveillance, and Reconnaissance Integration.** This task integrates ISR assets into an effort that produces intelligence, which leads to the commander's gaining situational understanding. These capabilities to collect, process, analyze and produce, and disseminate are critical to successful planning and conducting operations. Intelligence requirements are identified, prioritized, and validated; an ISR plan is developed and synchronized with the scheme of maneuver. This task is comprised of four subtasks:

  — **Develop Requirements** - Intelligence officers develop a prioritized list of what information needs to be collected and produced into intelligence. This list is placed against an LTIOV to ensure intelligence and information are reported to the unit in order for operations to proceed as planned.

  — **Analyze Requirements and Resources Available** - The entire staff under the direction of the intelligence staff analyzes each requirement to determine how best to satisfy it. The staff will receive orders and requests for information (RFIs) from both subordinate and adjacent units and higher headquarters. These requests are then balanced with resources available for tasking to ensure requirements can be met with available assets and their specific capabilities.

  — **Develop Specific Information Requirements (SIRs)** - SIRs break requirements into specific questions which, when answered, can satisfy the larger intelligence requirements. The requirements manager will develop sets of SIRs for each requirement with an LTIOV associated with each one.

  — **Develop ISR Plan.** The XO integrates and supervises the entire staff under the direction of the intelligence staff and develops an integrated and synchronized plan that places requirements to include time with recommended ISR assets. The ISR plan creates a collection strategy and employment scheme that will produce the intelligence required to effectively answer the commander's PIR.

- **Manage Intelligence Support to Information Operations** - Intelligence, both in offensive and defensive operations, provides the critical links for engagement with offensive IO. Intelligence also provides the capabilities and limitation of threat IO. This forms the basis of the defensive IO plan. Intelligence supports IO through its intelligence tasks and subtasks focusing on the target of IO.

EFFECTIVE INTELLIGENCE

1-11. The effectiveness of intelligence is measured against the following standards:

- **Timely:** Intelligence is useful only if you receive it soon enough to support planning, influence decisions, and prevent surprise.

- **Relevant:** Intelligence must answer your requirements and the requirements of your staff about the environment and threat in the format you designate. Your S2 must present you some basic products that help you visualize your battlespace (proportionate to his resources and the time available).

- **Accurate:** Intelligence must provide a balanced, complete, and objective picture of the threat and the operational environment. Alternative or contradictory assessments should be presented to ensure balance and bias-free intelligence.

When a certain degree of doubt exists, your S2 must capture and present that uncertainty.

- **Predictive**: Intelligence should advise you of present and future threat intent, objectives, capabilities, and COAs (with a description of supporting events by each threat operating system).

Chapter 2

Intelligence Preparation of the Battlefield

Longstreet looked up the long rise. He could begin to see it. When the troops came out of the woods the artillery would open up. Long-range artillery, percussion and solid shot, every gun on the hill. The guns to the right, on the Rocky Hill, would enfilade the line. The troops would be under fire with more than a mile to walk. And so they would go. A few hundred yards out, still in the open field, they would come within range of skirmish, aimed rifles. Losses would steadily increase. When they reached the road they would be slowed by the fence there, and the formation, if it still held would begin to come apart. Then they would be in range of the rifles on the crest. When they crossed the road, they would begin to take canister fire and thousands of balls of shrapnel wiping huge holes in the line. As they got close, there would be double canister. If they reached the wall without breaking, there would not be many left. It was a mathematical equation.

—Shaara, Michael. *Killer Angels.* New York, NY: Ballantine Books, 1974, p. 303.

RESPONSIBILITIES

2-1. The above passage details the vision General Longstreet had prior to the assault on Cemetery Ridge during the battle of Gettysburg. Because General Longstreet understood the critical elements of the terrain and the enemy, he was able to visualize this battle before it occurred. You rely on your S2 and staff to provide IPB analysis and graphic products that enable you to effectively visualize the battlefield and make decisions.

2-2. To visualize the battlefield, it is important that you and your XO take the lead to ensure that the IPB process is really an integrated staff effort (this is sometimes referred to as the cross-BOS IPB effort). Your S2 and staff must participate in initial IPB by—

- Analyzing the threat equivalent for their staff or functional area (red hat analysis). For example, the Engineer Officer will help analyze threat mobility, countermobility, and survivability capabilities.

- Helping the S2 capture any threat equivalent actions within the threat COAs for their staff or functional area (red hat actions) within standard or unique IPB products.

- Ensuring that their staff or functional area information requirements are answered or captured as an intelligence gap (in order to support planning and operations).

2-3. Although IPB is a G2/S2 responsibility, the entire staff contributes to the IPB process as shown in the Figure 2-1. However, Figure 2-2 shows the three most important MDMP steps for the commander to drive IPB.

FIRE SUPPORT OFFICER	**ENGINEER OFFICER**
▪ Provides templated locations for threat artillery and rocket systems. ▪ Provides the mission, task, and purpose of threat artillery and rocket systems. ▪ Assists the G2/S3 to accurately portray the threat's use of indirect fires, such as types and phases of threat fire.	▪ Provides templated locations for mobility, countermobility threat obstacles, and manmade obstacles. ▪ Provides information on the threat's preferred construct of survivability positions. ▪ Assists the G2/S2 to accurately portray the task and purpose of threat obstacles and threat mobility assets.
CHEMICAL OFFICER	AIR DEFENSE OFFICER
▪ Provides templated locations for NBC strikes. ▪ Provides information for manmade obstacles, such as NBC contaminated areas. ▪ Assists the G2/S2 to accurately portray the threat's use, intent, and purpose in the use of NBC units and capabilities.	▪ Provides templated locations for threat (air defense) assets. ▪ Provides assistance in identifying air corridors and avenues of approach (AAs). ▪ Provides assistance in identifying threat missions, tasks, and purpose of threat air defense artillery (ADA) and aerial assets. ▪ Assists the G2/S2 to accurately portray the threat's purpose and intent using ADA and aerial systems.

Figure 2-1. Example of staff IPB contributions to the G2/S2

COMMANDER'S INITIAL GUIDANCE - (STEP 1: RECEIPT OF MISSION)

2-4. In order to drive the IPB process, you must answer several questions:

- Do you disagree with or question any significant portions of the higher echelon's IPB products, analysis, facts, or assumptions? If so, you and your S2 must quickly resolve any issues to preclude problems between echelons.

- Does the staff need to focus on any particular part of the IPB process?

MDMP Steps	Commander's Output	The Commander Drive IPB
Step 1: Receipt of Mission	Initial Guidance	Disagree with higher IPB? Abbreviated initial IPB? Initial ISR support? Additional IPB analysis (besides normal procedures)?
Step 2: Mission Analysis	Restarted Mission. Commander's Intent. Commander's Guidance.	Area of interest (AOI). Significant characteristics of the environment. Important environment factors. Choose threat models and identify any refinements. How many threat COAs and their specifics? Initial threat culmination criteria.
Step 6: COA Approval	Approved COA. Refined Commander's Intent. Specified Type of Order. Specified Type of Rehearsal. HPTL.	Final threat culmination criteria. Guidance on refining IPB analysis and products.

- Are there any immediate ISR requirements that need to be addressed early?

Figure 2-2. Driving IPB

COMMANDER'S INTENT AND GUIDANCE - (STEP 2: MISSION ANALYSIS)

2-5. You must allocate adequate time and guidance to your S2 and staff to perform the initial IPB. Successful mission analysis requires a thorough initial IPB to provide the staff with the impact of the environment, weather, and threat for use in subsequent steps of mission analysis.

2-6. In this step the staff starts to convert your visualization of the battlefield into an operational framework. Focus the efforts of your S2 and staff on IPB.

- **Define the Battlefield Environment.** Provide guidance on the AO, AOI, and the significant characteristics of the environment. For example, during a friendly offensive operation, characteristics such as location and activities of threat reserves, reinforcements, and fire support assets are typically significant. During a humanitarian assistance operation, however, the location and activities of civilian relief organizations may be a significant characteristic. Articulate your view so your staff can build the correct framework for the rest of the IPB process.

Why is this important? Failure to focus on only the relevant significant characteristics wastes time and the IPB process will not influence mission success. On the other hand, failure to identify all the significant characteristics may result in your unit's failure to deal with a feature of the battlefield that you and your staff overlooked.

- **Describe the Battlefield Effects.** The S2 and staff use the factors defined in Step 1 and other characteristics to evaluate the battlefield thoroughly and to describe the

  battlefield effects. In stability operations and support operations, you and your battlestaff must view terrain in a unique way and keep in mind the political, economic, ethnic, and other characteristics of the population (the key terrain).

Why is this important? Commanders with a poor understanding of the battlefield effects will probably fail to exploit the opportunities the environment provides, and the threat will find and exploit opportunities in a way the command did not anticipate.

- **Evaluate the Threat.** Most of the analytical work for this step is performed prior to deployment; it is a part of intelligence readiness activities and contingency planning. It is at this point that your S2 and staff clearly define who the threat is and what the threat looks like. In stability operations and support operations the threat could range from conventional military forces to paramilitary forces, insurgents, terrorists, political groups, refugees, or environmental disasters. Understanding the threat's intent provides focus to the S2 so that as he moves to step 4, the threat COAs make sense.

  Why is this important? Failure to evaluate the threat adequately may result in—

  — A lack of intelligence, which is needed for planning.

  — Wasted time and effort in planning against threat capabilities that do not exist.

  — Surprise because of an unknown threat capability.

- **Determine Threat COAs.** Dictate how many and to what level of detail you want the S2 and staff to develop threat COAs, then provide macro-level guidance on how you visualize your intent in relationship to threat objectives and endstate. Finally, provide the S2 and staff guidance on criteria that will lead to culmination of the threat. For example, you could intend to defeat the threat by destroying 75 percent of his organic and attached artillery and 50 percent of the lead motorized rifle battalions (MRBs).

Why is this important? Failure to adequately determine threat COAs will allow the threat to surprise you and your staff. Viable and tactically sound threat COAs provides the framework required to build a successful friendly COA.

2-7. After the mission analysis briefing you approve a restated mission (which becomes the unit's mission) and the initial PIR. (The integrated ISR plan comes from these initial requirements.) Your S2 and staff will continue to refine the PIR (with your approval)

throughout the MDMP. You can also modify your intent (this provides the link between the mission and the concept of operations). Your last responsibility is to provide your staff with enough additional guidance to focus staff activities during the remainder of planning.

COMMANDER'S DECISION BRIEFING - (STEP 6: COA APPROVAL)

2-8. After the decision briefing, you approve the COA you believe to be the most advantageous; you then modify your intent statement and your commander's critical information requirements (CCIR) to support this selected COA and issue further guidance:

- State the final threat culmination criteria.
- Direct refinements for the IPB analysis and products to include greater detail on threat branches and sequels.

WHAT YOU SHOULD EXPECT

2-9. Your S2 and staff must complete IPB early in the MDMP because this process lays the groundwork for COA development and the subsequent steps of the MDMP. IPB analysis and products must help you and your staff do the following:

- Visualize the battlefield.
- Complete COA development, the wargame process, and COA refinement (to include building flexibility into the operation).
- Plan ISR operations.
- Provide the framework so your S2 can perform situation development and your XO/S3 can provide the common operational picture during the operation.

2-10. To meet these requirements, your S2 and staff perform IPB analysis and produce graphic products that—

- Describe the threat's mission, intent (two levels up), and how they see us.
- Portray an adaptive, cunning, and uncooperative threat. Provide a detailed picture of how the threat will operate with all of his combat multipliers (not just a template of how and where he will move).
- Include the task and purpose of all relevant threat ISR systems.
- Supply the level of detail appropriate for the audience in a user-friendly manner.

2-11. The lessons learned discussed herein are from the National Training Center but apply to any brigade or regiment and battalion or squadron level S2.

2-12. During mission analysis, expect your S2 and staff to "paint a picture" you can remember. Require your S2 to begin with the bottom line up front. They should produce the following during mission analysis and present it during the mission analysis brief.

- Battlefield environment visualization analysis and products to include terrain and current weather and weather effect charts.
- Threat organization and timelines: macro to micro. Develop the threat picture from the largest echelon given all the way down to individual vehicle, time permitting. The timelines should also reflect from largest echelon to smallest element.
- Threat commander's intent (two levels up in terms of strategic and tactical missions).
- Threat COA sketches (macro-level).
- Threat COA snapshots. This includes sketches and overlays consisting of the task and purpose of all relevant threat intelligence operating systems (for example, detailed situation templates).

BATTLEFIELD ENVIRONMENT VISUALIZATION ANALYSIS AND PRODUCTS

Terrain

2-13. Expect your staff (led by the S2 and supported by the Engineer Officer) to clearly illustrate how terrain will affect the movement of friendly and threat forces.

- Include the entire AOI.
- Demonstrate the terrain's effects (line of sight, covered and concealed mobility corridors) on combat, CS, and CSS operations.
- Emphasize the significance of key and decisive terrain.

2-14. When possible, your S2 and staff should use and brief from 1:12,500 or 1:25,000 scale maps or photographs to supplement standard 1:50,000 scale maps—a higher resolution map provides a better depiction of the terrain. The divisional terrain team is the primary source of terrain data. Some other products available include digital terrain elevation data (DTED), Arc Digitized Raster Graphics (ADRG), satellite imagery, and the Urban Tactical Planner (UTP) (see FM 5-33).

2-15. In stability operations and support operations, your S2 and staff must analyze and describe those population characteristics that are important to your mission (for example, knowing the routes that are off limits to US forces but available for the threat to accomplish house bombings and theft of building supply materials).

Weather

2-16. Expect your S2 to communicate how weather affects operations in the initial IPB analysis and products. An example of an important impact of weather is the increased effectiveness of obscuration during an operation because of a low wind speed and temperature inversion.

2-17. Weather may have a unique impact on stability operations and support operations in both threat and friendly operational patterns. For example, weather could—

- Cause the threat to cancel demonstrations or rallies during inclement weather.
- Affect friendly psychological operations (PSYOP) because rain and heavy winds disrupt leaflet drops.
- Impact civil affairs (CA) operations; heavy rain could disrupt construction projects or a medical and veterinary assistance program.

THE THREAT

2-18. The S2 should remember that the threat will be capable of adaptive operations, asymmetric methods of attack, hiding their operational patterns from friendly forces, and conducting atypical operations. An asymmetric approach is the employment of non-conventional forces, means, or technology (such as weapons of mass destruction [WMD], small-scale chemical attacks or computer network attacks) to offset the advantage of a superior military force. One possible threat COA would be to apply an asymmetrical method and attack US Forces at a critical point when we are vulnerable in order to prevent us from synchronizing our operations. For example, a terrorist attack on the infrastructure of a port of debarkation just as US Forces start to deploy could have a devastating impact.

2-19. Within the current operational environment, friendly forces face the probability of deploying with few or no threat models (that consist of doctrinal templates with a description of tactics and options and type high-value target [HVTs]). During staff operations the CofS (XO) ensures all staff members participate in and provide their functional expertise into the IPB process and ISR planning and execution under the direction of the G2 (S2). In many operations, your staff will have to perform detailed analysis over a period of time in order to determine threat patterns and develop threat models. However, the staff must develop a modified combined obstacle overlay (MCOO), multiple situation and event templates, and other IPB products. In order to support planning, the staff adapts these products based on the particular operation. The staff must develop these products in spite of the difficulty of developing threat models and predicting threat actions for an adaptive adversary.

2-20. One technique to deal with the uncertainty of making predictions without a threat template for an adaptive adversary is to develop more tailored threat models and templates for specific types of smaller scale activities than the staff produces for conventional offensive operations. While some of the models and templates will contain less level of detail, these products can cover more “worst case” and “most likely” threat operational patterns and COAs. Like most staff planning processes, IPB only reflects the staff’s best assessment. In these circumstances operational planners may use techniques to accept less or mitigate risk in the conduct of operations (for example, developing more branches and sequels). Even after the intelligence staff identifies threat patterns and develops threat models, analysts must remain vigilant and try to predict those operational changes an adaptive threat is most likely to adopt. The IPB discussion within most of the rest of this chapter is based on Krasnovian Opposing Forces (the Army’s standard training and simulations tool) and the use of threat models and the other mandatory IPB.

Threat Organization And Timelines: Macro to Micro

2-21. Expect the S2 to describe those forces the threat will use, or potentially use, in the conduct of his operations. An order of battle (OB) chart, as shown in Figure 2-3, is a good tool. The chart should include the unit designation, if known, the type of unit such as a tank regiment, and the equipment by nomenclature and number within the unit (for example, 104 x T-72's; 33 x BMP-3's), and unit subordination.

2-22. Some threats could use indirect, often subtle methods to attack US Forces. The assumption that the adversary will “fight fair,” consider delivery methods or collateral damage, or comply with the current “laws of warfare” is not necessarily true.

2-23. Your S2 can also produce a graphic timeline, as depicted in Figure 2-4, to assist in developing your own COAs and associated decisions. The threat COA matrix in Figure 2-5 shows a comprehensive breakdown of several different threat COAs.

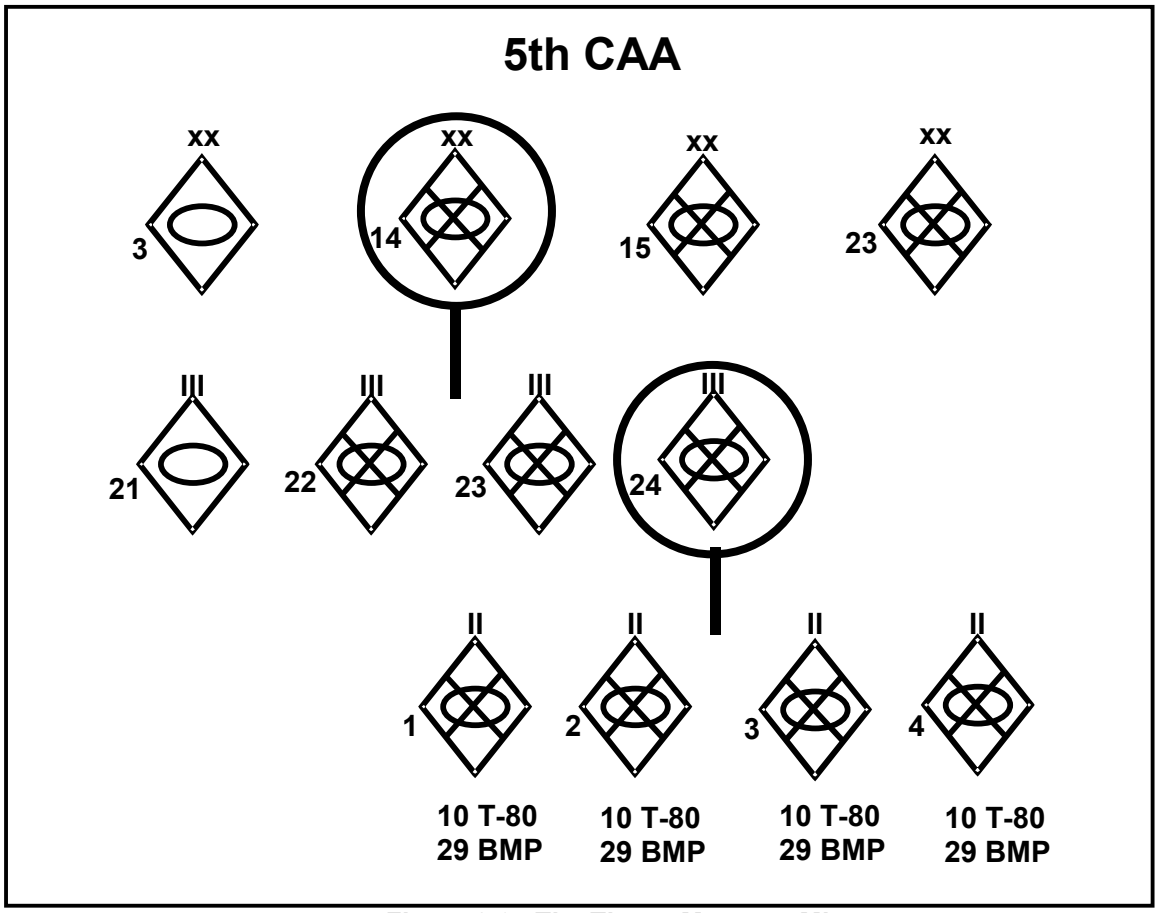


Figure 2-3. The Threat-Macro to Micro

2-24. The threat COA matrix works equally well in stability operations and support operations. The threat COA may include demonstrations causing US casualties, interrupting relocation efforts, or disrupting elections. The rest of the matrix should reflect friendly actions to counter threat actions.

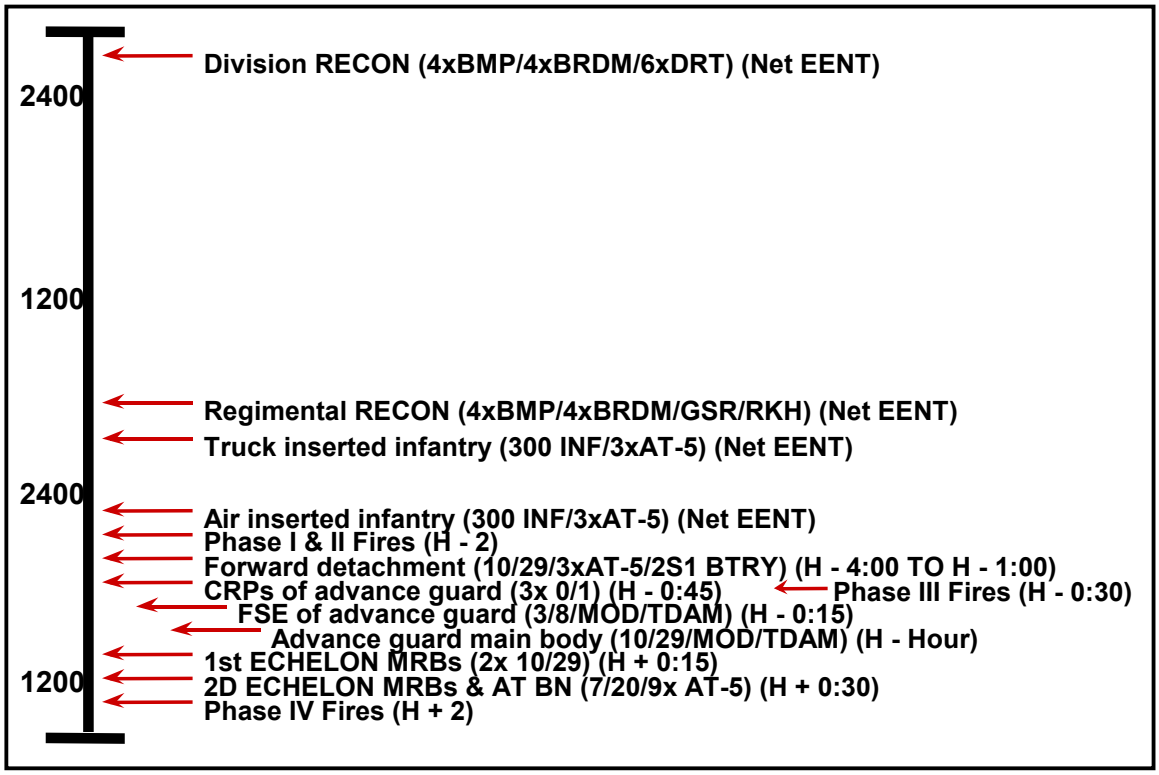


Figure 2-4. Threat timeline

	Threat COA 1 (Brown Pass)	Threat COA 2 (Debnam Pass)	Threat COA 3 (South Wall)
TF Destroyer	Truck insert and infiltrate to goat trail to attrit CO/TM	Truck insert and infiltrate to Debnam Pass to breach and facilitate movement of the regiment main body	Truck insert and infiltrate to secure Hill 899 to facilitate the movement of the AGMB
TF Angel	Air insert and infiltrate through Bruno Escarpment to attrit northern CO/TM	Air insert vic Matterhorn and infiltrate to attrit CO/TM	Air insert vic Matterhorn and infiltrate to prevent repositioning
FD	Atk to secure Brown Pass to open point of penetration	Atk to Brigade Hill to facilitate movement of regiment main body	FD: Atk to fix two CO/TMs of northern TF
Special Munitions	Prevent forces from repositioning north out of Colorado/Washboard	Prevent forces repositioning out of Colorado/Washboard and protect the north flank of the regiment	Protect the north flank of the regiment
FSE of AG	Atk to secure Brown cut or reinforce FD	Atk to secure Debnam Pass to facilitate movement of the regiment main body	Atk to Brigade Hill to facilitate movement of regiment main body
AGMB	Atk to secure Crash Hill to protect the south flank of the regiment	Atk to secure Debnam Pass to facilitate movement of the regiment main body	Atk to Hill 899 to facilitate movement of regiment main body
1st Echelon North	Atk to seize the regiment subsequent objective	Atk to secure Crash Hill to protect the north flank of the regiment	Atk to secure firing lines to protect the north flank of the regiment
1st Echelon South	Atk to seize the regimental subsequent objective; O/O protect the south flank of the regiment	Atk to secure firing lines vic Matterhorn to protect the south flank of the regiment	Atk to secure the regimental subsequent objective
AT Bn	Protect the south flank of the regiment	Protect the south flank of the regiment	Protect the north flank of the regiment
2d Echelon	Follow and assume main effort	Follow and assume main effort	Follow and assume main effort

Figure 2-5. Threat COA matrix

Threat Commander's Intent

2-25. Expect your S2 to clearly articulate how the threat perceives our operations and the threat commander's intent (from one echelon down to two echelons up). The threat commander's intent should be loosely based off your intent. The threat's perception of us and the threat intent drives how the S2 develops each threat COA (by identifying logical options).

2-26. Your S2 should develop the threat intent and the initial threat COA from macro to micro resolution. Many threats use some form of doctrine to conduct operations (for example, fixing a part of a defensive position, while suppressing, and flanking another part of the same position).

Threat COA Sketches (Macro-Level)

2-27. Expect your S2 to use cartoon sketches to show all feasible threat COAs. These sketches should show the threat mission statement and how the threat will fight. You

should address all the sketches to better prepare you to deal with a thinking and adaptive threat.

2-28. Although the S2 can develop a full set (five or more) of broad sketches, he rarely has the time to develop that many detailed threat COAs (for example, detailed situation templates). Your S2 should provide you with two or three detailed threat COAs and two or three broad threat COAs. The total package helps build more flexibility into the plan. At a minimum, the detailed threat COAs must include the most dangerous and most likely threat COAs. Remember, the most likely and most dangerous threat COAs can change based on your actions or COA and how much information the threat collects about you.

Example for Most Probable Threat COA

During mission analysis the S2 decides the threat's most probable COA is to attack into the northern part of the friendly sector. The IPB process drives a friendly COA to defend with a heavily weighted effort in the north. Successful threat reconnaissance reports that the bulk of the engineer effort, especially obstacle work, is occurring in the north.
The threat may have initially planned to attack north but decided against it once his reconnaissance confirmed your strength. Expect your S2 to consider and articulate this type of possibility when briefing.

2-29. Figures 2-6 through 2-9 show a method of using a combination of text and graphics to communicate several feasible threat COAs quickly and clearly.

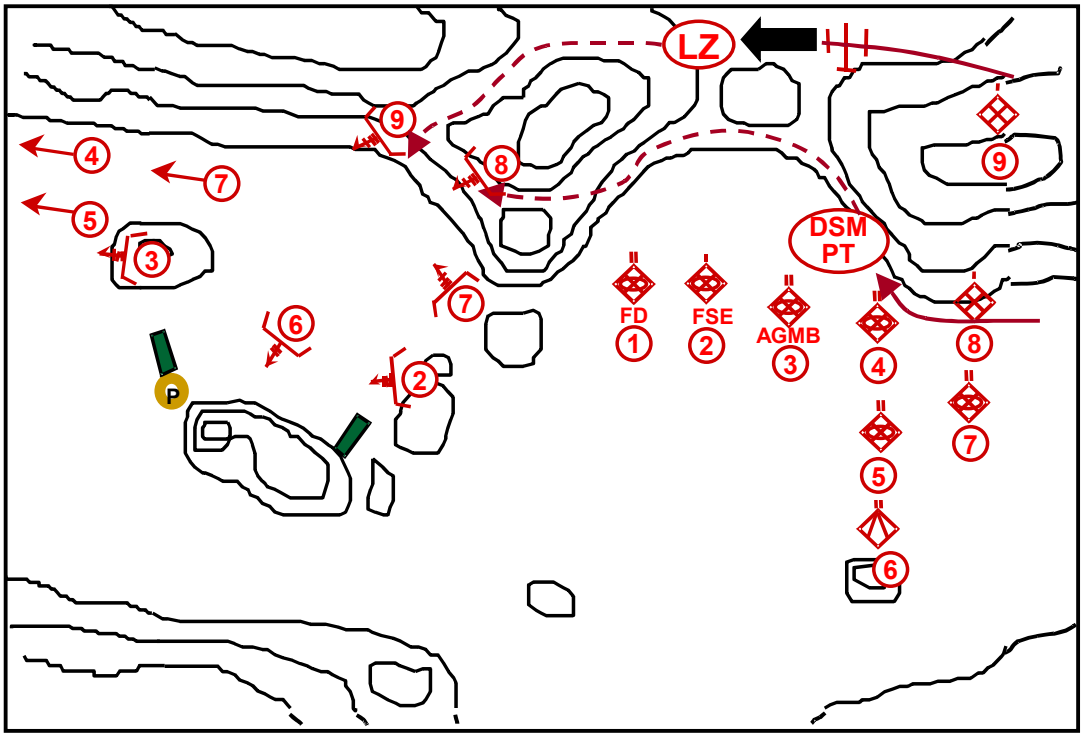


Figure 2-6. Brown Pass (Threat)

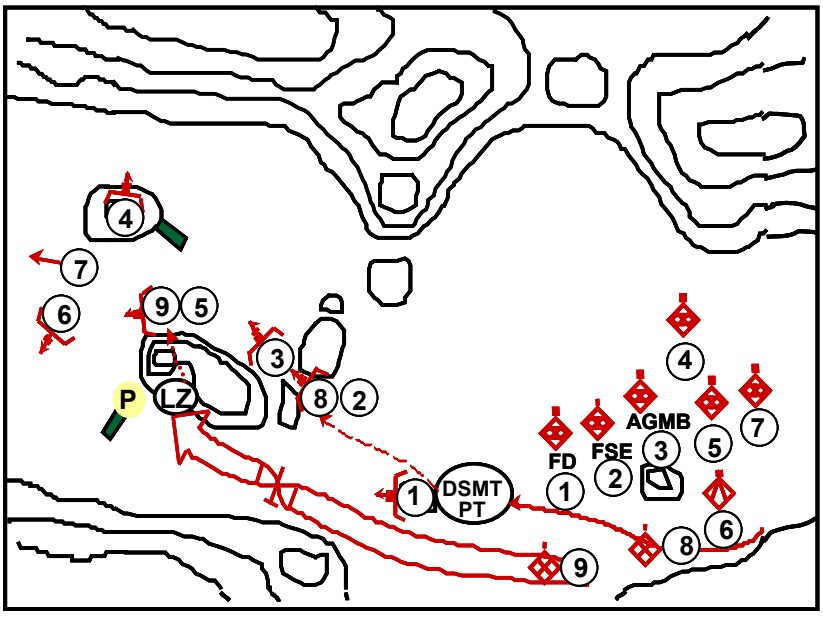


Figure 2-7. Debnam Pass (Threat COA 2)

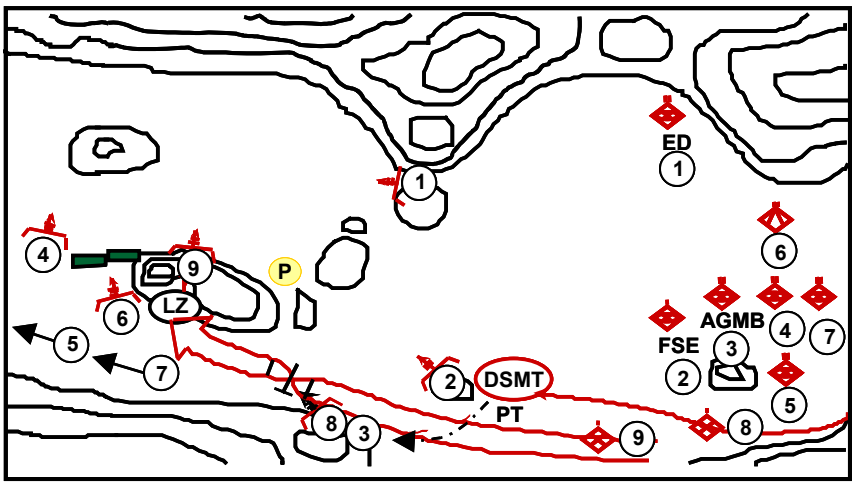


Figure 2-8. Southwall (Threat COA 3)

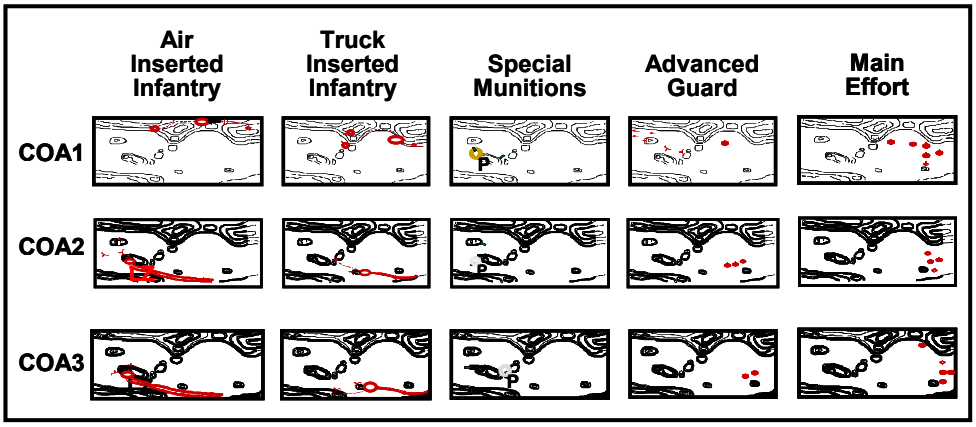


Figure 2-9. The Storyboard

2-30. Figure 2-9 is a storyboard that shows broad threat COAs during a motorized rifle regiment (MRR) attack. Similar map sketches showing the necessary terrain are pasted in each square. Threat critical events are labeled across the top of the chart and each box provides a space for your S2 to sketch out different threat options. Each sketch should include composition, task, and purpose.

2-31. In a stability operation or support operation, intelligence may reveal that the intent of the threat is to force the US military to leave. Based on this intent, the S2 develops a threat COA for inflicting US casualties. The S2 expects the attack will come from a paramilitary organization and describes the threat COA using a sketch (see Figure 2-10).

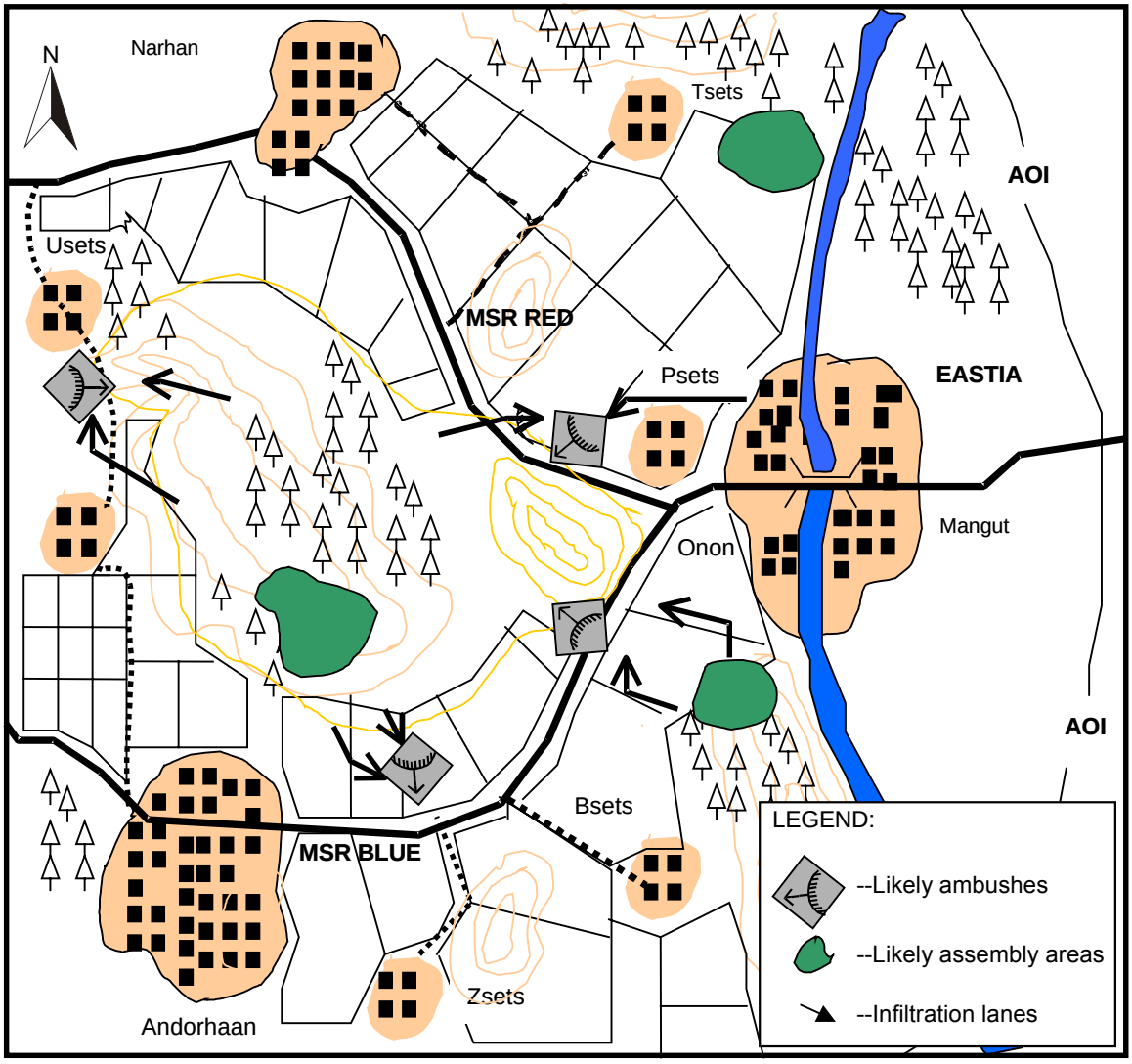


Figure 2-10. Threat COA

2-32. Every option should indicate something critical (an indicator) to the threat's plan. Once the threat starts their operation your S2 can quickly confirm and/or deny threat COAs.

Threat COA Snapshots

2-33. Without an accurate depiction of how and when threat forces will deploy, it is difficult to adequately plan operations (in accordance with your intent). If possible, your S2 should develop threat models before deployment. If your S2 "front loads" this work, he can easily build a detailed situation template.

2-34. It is also important that your XO takes the lead and ensures that the IPB process is really an integrated staff effort. Every staff or functional area representative should fully participate in each step of IPB (this is sometimes referred to as the cross-BOS IPB effort). The bottom line of this participation is "red hat" analysis of their staff or functional equivalent and integrating the results into existing or additional IPB products. For example, the brigade fire support coordinator (FSCOORD) should help the S2 template threat artillery, identify the threat's high-payoff targets (HPTs) (friendly assets whose destruction is critical to support the threat mission), and timeline important phases of fire. This type of staff interaction is critical to the quality of the IPB process and products and to meet the short timelines for initial IPB.

2-35. Expect your S2 and staff to provide you with the threat's method of employment to include dispositions, main effort, scheme of maneuver, and his use of a full range of combat multipliers. An effective way to do this is to create predictive snapshots of the threat at critical places and times. Figures 2-11 through 2-13 illustrate a technique to display the critical events of an MRR attack. Figure 2-14 shows these figures in a consolidated format.

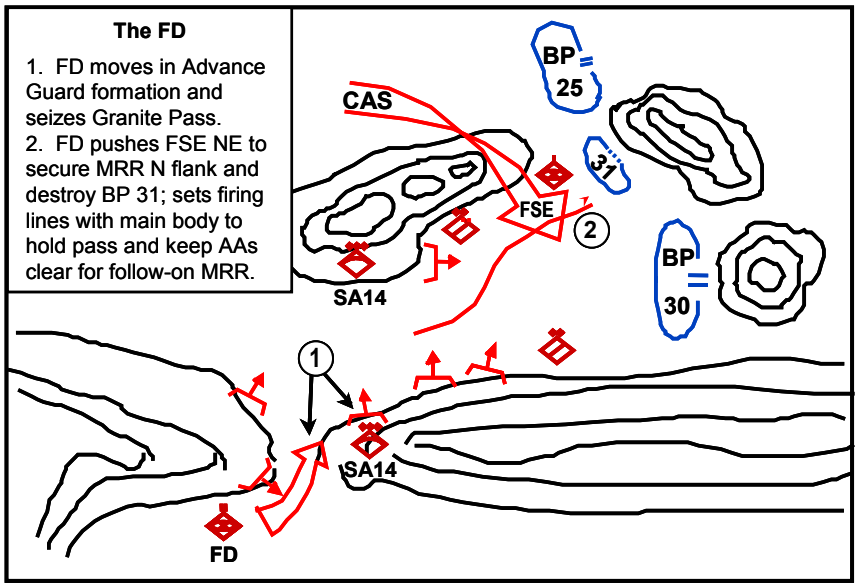


Figure 2-11. Snapshot Sketch #1

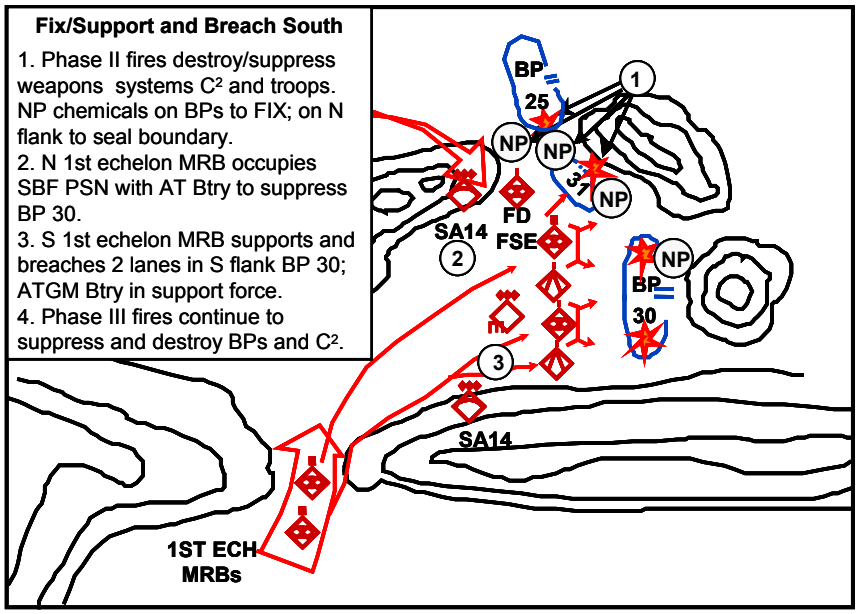


Figure 2-12. Snapshot Sketch #2

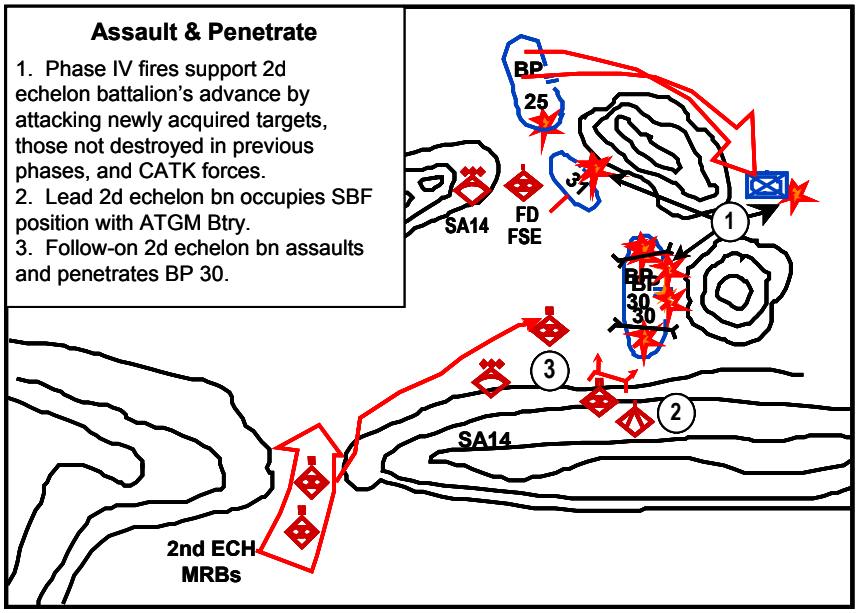


Figure 2-13. Snapshot Sketch #3

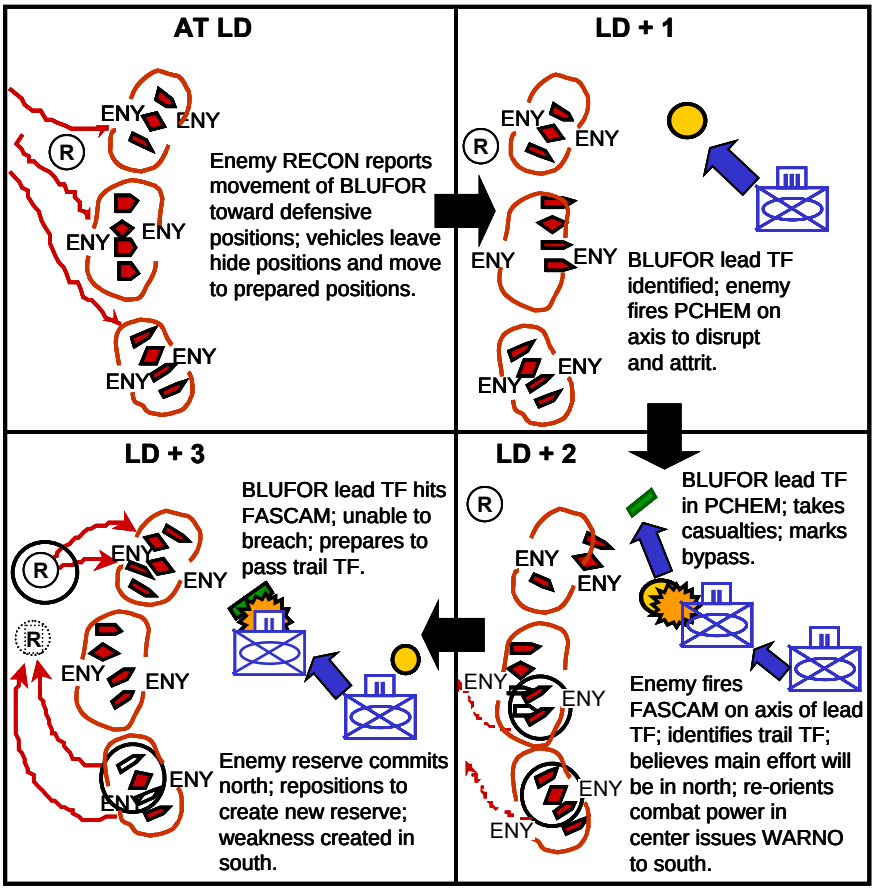


Figure 2-14. Threat COA sketch

FRIENDLY VULNERABILITES

2-36. Your S2 is responsible to provide a detailed description of how the threat can exploit any friendly vulnerabilities. There are three questions that your S2 uses to predict how the threat will try to exploit friendly vulnerabilities.

- Where are we vulnerable? The S2 must determine where (for example, critical systems or world opinion) the threat believes we are vulnerable and also looks at where you and your staff assess you are vulnerable.

- What will they attack? The S2 then looks at the friendly plan and threat capabilities and COAs to determine what the threat commander will most likely attack. This analysis supports the determination of essential elements of friendly information (EEFI) and friendly operations security (OPSEC) measures. Additionally, at higher echelons this helps drive CI analysis.

- When and how? By analyzing what the threat will attack, the S2 then uses threat doctrine or a reasonable prediction of likely actions to answer how and when the threat will attack.

Chapter 3

S2/G2 Organizations and Functions

THE BATTALION S2

3-1. Your battalion S2 section is austere. Even when fully staffed, your S2 section is not resourced to conduct sustained operations at both the tactical operations center (TOC) and tactical command post (TAC). Battalion S2 operations usually provide few detailed products because of the lack of time and resources.

OPERATIONS

3-2. Every member of the S2 section should be able to perform any of the intelligence functions. Your S2's priorities are to—

- Perform mature IPB (for more information, see Chapter 2).
- Plan, task (through your S3), and control ISR operations as part of an integrated effort by your staff. You must protect your scant resources and focus on your PIR.

3-3. The S2 must carefully drive planning that leads to the scout platoon mission. The fragmentary order (FRAGO) that the scout platoon uses to begin its mission must include precise guidance on the infiltration method, collection tasks, reporting criteria and timelines, fire support, casualty evacuation plan, and many other aspects of the mission. The S2 should also debrief scouts and patrols, when time permits, to obtain all relevant information. The S2 should also—

- Task frontline troops and combat patrols for collection.
- Perform a very basic level of situation development to advise you on threat actions, capabilities, and vulnerabilities.

3-4. Reports from scout platoons and every company or company team vary in accuracy. The S2 must conduct analysis to integrate all the information from many means (for example, the scouts, fire support net, and command net) to provide you timely, relevant, accurate, and predictive intelligence as you execute the operation.

STAFF INTERACTION

3-5. Although the XO is responsible for integrating and synchronizing operations plans (OPLANs) and operations orders (OPORDs); directing and supervising the staff's planning process; and ensuring all staff members provide IPB input to the S2/G2, your XO, S2, S3, Fire Support Officer (FSO), and Engineer Officer should work closely in planning and synchronizing battalion operations. Through the XO, train your S2 on the products you expect him to produce and your standards. You and your XO must also train your staff on intelligence capabilities, limitations, and operations.

PRODUCTS

3-6. Your S2 does not have the time nor the resources to develop many detailed IPB products. Once you and your S2 accept the brigade IPB results, the S2 section starts to develop those products to the level of detail needed to support battalion operations.

3-7. Your S2 should always produce (and modify when necessary) the following:

- A set of detailed situation templates or other threat model for at least two threat COAs (most dangerous and most likely).
- An event template.
- An integrated ISR plan to answer your PIR in a timely manner.
- The intelligence portion of the decision support template (DST).

MI SUPPORT AND ATTACHMENTS

3-8. Except for ground surveillance radar (GSR) and the Remotely Monitored Battlefield Sensor System (REMBASS), you will probably not have MI assets attached to your unit. Ensure your staff fully integrates any MI assets you receive into the ISR plan. However, you can expect additional MI support and assets operating in your AO during stability operations and support operations (particularly tactical HUMINT teams).

THE BRIGADE S2

3-9. The S2 section is much larger at the brigade level than at the battalion. However, light brigades will have fewer personnel than heavy brigades.

OPERATIONS

3-10. IPB is a more systematic process at brigade level than at battalion level. A significant amount of training is necessary at the brigade level to bring the section together as a team. Your S2 will have to conduct a more thorough and comprehensive IPB and situation development (this includes accepting risks with the predictive nature of IPB). These tasks require a confident, experienced tactical MI officer who understands friendly operations and the threat.

3-11. If you do not have organic scout assets (like the brigade reconnaissance troop), you will have to either use subordinate unit soldiers and equipment to perform that function or rely on subordinate battalions and the division to provide you information and intelligence. When scouts are organic to the brigade, the brigade S2 should drive the planning just like the battalion S2.

STAFF INTERACTION

3-12. Although the XO is responsible for integrating and synchronizing OPLANs and OPORDs; directing and supervising the staff's planning process; and ensuring all staff members provide IPB input to the S2/G2, your XO, S2, S3, FSO, and Engineer Officer should work closely in planning and synchronizing brigade operations. Due to the size of the brigade staff, it is not as easy for you, the XO, and the S2 to educate the entire staff on intelligence operations. An aggressive series of officer and noncommissioned officer (NCO) professional development classes can help train your staff on intelligence. The S2 section must carefully disseminate intelligence to many users to include using short but

effective briefings. Through the XO, train your S2 on the products you expect him to produce and your standards. You and your XO must also train your staff on intelligence capabilities, limitations, and operations.

3-13. As a rule, the S2 sends an assistant S2 with an analyst to the brigade TAC to perform limited analysis and advise the commander and any staff (when they are present). For detailed analysis the TAC must depend on the TOC.

PRODUCTS

3-14. Your brigade S2 develops more products (representing a larger area and some with more detail) than the battalion S2. When your brigade S2 completes his products and forwards them to the battalion S2, he should expect to explain the results, answer questions on his analysis and products, and change any products as appropriate. Your S2 should always produce (and modify when necessary) the following:

- Basic products to describe the battlefield's effects to include weather and terrain. In stability operations and support operations, the S2 must produce more complex products that graphically depict key characteristics of the local population.
- A set of detailed situation templates or other threat models for at least three threat COAs (to include the most dangerous and most likely).
- An event template, the intelligence estimate, and an integrated ISR plan (with a supporting ISR matrix) to answer your PIR in a timely manner.
- The intelligence portions of the DST and operating system synchronization matrix (for example, PIR, named areas of interest [NAIs], and R&S collection).
- A separate ISR synchronization matrix that ties the integrated ISR plan with the operating system matrix.
- Appendix B, Intelligence to the OPORD (a good matrix appendix is acceptable).

TYPICAL MI SUPPORT TO A BRIGADE

3-15. Your brigade is normally supported by a direct support (DS) MI company with a habitual relationship to your brigade (see Chapter 4). The DS MI Company provides several significant capabilities:

- A commander to help the S2 plan.
- C^2 for all MI assets (to include any other assets or units attached or supporting the brigade). The MI company command post serves as the control mechanism for all MI assets. Any additional control teams that support the brigade (for example, a tactical HUMINT control team during some types of operations) collocate and operate with the analysis and control team (ACT).
- Analytical support to the S2 and processing and fusion systems.
- Organic intelligence collection systems.

THE DIVISION AND CORPS G2

3-16. The G2 sections at division and corps are significantly larger staff organizations than the brigade S2 section. For example, the G2 section functionality normally includes

a Deputy G2, Operations, Plans, Training, special security officer (SSO), CI, terrain team, and the ACE, and is supported by the staff weather officer (SWO).

OPERATIONS

3-17. The G2 operations officer directs and coordinates intelligence, the division SSO, the staff weather team, and the terrain team based on G2 guidance. He is responsible for proper integration and dissemination of all intelligence and combat information that the ACE and subordinate S2s report. He combines that intelligence and combat information and presents the current intelligence (the threat portion of the common operational picture) to the commander and staff. This helps the division commander visualize his battlespace, by graphically and effectively depicting the environment, and depict current threat actions and predicted threat capabilities, intentions, and COAs.

ANALYSIS AND CONTROL ELEMENT (OPCON)

3-18. The ACE is the focal point for all division ISR operations (to include planning, processing, producing, and dissemination). It consists of a single-source analysis section, an all-source analysis section, a collection management team, and a targeting team. The ACE is under operational control (OPCON) to the G2 (from the MI battalion). ACE personnel perform all of the tactical intelligence tasks (see Chapter 1) in support of division operations. The ACE fuses information from all ISR assets and units into intelligence products and the all-source correlated database. The ACE also provides an accurate, relevant picture of the battlefield to the G2 operations section. The G2, terrain team, SWO, and ACE work together to develop, present, and distribute IPB products across the division.

PLANS

3-19. The G2 plans is responsible for all products required for mission analysis and wargaming. (He is supported by the all-source production section of the ACE.) The G2 plans drives the MDMP because he understands and describes the environment and the threat. During mission analysis, the planner also relies on the electronic warfare officer (EWO), SWO, and terrain team for products and integrates the products into the wargame and targeting sessions.

TRAINING

3-20. The G2 training office can help you train your S2 and his section. The training officer prepares and consolidates the intelligence requirements for field training exercises, command post exercises, joint training support, and other training events. Along with the G3, this office develops the training requirements and standards for the division intelligence system and interfaces with intelligence simulation systems. The training office also manages the division's readiness training and other valuable intelligence training programs.

STAFF WEATHER OFFICER (SPECIAL STAFF UNDER THE G2)

3-21. The Air Force provides an SWO and a supporting combat weather team (CWT) to major subordinate commands, corps, divisions, and separate brigades to work under the supervision of the G2. The CWT can provide tailored tactical decision aids and overlays depicting the effects of weather on systems, personnel, and equipment.

TERRAIN TEAM (NO COMMAND OR SUPPORT RELATIONSHIP)

3-22. The G2 is the primary "customer" for terrain analysis. The terrain team supports

the G2 by providing terrain analysis and analysis products to describe the battlefield's effects. The terrain team can provide unique products for use by the intelligence analysts in determining AAs, axis of advance, and mobility corridors. (NOTE: the G4, and not the terrain team, is responsible for supplying Army units with maps.)

ELECTRONIC WARFARE OFFICER (NO COMMAND OR SUPPORT RELATIONSHIP)

3-23. Although the EWO works directly for the G3 and is integral to integrating EW into the targeting process, he is an intelligence officer and works closely with the ACE and G2 plans officer. He is also involved in coordinating frequency management and deconfliction with the division signal officer prior to planning and executing EA missions.

OPERATIONS

3-24. The division and corps G2s work together to build a complementary intelligence architecture within the corps. Each echelon has unique collection capabilities and requirements, but both G2s (and their ACEs) rely on a distributed and collaborative environment that allows users to share both information and intelligence down to the battalion level (through your S2).

3-25. Depending on the intelligence architecture and who is designated the joint task force (JTF) and/or the Army force (ARFOR), the division G2 coordinates with the corps or ARFOR G2 to—

- Maintain the integrity of most intelligence databases.
- Provide detailed, thorough, and "long-term" analysis.
- Conduct more robust ISR collection and processing (through more capable downlinks like certain Tactical Exploitation of National Capabilities [TENCAP] systems). Some of these units and/or systems may operate in your AO, especially during stability operations and support operations. They also may provide you with tactical HUMINT teams.

Chapter 4

Military Intelligence Capabilities

No single echelon has sufficient organic intelligence capabilities to satisfy all of your requirements. In order to efficiently use the intelligence operating system, you must understand the following:

- Intelligence disciplines.
- Intelligence functions.
  - Combat information and intelligence.
  - Electronic warfare.
- MI organizations.
- Limitations of intelligence.

To clearly describe the intelligence operating system, intelligence is divided into five disciplines and two multidiscipline functions (CI and Technical intelligence [TECHINT]).

- HUMINT.
- Imagery intelligence (IMINT).
- Measurement and signature intelligence (MASINT).
- Signals intelligence (SIGINT).
- All-source intelligence.

INTELLIGENCE DISCIPLINES

4-1. The first five disciplines are directed toward the collection, processing, and analysis of information from a specific category of sources. The two multidiscipline functions are directed toward the integration of the information collected through the first five disciplines and the production of a category or categories of intelligence. Intelligence production includes the intelligence categories of I&W, current, general military, target, and scientific and technical intelligence (S&TI). CI produces the intelligence category of CI.

4-2. Single-discipline collection or analysis rarely produces a comprehensive picture of the threat and is subject to deception. However, all-source intelligence that is produced from an adequate amount and mix of information (from the different disciplines) will meet your requirements. Each discipline must complement and cross-cue each other for maximum effectiveness. All disciplines use a combination of open and closed sources in the process of their collection and/or production.

HUMAN INTELLIGENCE (HUMINT)

4-3. HUMINT is the intelligence derived from the analysis of information obtained from a human source or a related document by a HUMINT collector. The HUMINT discipline

includes those personnel and organizations directed toward the collection, processing, analysis, and production of HUMINT.

- A HUMINT source is a person from whom information can be obtained. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. HUMINT sources include literally every human being (non-US citizens). Potential HUMINT sources include threat, neutral, and friendly military and civilian personnel; people of all ages, occupation, ethnic, religious, economic, and political groups.

- A HUMINT collector is a person who by training is tasked with and engages in the collection of information from individuals (HUMINT sources) for the purpose of answering intelligence information requirements. HUMINT collectors specifically include personnel in military occupation specialty (MOS) 97E (HUMINT) and Warrant Officers in MOS 351E (HUMINT). Other personnel that can perform HUMINT collection tasks are unit S2s acting in the capacity of tactical questioners, CI agents involved in counterintelligence force protection source operations (CFSO) and Special Forces personnel engaged in low-level source operations.

- HUMINT collection involves the use of tactical questioning, interrogation, debriefing, elicitation, and document exploitation (DOCEX) techniques to extract information from a HUMINT source. For more information on HUMINT, refer to FM 34-5(S) and FM 2-22.3 (FM 34-52).

EMERGING DOCTRINE (TACTICAL HUMINT)

Tactical HUMINT is the combination of HUMINT collection assets and CI assets using HUMINT collection techniques to support a tactical commander. This package provides a unique ability to support force protection, conduct HUMINT collection (to include counter-HUMINT), or to perform vulnerability assessments and is more common in stability operations and support operations than in war. Tactical HUMINT platoons and teams are task organized based on METT-TC. When supported by a platoon or team, it is important that you—

- Understand the capabilities, control requirements, and limitations.
- Weigh your requirements for intelligence and force protection against the risk to the platoon or teams.
- Approve the best mix of HUMINT collectors and CI personnel (through the DS MI company and employment techniques).

IMAGERY INTELLIGENCE

4-4. IMINT is the intelligence derived from the analysis of imagery derived from, but is not limited to, radar, infrared, optical, and electro-optical (E-O) sensors. The IMINT discipline includes the

following personnel and organizations directed toward the collection, processing, analysis, and production of IMINT:

- Imagery Sources (LRS, Apache, Kiowa Warrier, HUMINT).

- Imagery Collectors (U2R Advanced Synthetic Aperture Radar System [ASARS), Joint Surveillance Target Attack Radar System [Joint STARS], unmanned aerial

vehicle [UAV], TENCAP systems, and airborne reconnaissance low-multifunction [ARL-M]).

4-5. For more information on IMINT, refer to FM 2-50.1 (FM 34-25-1), FM 2-55.1 (FM 34-25-2), and TC 34-55.

MEASUREMENTS AND SIGNATURE INTELLIGENCE

4-6. MASINT is the intelligence derived from the analysis of information gathered by technical instruments such as radars, lasers, passive E-O sensors, radiation detectors, seismic, and other sensors to measure objects or events to identify them by their signatures. The MASINT discipline includes those personnel and organizations directed toward the collection, processing, analysis, and production of MASINT. REMBASS is an example of a MASINT collector. (For more information on REMBASS, refer to FM 2-00.10 (FM 34-10-1.)

SIGNALS INTELLIGENCE

4-7. SIGINT is the intelligence derived from the analysis of information obtained through the intercept of adversary communications and noncommunications emitters. The SIGINT discipline includes those personnel and organizations directed toward the collection, processing, analysis, and production of SIGINT. SIGINT is subdivided into—

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

4-8. Examples of SIGINT ground-based intercept and direction finding (DF) systems are the AN/MLQ-40(V)2 Prophet, AN/PRD-12/13, the AN/TRQ-32A (V) 2 (TEAMMATE), and the AN/TRQ-152 (TRACKWOLF) systems. The GUARDRAIL common sensor (GRCS) is an example of an airborne intercept and DF system for both communications and noncommunications emitters. The AN/FSQ-144V (TROJAN) is the Army's remote collection system supporting in-garrison collection by tactical MI units.

COUNTERINTELLIGENCE

4-9. CI is derived from the analysis of all-source information concerning the threat posed by activities of foreign intelligence and security services and the intelligence activities of non-state entities such as organized crime, terrorist groups, and drug traffickers. The CI discipline includes those personnel and organizations directed toward CI investigations and the collection, processing, analysis, and production of CI. The CI discipline also involves the recommendation of methods to counter the threat intelligence collection effort to include support to OPSEC and deception. CI personnel advise deception planners on the vulnerabilities of threat foreign intelligence services (FISs) and associated battlefield collection systems to various friendly deception capabilities and techniques. For more information on CI functions and activities, refer to FM 2-00.5 (FM 34-5)(S) and FM 2-01.2 (FM 34-60).

TECHNICAL INTELLIGENCE

4-10. TECHINT is the intelligence derived from the scientific analysis of adversary materiel to include its composition, performance, and operational capabilities. The TECHINT discipline includes those personnel and organizations directed toward the

collection, processing, analysis, and production of TECHINT.

ALL SOURCE INTELLIGENCE

4-11. All-Source intelligence is the intelligence derived from the analysis and fusing of all relevant information and single discipline intelligence products. The All-Source intelligence discipline includes those personnel and organizations directed toward the production of all-source intelligence products.

INTELLIGENCE FUNCTIONS

COMBAT INFORMATION AND INTELLIGENCE

4-12. Combat information is unevaluated data, gathered by or provided directly to the tactical commander, which due to its highly perishable nature or the criticality of the situation cannot be processed into tactical intelligence in time to satisfy your intelligence requirements. Every soldier in an operation can contribute to intelligence operations or can provide combat information through timely reporting. Some common sources of valuable and reliable information include—

- Scouts, cavalry, patrols, and individual soldiers, who can provide you with critical and exact information based upon reliable visual contact.

- Long-range surveillance (LRS) units, which provide reliable information against deep targets. LRS units conduct stationary surveillance and limited reconnaissance. They are uniquely equipped and trained to deploy deep into the threat area to observe and report threat dispositions, movement and activities, and battlefield conditions. They are not equipped or trained to conduct direct-action missions.

- Open sources, depending on the operation, are often numerous with information of varying degrees of timeliness, relevancy, and accuracy. An analyst's ability to collect, analyze, and use open-source information, however, is limited by his workload and the time available. Common open sources include news reports, Cable News Network, the Internet, magazines, textbooks, archives, and tours.

ELECTRONIC WARFARE

4-13. EW is one of your multipliers. It can disrupt threat C^2 and fire support communications during a critical phase of operations. There are three elements of EW:

- Electronic warfare support (ES) provides immediate threat intention and targeting information. It also supports all-source analysis, EA, and EP by providing threat recognition, combat information, and target acquisition as well as the specific frequencies and radio nets you want to jam.

- Electronic attack (EA) uses lethal (directed energy) and non-lethal (jamming) electromagnetic energy to disrupt, damage, destroy, and kill threat forces. MI units use non-lethal EA to jam threat C^2 and targeting systems. Electronic deception can also cause a threat to misinterpret your intentions. Used properly EA complements lethal fires.

- Electronic protection (EP) consists of measures to protect your command, control, and communications (C^3) . Your signal officer is responsible for EP.

MI ORGANIZATIONS

MI COMPANY (SEPARATE BRIGADE OR ARMORED CAVALRY REGIMENT)

4-14. This MI company has fewer capabilities than the MI battalion but more capabilities than a DS MI company. The MI company in support of the armored cavalry regiment (ACR) or separate brigade provides—

- Communications intercept, DF, and EA.
- CI.
- HUMINT collection.
- Ground surveillance. This is an interim capability and will end with the fielding of the tactical UAV systems. (Tactical UAVs will be fielded to this organization in the future.)
- Personnel to staff the S2/S3. These soldiers conduct—
  - ISR planning.
  - All-source analysis and dissemination.
  - Technical control and tasking.
  - Intelligence support to force protection and OPSEC support.

EMERGING DOCTRINE (IBCT)

MI COMPANY (INITIAL BRIGADE)

The MI Company conducts intelligence analysis, ISR integration, and HUMINT collection in support of the IBCT. This company supports the planning, preparation, and execution of multiple, simultaneous decisive actions across the distributed AOs. Additionally, it contains a much more robust analytical and HUMINT control and collection capability than the MI companies that support divisional maneuver brigades, separate brigades, and ACRs. This company consists of a—

- Small headquarters element.
- ISR analysis platoon that conducts situation development, target development, and BDA in support of the Brigade S2 section.
- ISR integration platoon that serves as the focal point for intelligence support to planning, situation awareness, and targeting. ISR integration encompasses the tasking, processing, redirecting, and fusion of information derived from sensors across all combat information, target acquisition, and intelligence assets. The most unique feature of this platoon is an organic S2X team that provides dedicated mission management for tactical HUMINT collection—a critical intelligence capability in small-scale contingency operations.
- Tactical HUMINT platoon with both operational management teams and tactical

HUMINT teams.

- US Air Force Combat Weather Team.

SURVEILLANCE TROOP (RSTA SQUADRON – INITIAL BRIGADE)

The surveillance troop is organic to the RSTA squadron of the Initial Brigade. It conducts IMINT, MASINT, SIGINT, and NBC surveillance operations in support of the Initial Brigade's planning, preparation, and execution of multiple, simultaneous decisive actions across the distributed AOs. Successful planning, preparation, and execution of these operations requires the troop's leadership and soldiers to have a clear understanding of the brigade commander's ISR requirements as well as the squadron commander's intent and concept of operations. The surveillance troop consists of a—

- Headquarters section.
- ISR integration team which is collocated with the S2 section at the squadron command post. It supports the S2 in developing, monitoring, and recommending changes to the squadron's operations. Additionally, this team assists the S2 in tracking the execution of the squadron's R&S tasks by receiving and fusing the combat information from RSTA squadron assets into a current threat picture.
- Air reconnaissance platoon (tactical UAV).
- Multi-sensor platoon which includes four multi-sensor sections. Each section consists of a SIGINT team and MASINT team. The platoon depends upon the ISR Integration Team for SIGINT mission management, technical support, and direction finding analysis.
- NBC reconnaissance platoon which can locate and identify life threatening chemical and radiological contaminants, and some forms of biological warfare. The platoon also performs extensive planning and analysis to determine threat WMD capabilities in the brigade's AO.

Additionally, the troop may receive a TROJAN Special Purpose Intelligence Remote Integrated Terminal (SPIRIT) (Light) team from the signal company to support UAV video dissemination.

MI BATTALION (DIVISION)

4-15. The MI battalion at division level provides ground-based communications intercept, DF capability, EA, HUMINT collection, ground-based surveillance, and UAV imagery support (in the future). Specifically, the MI battalion includes—

- LRS teams are deployed 15 to 80 kilometers (km) beyond the division forward line of own troops (FLOT) to observe selected NAIs. Their insertions are time phased to ensure continuous coverage of selected deep divisional NAIs. LRS teams are organic only to light, airborne, and air assault divisions.
- Ground surveillance systems are frequently attached to the maneuver units to locate moving targets. UAV assets (in the DS MI company) will replace these in the future.
- The MI Battalion will also support the division with GS UAV assets in the future.
- The present MI battalion organization includes a battlefield deception cell. That

responsibility will probably transfer to the RC in the future organization.

GS MI Company

4-16. The GS MI company provides intelligence and electronic warfare (IEW) support to the division.

- Deploys ground-based assets throughout the battlefield.
- Will include one UAV baseline GS to the division.
- Is tasked by the MI battalion commander and S3 as directed by the G2 or ACE.
- Responds to centralized control by the MI battalion, which—

— Increases system-tasking flexibility (available systems).

— Allows for coordinated DF operations.

— Contributes to more coordinated and survivable EW operations.

DS MI Company

4-17. The DS MI company provides IEW support to the division's brigades.

- Responds first to the brigades.
- Brigade (through the DS MI company) tasks and moves assets.
- Has CI and HUMINT collection assets.
- Will have UAV imagery capabilities through organic UAV assets.
- Will have a Common Ground Station (CGS) which provides a significant broadcast downlink capability to include Joint STARS moving target indicators.

MI BRIGADE (CORPS)

4-18. The MI brigade provides aerial SIGINT, HUMINT collection, and links to national and theater intelligence systems. The MI brigade can provide IEW assets to subordinate commands to weight the main effort. The corps MI brigade has three battalions: operations battalion, tactical exploitation battalion (TEB), and aerial exploitation battalion (AEB).

Operations Battalion

4-19. The operations battalion provides the ACE that performs IEW analytical, processing, and management functions in support of overall corps operations (see Chapter 3).

Tactical Exploitation Battalion

4-20. The TEB provides CI, HUMINT collection, and LRS support to corps operations. It

provides—

- GS collection to the corps in response to corps taskings.
- CI and HUMINT assets for intelligence support to force protection, OPSEC, HUMINT collection (to include DOCEX), and can be deployed throughout the corps and subordinate divisions.
- The LRS company is reliable and is deployed 60 to 150 km beyond the corps FLOT. Team deployment is time phased based on the friendly concept of the operation, number of NAIs, availability of insertion and extraction means, unique insertion skills, and need for continuous coverage.

Aerial Exploitation Battalion

4-21. The AEB allows the commander to visualize the battlefield well beyond the depth of the AO. The battalion gives you "deep look" aerial R&S and SIGINT collection capability. It provides—

- The ability to weight the main effort by prioritizing intelligence support and responsiveness to subordinate commanders.
- SIGINT data that can be sent in near real time (NRT) to multiple corps and divisional nodes to support situation and target development. With the fielding of the CGS, this information is broadcasted and downlinked through your CGS (in the DS MI company).

LIMITATIONS OF INTELLIGENCE

4-22. Your intelligence operating system has some limitations:

- Intelligence reduces uncertainty on the battlefield but cannot entirely eliminate it—"the fog of war." You will always have to accept some risk.
- You will never have enough organic and DS intelligence assets to satisfy all of your intelligence requirements.
- Limited communications systems within the intelligence architecture which, if not aggressively and proactively managed, can delay the dissemination of intelligence and combat information.
- Single-source collectors are sometimes susceptible to deception. The balanced and focused use of collection assets from multiple intelligence disciplines and careful distributed or collaborative all-source analysis are required to guard against deception.
- Degraded SIGINT collection if the threat chooses not to use communications and noncommunications systems. For example, during Operation DESERT STORM, Iraq did not employ tactical communications for fear of being intercepted and located (by DF systems).
- Adverse weather degradation on ISR operations, antenna arrays, aerial collection, and EA systems.

- Inability of ground-based SIGINT systems to operate on the move. Positioning and integration of mutually supporting ground and aerial SIGINT systems are critical to provide continuous support.

Appendix A

Intelligence and the Military Decision-Making Process

A-1. As the commander and XO, use the seven steps of MDMP to execute actions. This appendix focuses on the role of intelligence and how intelligence supports each step of the MDMP. It provides the commander and XO a checklist to use during the MDMP on what the S2 and intelligence staff provide.

- Step 1. Receipt of the Mission
- Step 2. Mission Analysis
- Step 3. COA Development
- Step 4. COA Analysis (Wargame)
- Step 5. COA Comparison
- Step 6. COA Approval
- Step 7. Orders Production

A-2. The targeting process is closely related to MDMP. The S2 conducts the **detect** and **assess** portions of the targeting process.

WHAT TO EXPECT FROM YOUR S2

STEP 1. RECEIPT OF THE MISSION

A-3. Task the S2 to start work as soon as you get the mission. (See Table A-1.)

Table A-1. Receipt of the mission

Commander's Interaction	
Initial Guidance. • Disagree with higher IPB? • Abbreviated initial IPB? • Initial ISR support? Additional IPB analysis (besides normal procedures)	
Commander's Checklist	
❑ Did the S2 begin parallel planning and collaborate with higher HQ before and during receipt of the mission to facilitate the IPB process? ❑ Did the S2 identify gaps in higher HQ ISR plan, intelligence database, and IPB products? ❑ Did the entire staff identify specified and implied intelligence tasks from higher HQ order to begin the ISR collection effort? ❑ Did the S2 start the terrain products: weather, light, and climatology data?	❑ Is the S2 continuously updating the MCOO and doctrinal templates and maintaining the threat situation? ❑ Did the S2 alert ISR assets of impending mission in order to provide sufficient time to begin troop-leading procedures? ❑ Did the S2 develop and submit initial requests for information based on gaps in the intelligence?

STEP 2. MISSION ANALYSIS

A-4. Ask the S2 for a complete analysis. Understand that everyone, not just the S2, performs IPB. Ask for a staff briefing on these products: complete MCOO, weather and light analysis, situation templates, threat COAs, initial event template, and an initial ISR plan. **Ask the staff where the higher HQ intent is captured in the products.**

Table A-2. Mission analysis

<table>
<tr><th colspan="2">Commander's Interaction</th></tr>
<tr><td colspan="2">Restated mission.

Commander's intent.

Commander's guidance—
• AO.
• AOI.
• Significant characteristics of the environment.
• Who is the threat and what it looks like?
• Choose threat models and identify any refinements.
• How many threat COAs and to what specificity?
• Initial threat culmination criteria.</td></tr>
<tr><th colspan="2">Commander's Checklist</th></tr>
<tr><td>❑ Did the S2 use the other staff officers' areas of expertise in conducting the IPB process?

❑ Did the AOI consider all threat forces— committed, supporting, reinforcing— that can impact your operation from start to finish?

❑ Did the S2 assist in the identification of the initial PIR?

❑ Did the S2 assist in the determination of the initial OPSEC or EEFI requirements to include CI considerations?

❑ Did the entire staff produce a MCOO that—
• Defines defensible terrain?
• Identifies—
– Key or decisive terrain?
– Mobility corridors (air and ground)?
– Restricted or severely restricted terrain?
– Infiltration lanes? Landing zone (LZ) and pickup zone (PZ)?

❑ Did the S2, in conjunction with the entire staff—
• Develop situation templates of the threat based on the constraints of the terrain?</td><td>❑ Do the situation templates—
• Include all committed and reinforcing forces as well as combat multipliers?
• Focus two levels down in detail to include all threat operating systems?
• Identify OB, weaknesses and peculiarities, activities, and capabilities for each COA with graphics?

❑ Do the IPB products identify facts and assumptions that assist in the determination of likely threat COAs?

❑ Did the S2 prepare terrain and weather analysis products to describe what effects will significantly impact the upcoming battlefield on both threat and friendly forces?

❑ Did the S2 develop a line-and-block chart with the number of killing systems depicting the threat composition?

❑ Did the initial ISR plan—
• Consider the AO and the mission statement?
• Consider the current event template?

❑ Is the initial ISR plan based on the—
• PIR?
• Information requirements (IR)?
• NAIs?

❑ Did the S2 provide ISR assets with an initial ISR plan that facilitated dissemination of orders, conduct of rehearsals, and ensured ISR activities in support of the decisionmaking process by ongoing ISR</td></tr>
</table>

• Prepare threat situation templates depicting the threat disposition? • Prepare as many situation templates as time allowed? ❑ Do the event templates identify and focus on— • NAIs? • Time phased lines? • Time distance analysis? • Critical actions? • Threat decision plan? ❑ Did the S2 provide subordinate units with a copy of all intelligence products to facilitate their IPB process?	operations? ❑ Did the S2 incorporate higher HQ collection requirements? ❑ Did the S2 forward intelligence requirements that cannot be answered by assigned collection assets to higher HQ? ❑ Did the MI battalion or DS MI company commander brief the collection status and capabilities?

STEP 3. COA DEVELOPMENT

A-5. Ask for and expect a thorough analysis of the threat on combat organization (composition and disposition) and possible threat COAs. Ask the S2, in conjunction with the entire staff, to provide intelligence about the threat's main effort and how they will employ their combat multipliers (fires, ADA, engineers, C^2, intelligence, CSS, and chemical) to support their COAs. Ask what key indicators are used to confirm or deny threat COAs, critical decision points (DPs), and friendly and threat vulnerabilities. Ask how often the S2 updates intelligence-related products. (See Table A-3.)

Table A-3. COA development decision points

Commander's Interaction	
Has the S2 provided intelligence about— • The threat main effort? • Employment of their combat multipliers (fires, ADA, engineers, C^2, intelligence, CSS, and chemical) to support their COAs? Ask the S2 what the key indicators are used to confirm threat COAs, critical DPs, and friendly and threat vulnerabilities. Ask how often the S2 updates intelligence-related products.	
Commander's Checklist	
❑ Has the S2— • Refined and prioritized the situation templates? • Refined the event template and matrixes? • Developed an initial EW target list (EWTL)? ❑ Did the S2 take an active part in analyzing combat power by providing all available information on the current threat forces and situation? ❑ As time permits, while analyzing relative combat power, did the S2 provide the staff with information on threat vulnerabilities?	❑ Did the S2 consider as many possible COAs as time permits, starting with the most likely and including the worst case (most dangerous)? ❑ Did the S2 provide critical input to the MDMP through continual analysis of information provided by ongoing ISR operations? ❑ Did the S2 and S3 task ISR assets without overtasking them? ❑ Did the S2 and S3 allocate sufficient assets to conduct the ISR plan?

STEP 4. COA ANALYSIS (WARGAME)

A-6. During the wargame each staff member is responsible for his area of expertise. It is recommended that the S2 play the role of the threat commander. (See Table A-4.)

Table A-4. COA analysis (wargame)

Commander's Interaction	
No interaction necessary at this point.	
Commander's Checklist	
❑ Did the S2— • Refine the PIR with the LTIOV? • Assist in the development of the HPTL? • Finalize the situation template? • Redefine the threat COAs based on the developed DPs and finalize the situation template? ❑ Did the S2 develop critical threat DPs in relation to the friendly COA? ❑ Did the S2 fight as an uncooperative threat to develop DPs and project threat losses? ❑ Did the S2, in conjunction with the entire staff, address all relevant threat operating system activities? ❑ Did the S2 assist in developing the target selection standards and attack guidance matrix from the wargamed COAs?	❑ Did the S2 update the collection and ISR plan? ❑ As a result from the wargame, did the S2 identify IR and refine the event template to include NAIs and refine the event matrix with corresponding decision points? ❑ Did the S2 indicate target areas of interest (TAIs) and HVTs? ❑ Did the S2 refine the situation templates from the results? ❑ Did the S2 participate in the targeting process and identify and prioritize HVTs as determined by IPB? ❑ Did the assistant S2 (from the wargame) determine what information to collect, who is to collect, as well as when and where to collect it?

STEP 5. COA COMPARISON

A-7. Although your S2 plays the uncooperative threat commander, he still has requirements to deliver various intelligence products to you and the staff. (See Table A-5.)

Table A-5. COA Comparison.

Commander's Interaction	
No interaction necessary at this point.	
Commander's Checklist	
❑ Did the S2 coordinate with the other staff elements in order to start developing the integrated ISR plan and the intelligence portion of the synchronization matrix?	❑ Did the S2 update the IPB products for the decision briefing?

STEP 6. COA APPROVAL

A-8. Refine the intent statement and CCIR to support the selected COA. The staff refines its products in anticipation of the orders production. (See Table A-6.)

Table A-6. COA approval

Commander's Interaction	
Approved COA. Refined commander's intent. Specified type of order. Integrated ISR plan. Specified type of rehearsal.	
Commander's Checklist	
❑ Did the S2— • Update the PIR with LTIOV for your approval supporting the approved COA? • Finalize the event template matrixes and the ISR plan? • Plan for BDA support in coordination with the ISR plan?	❑ Did the staff refine— • The DST? • The operating system synchronization matrix? • ISM based on the approved COA? • Integrated ISR plan

STEP 7. ORDERS PRODUCTION

A-9. After you issue final guidance, the staff begins preparing the order for dissemination. (See Table A-7.)

Table A-7. Orders protection

Commander's Interaction	
No interaction necessary at this time.	
Commander's Checklist	
❑ Did the S2— • Assist in preparing the order? • Submit the Intelligence Annex (B) as part of the order? • Finalize the ISR plan and provide an ISR Annex (L) and overlay?	• Assist with the C^2 Warfare Annex (P), OPSEC Annex (Q), Deception Annex (S), and the EW Annex (T)? ❑ Did the S2 integrate the ISR plan with the S3's scheme of maneuver and fires?

TARGETING MEETING

A-10. Each participant should bring the essential information to the targeting meeting. After the targeting meeting, each participant should leave with some critical information. (See Table A-8.)

Table A-8. Targeting meeting

Commander's Interaction	
No interaction necessary at this time.	
Commander's Checklist	
❑ Did the S2 have— • The current situation map? • Situation templates with detailed information on each BOS and capability? • HVTs and recommended HPTs? • Information about the collection assets available? • Intelligence synchronization matrix (ISM) and event template? • Plan for tracking BDA? • Current BDA on hand? • Current PIR and CCIR? ❑ Did the S2 provide the proposed threat activity within the current 24-hour period?	❑ Did the S2 provide the proposed threat activity within the next 24 to 48 hours? ❑ Did the entire staff plan the use of lethal and non-lethal fires to support the operation? **After the Targeting Meeting** ❑ Did the S2— • Have the updated PIR? • Know who will collect what, where, when, and have the taskings for them? • As a result of the targeting meeting provide the intelligence portion to the upcoming FRAGO? • Know his role, the S3 role, and FSO role in the sensor-to-shooter links and controls?

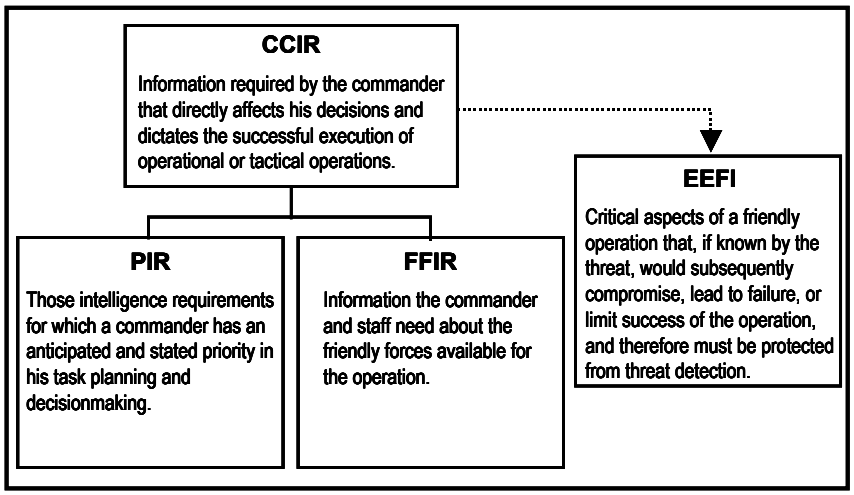
Appendix B

Commander's Critical Information Requirements

B-1. CCIR is information required by the commander that directly affects his decisions and dictates the successful execution of tactical operations. You can get more information than you need or want. Your CCIR will allow you and your staff to focus on the information that is important to your decisions. The CCIR help to focus your staff so they can produce timely and accurate information and a common operational picture (COP). CCIR are—

- Applicable only to you.
- Situation-dependent.
- Events or activities that are predictable.
- Specified by you for each operation.
- Time-sensitive information that must be immediately reported to the commander, staff, and subordinate commanders.
- Always included in paragraph 5 of an OPORD or OPLAN.
- Transmitted by a communications system specified in the standard operating procedures (SOPs).

B-2. Limit CCIR to 10 or fewer items so the staff can focus its efforts better. The CCIR are expressed as two types of requirements: PIR and friendly forces information requirements (FFIR). Although EEFI are not a part of CCIR anymore, they become a commander's priority when he states them. Figure B-1 shows the



elements of CCIR.

Figure B-1. Elements of CCIR.

PRIORITY INTELLIGENCE REQUIREMENTS

B-3. These are intelligence requirements for which you have an anticipated and stated priority for planning and decisionmaking. PIR support your DPs. Without the answer, you accept a greater level of risk during operations. You dictate the format of the answer (for example, a graphic product, verbal report, or image) and you must set an LTIOV.

B-4. Base most of your PIR on a specific fact, event, or activity that the threat has or is known to do (or specific to the environment) but remember to consider how the threat could surprise you (an atypical threat)—potentially one of their greatest advantages. PIR are listed and ranked in order from most to least important. Do not give multiple questions in a single PIR or you will not focus on your real requirement and may not satisfy your requirement. Do not ask questions that have been answered.

B-5. Examples of **Good** PIR:

- Will the threat defend OBJ Bruno using a forward slope defense 121630Z JUL 99 LTIOV? (DP: Fire artillery preparation).
- Will the threat reserve tank battalion reach PL Mike before 121630Z JUL 99 LTIOV? (DP: Commitment of the reserve).
- Will the 43d MRD send its main attack along the AA 121630Z JUL 99 LTIOV? (DP: Commitment of deep strike).
- What size force is defending OBJ Gun LTIOV? (DP: Composition of the main attack).

B-6. Examples of **Bad** PIR:

- When, where, and in what strength will the threat attack?
- What are the fuel levels in the threat's depots?
- What is the current readiness of all threat armor, artillery, and anti-tank units?
- What is the morale of the threat rear echelon units?

B-7. The above PIR are bad because they reflect multiple questions, not focused on the real requirement, and do not satisfy the requirement.

B-8. There are other requirements that entail collection. They are of lower importance than any PIR but are still an important part of the ISR plan. Information requests, indicators, specific information requirements (SIRs), and specific orders and requests (SORs) are closely related to PIR.

INFORMATION REQUIREMENTS

B-9. IR are those items of information regarding the threat and his environment which need to be collected and processed. These requirements are necessary to perform situation development, support to targeting, IPB, and support to force protection but are less critical than PIR.

INDICATORS

B-10. Indictors are threat actions, activities, or signatures whose absence or presence

show evidence of threat intentions, capabilities, and vulnerabilities, and help to confirm or deny a threat COA. The predictions and projections within the situation and event templates are an important factor in performing situation development based on threat activities. A thorough knowledge of when and where activity is likely to occur on the battlefield helps an analyst develop indicators. The indicators in turn help the analyst develop PIR and build SIRs.

SPECIFIC INFORMATION REQUIREMENTS

B-11. A complete SIR describes the information required, the location where the required information can be collected, and the time during which it can be collected. Generally, each PIR or IR generates sets of SIRs. These may partially or fully answer a PIR or IR and provide the analyst the information necessary to confirm or deny threat COAs.

SPECIFIC ORDERS AND REQUESTS

B-12. This is the specific tasking orders approved by the S3 or request for support higher that generates planning and execution of a collection mission or analysis of database information. Specific orders (for example, S3 approved taskings) are orders for subordinate commands; requests (for example, for support) are sent to other commands or higher echelons.

FRIENDLY FORCES INFORMATION REQUIREMENTS

B-13. This is information you and your staff need about the friendly forces available for the operation. This includes personnel, maintenance, supply, ammunition, and petroleum, oils and lubricants (POL) status, and experience and leadership capabilities.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION

B-14. The EEFI help protect your operation. They are critical aspects of a friendly operation that, if known by the threat, would subsequently compromise, lead to failure, or limit success of the operation and therefore must be protected from threat detection. EEFI help commanders understand what threat commanders want to know about friendly forces and why. They tell commanders what cannot be compromised. EEFI provide the basis for indirectly assessing the quality of the threat's situational understanding: if the threat does not know an element of EEFI, it degrades his situational understanding.

Appendix C

ISR Integration Within the Synchronization Matrix

C-1. Successful synchronization of ISR collection with operational decisionmaking results in effective, timely intelligence. Failure to synchronize ISR results in the waste of valuable ISR assets against requirements that are not critical to the commander's decisions. This waste results in making a decision with erroneous intelligence or no intelligence at all.

C-2. The intelligence BOS has responsibility for the portion of the synchronization matrix that deals with intelligence collection. The S2 should always contribute to the production of the synchronization matrix. The S2 inputs all information for NAIs or TAIs, to include timeline, task, mission, purpose for collection, and DPs tied to the collection or lack of information collected.

C-3. The synchronization matrix is produced after wargaming, when the commander has established a COA and DPs supported by intelligence. The G2/S2 then determines the LTIOV for each NAI and event, based on those DPs and targeting requirements identified during wargaming.

C-4. The S2 links each PIR to a DP. Each PIR should be linked to only one operational decision. The S2 then develops the ISR plan for the unit, and checks that each PIR will be answered in time to influence operational decisions.

C-5. The S2 selects ISR assets based on the situation, asset capabilities, and availability. The ISM in Figure C-1 depicts how each NAI and TAI will be covered by an ISR system while that NAI or TAI is active.

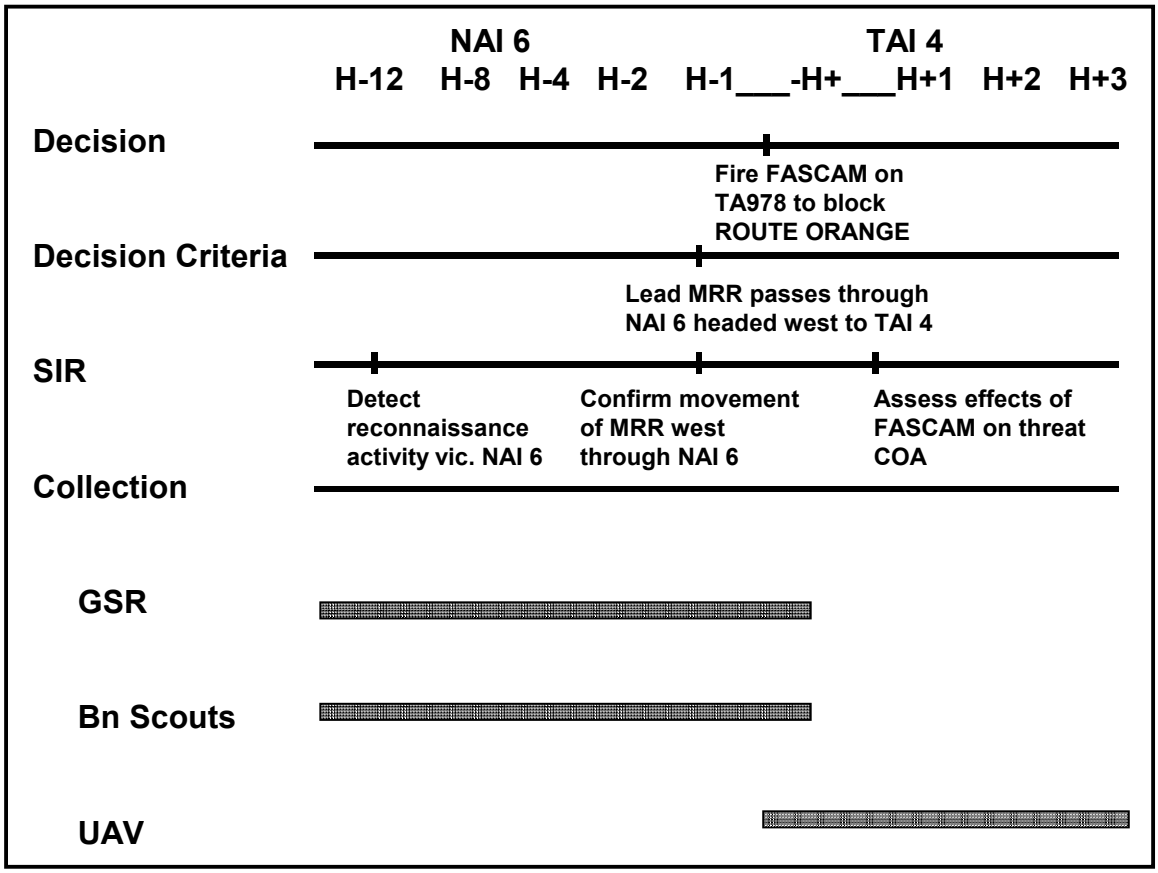


Figure C-1. Sample of intelligence portion of the synchronization matrix

Appendix D

Intelligence, Surveillance, and Reconnaissance Planning

D-1. ISR is essential to gain and maintain contact with the threat. In certain situations gaining contact with the threat can include a combination of technical means and traditional contact as defined in cavalry doctrine. Many battles at the combat training centers prove that successful ISR operations are critical to successful operations.

D-2. During operations you should task your ISR assets to find and report—

- Gaps or vulnerabilities in the threat's operations.
- Defensive preparations to include primary and secondary positions and prepositioned supplies.
- Location of any threat reserves and supporting forces (for example, a supporting artillery or air defense positions).
- Obstacles, threat engagement areas, and potential ambush areas.
- Information that answers threat intentions and capabilities.

D-3. During operations, you must focus your staff on blinding the threat through an aggressive counterreconnaissance. This effort requires an active, predictive intelligence effort. CI analysis of threat multidiscipline ISR operations is integral to counterreconnaissance analysis and operations. Your S2 should use any threat assessment and other CI products, as appropriate, and forward analytical requirements to the CI analytical element at division and above (through standard procedures).

D-4. In the future, CI functionality will include analysis of threat IO and other full-dimensional counter-ISR tasks. CI analysis is especially important during stability operations and support operations, and is one of the primary contributors to the counterreconnaissance effort.

D-5. In order to drive ISR planning ask the following:

- Did the S2 develop threat COAs and event templates based on your initial guidance?
- Did you refine your PIR and the ISR plan (tasks) based on the friendly COA?
- Did the S2 and S3 integrate the ISR plan with the scheme of maneuver? Are the NAIs and TAIs the focus of the ISR plan and do they support the DST for the friendly COA? At brigade level, does the ISR synchronization matrix answer your PIR and targeting requirements?
- Are all organic and supporting collection assets considered in the ISR plan? Was the ISR plan developed in relation to the overall ISR architecture? Have

sufficient resources been dedicated to the ISR plan?

- Does the IPB identify the risks during infiltration of ISR assets? Are ISR assets teamed to improve their chances of success and minimize the changes of casualties? Are adequate fires planned to support ISR operations?

- Did the S4 and/or headquarters and headquarters company (HHC) commander plan casualty evacuation and allocate resources to support the reconstitution of ISR assets? Did the signals officer plan adequate communications support for ISR operations?

- Did the staff use a five-paragraph FRAGO based on an ISR tasking matrix to capture all of the integrated staff planning?

- Did the staff develop the counterreconnaissance plan and is its emphasis on identifying threat reconnaissance COAs?

- Did you assign the right assets required to execute your ISR?

- Did you assign the right assets required to execute your counterreconnaissance effort?

D-6. Make the S2 and S3 brief you and the staff on how they will track ISR execution? Train your staff to track the battle, using the DST and the synchronization matrix. The S2 and S3 must use the ISR plan and ISR synchronization matrix (at brigade) to track and retask assets in order to answer your PIR.

D-7. In order to track and retask ISR operations, ask the following:

- Is the S2 using the event and situation templates to analyze the information and perform predictive analysis?

- Are the S2 and S3 tracking the status of ISR assets in a timely manner and cross-cueing ISR assets and teaming them to minimize the chances of casualties?

- Is ISR reporting confirming the initial assumptions about the threat COAs (or the environment)? If not, is the staff using a “mini-wargame” to reevaluate initial assumptions, reinitiate an abbreviated IPB and MDMP, and quickly change the operation?

Appendix E
Foreign Language Support

INTRODUCTION

E-1. You need linguists for full spectrum operations especially when the focus is on stability operations and support operations. You need a good linguist support plan to select qualified linguists for each requirement. The growing focus on multinational operations increases the competition for limited linguist resources vital for mission success. Consider the lowest possible foreign language qualification needed for each mission, taking into account the limitations of the Defense Language Proficiency Test (DLPT) for Army linguists.

LINGUISTIC SUPPORT CATEGORIES

E-2. Foreign language support to US Armed Forces engaged in stability operations and support operations falls into one of four categories:

- **INTELLIGENCE AND INFORMATION COLLECTION.** TRADITIONAL SIGINT AND HUMINT DISCIPLINES, AS WELL AS FOREIGN LANGUAGE SUPPORT TO FORCE PROTECTION AND EXPLOITATION OF OPEN-SOURCE INFORMATION.
- **CIVIL/MILITARY OPERATIONS**. MILITARY INTERACTION WITH THE CIVILIAN POPULATION FOR GOVERNMENT LIAISON, LEGAL AGREEMENTS, MEDICAL SUPPORT AND OPERATIONS, LAW ENFORCEMENT, ENGINEERING PROJECTS, PUBLIC SAFETY, SECURITY AND POPULATION CONTROL, CA, AND PSYOP.
- **LOGISTICS.** SUSTAINMENT OR TRANSPORTATION FUNCTIONS. FOR LOGISTICAL CONTRACTING, PORT, RAILHEAD, AIRHEAD, OR TRANS-SHIPMENT OPERATIONS AND CONVOY OPERATIONS**.**
- **MULTINATIONAL MILITARY OPERATIONS AND LIAISON.** COORDINATION WITH ALLIED PARTNERS, COALITION PARTNERS, AND PREVIOUSLY UNAFFILIATED NATIONS.

DETERMINING LINGUIST REQUIREMENTS

E-3. The staff uses METT-TC, organization or echelon of command, and the environment to—

- Determine the number of linguists for a particular mission.
- Allocate linguists by one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed.

- Conduct mission analysis and identify specified or implied tasks requiring foreign language support.

E-4. Task organization and scheme of maneuver are then applied to determine the number of linguists needed for an operation. The staff must analyze each operation to determine the language requirements. While interpretation for a peace negotiation requires not only outstanding linguistic capability but also cultural acumen, the translation of routine documents with the aid of a dictionary requires a much different skill set. Poor identification of language requirements can tie up the best linguists in a less effective role, creating linguist shortfalls in other areas.

E-5. The relative importance of each of the four linguist support categories is mission dependent. For example, during a noncombatant evacuation operation (NEO) civil or military coordination would probably not be as critical as collecting intelligence and information. The situation is reversed for a humanitarian assistance mission in which civil or military operations have a significant impact on mission success. Identifying these dynamics helps the commander and staff prioritize linguist requirements.

E-6. Determining stability operation and support operation linguist requirements can be difficult because each operation is unique. Commanders and staff with a basic knowledge of organic Army linguistic assets, foreign language resource alternatives, and MI skills can successfully utilize linguists in support of their military operations.

PLANNING AND MANAGING LINGUIST SUPPORT

E-7. Commanders who conduct stability operations and support operations must include linguist requirements as part of their MDMP. Decide what foreign languages are needed, what types of foreign language requirements are needed for each assignment, and what would be the best source of linguist assets. If the mission includes intelligence and information collection, you must decide on which MI collection skill is needed.

E-8. You should consider linguist requirements for every contingency plan and OPLAN assigned to your command. Linguist requirements should be considered in at least the first nine steps of mission analysis (see FM 5-0 and FM 6-0 (FM 101-5)). Additionally, you must decide on security clearance requirements early in the mission; also, it is helpful to initiate linguist researching and command relationships before actual operations.

PRIMARY STAFF RESPONSIBILITIES

E-9. Primary staff at each echelon has responsibilities for evaluating requirements and managing linguist support. The responsibilities include but are not limited to the following:

- Assistant Chief of Staff, G1 (S1), Personnel will—
  - — Identify linguist requirements needed to support G1/S1functions in all contingency areas.
  - — Manage linguist staffing and linguist replacement management.
  - — Identify foreign language skill identifiers for all assigned, attached, or OPCON Army linguists.

- Identify all Army foreign language skilled soldiers not identified in the Standard Installation Division Personnel Section (SIDPERS).
- Ensure language skills are added to SIDPERS.
- Deploy and provide administrative support of Department of the Army and Department of Defense civilian linguists.
- Hire, contract for, and provide administrative support of local national linguists.
- Procure Army foreign language support personnel for screening local labor resources.

- Assistant Chief of Staff, G2 (S2), Intelligence will—
  - Identify linguist requirements needed to support G2/S2 functions in all contingency areas.
  - Determine, during the initial IPB, all foreign languages (spoken and written) and dialects needed for mission accomplishment.
  - Collect, process, produce, and disseminate information derived from linguist sources.
  - Provide intelligence training for MI linguists employed in the AO.
  - Coordinate for security investigations, as necessary, for local hire linguists.
  - Provide support to CI screening of contracted linguists and the local national labor force.

- Assistant Chief of Staff, G3 (S3), Operations will—
  - Identify linguist requirements needed to support G3/S3 functions in all contingency areas.
  - Consolidate unit linguistic requirements and establish priorities.
  - Develop linguist deployment and employment plans.
  - Develop plans to train linguists and to use linguists for training the force in AO foreign language survival skills.
  - Assign, attach, and detach linguists and linguist teams.
  - Integrate additional or replacement linguists through operational channels.
  - Recommend modernization and development of linguist systems and methods.
  - Coordinate mobilization and demobilization of RC linguist support.
  - Plan linguist usage for deception operations.
  - Plan linguist support to movement of enemy prisoner of war (EPW), detainees, and refugees.
  - Coordinate evaluation of linguist support by all staff elements.

- Assistant Chief of Staff G4 (S4), Logistics will—
  - Identify linguist requirements needed to support G4/S4 functions in all contingency areas.
  - Provide logistical, supply, maintenance, and transportation support to attached linguists.

- Assistant Chief of Staff G5 (S5), Civil-Military Operations will—
  - Assist the G1 in the contracting of local hire linguists.
  - Identify foreign language requirements for NEO and other civil and military operations.

- Assistant Chief of Staff G6 (S6), Signal will—
  - Manage radio frequencies assignments to supporting SIGINT linguist elements.
  - Support linguist operations with internal document reproduction, distribution, and message services.
  - Integrate automation management systems of linguist units.

E-10. In addition, each staff section has to determine the linguist support required to meet its operational missions. Staff requirements for linguist support include but are not limited to the following:

- Assistant Chief of Staff, G1 (S1), Personnel will—
  - Coordinate with local authorities on matters of civilian hire, finance, and recordkeeping.
  - Contract local hire personnel.
  - Coordinate local morale support and community activities.
  - Coordinate with local authorities for postal operations.
  - Support administration, counseling, personal affairs, and leave for local national and third-country national personnel.
  - Coordinate local medical support.
  - Liaison with coalition counterparts.

- Assistant Chief of Staff, G2 (S2), Intelligence will—
  - Evaluate and use local maps and terrain products in operations.
  - Process, for MI purposes, material taken from EPWs or civilian internees.
  - At lower echelons, conduct tactical questioning of refugees, detainees, and EPWs.
  - Assess local open-source information for intelligence value.
  - Ensure intelligence coordination and liaison with coalition and HN counterparts.

- Assistant Chief of Staff, G3 (S3), Operations will—
  - Ensure operational coordination and liaison with coalition and HN counterparts.
  - Translate OPORDs and OPLANs for use by coalition counterparts.

- Assistant Chief of Staff G4 (S4), Logistics will—
  - Procure local supply, maintenance, transportation, and services.
  - Coordinate logistics at air and seaports of debarkation.
  - Provide logistic support to local population.
  - Coordinate foreign language support to help contract for water, food service, bath and laundry if necessary.
  - Contract with local governments, agencies, and individuals for sites and storage.

- Assistant Chief of Staff G5 (S5), Civil-Military Operations will—
  - Assist the G1 in the contracting of local hire personnel.
  - Determine civilian impact on military operations.
  - Minimize civilian interference with combat operations.
  - Inform civilians of curfews, movement restrictions, and relocations.
  - Provide assistance to liaison with HN and multinational agencies, dignitaries, and authorities.
  - Promote positive community programs to win over support.
  - Determine if combined operations PSYOP efforts are mutually planned and synchronized.
  - Support interpretation to assist resolution of civilian claims against the US government.
  - Solicit linguistic and cultural knowledge support to protect culturally significant sites.
  - Use linguistic and cultural support to identify cultural and religious customs.

- Assistant Chief of Staff G6 (S6), Signal will—
  - Coordinate suitable commercial information systems and services.
  - Coordinate with multinational forces on command frequency lists.
  - Coordinate signal support interfaces with HN and multinational forces.

USE OF CONTRACT COMPANIES TO HANDLE LINGUISTS AND LINGUIST SUPPORT

E-11. Contract linguists can be used to backfill shortfalls in military linguist resources. Contracting is usually managed at or above the brigade level, and funding is requested through channels.

E-12. Contract linguists are supervised by the gaining military organizations. The G3 (S3) usually has responsibility. The contract linguists are controlled by the vendor who resolves performance and discipline issues.

SPECIAL STAFF OFFICERS RESPONSIBILITIES

E-13. If no special staff officer is assigned the duties below, the corresponding coordinating staff officer should assume those responsibilities. Linguist requirements for special staff officers include but are not limited to the following:

- Liaison Officer:
  - Should speak the required foreign language; if not, a translator or interpreter is necessary for all aspects of his duties.
  - Request interpreters to assist when representing the commander in combined or multinational operations.
  - Translate orders, maps, traces, overlays, and documents into coalition foreign languages.
- Civilian Personnel Officer:
  - Recruit, interview for suitability, and hire civilian local labor force if required.
  - Host country negotiations on labor agreements.
- Dental Surgeon:
  - Administer dental care to support humanitarian mission requirements.
  - Rehabilitate, construct, and gain usage of existing dental facilities as required.
- Finance Officer:
  - Coordinate exchange of US funds into needed local currencies.
  - Provide non-US and US pay functions to foreign national, HN, and civilian internees, and EPWs.
- Surgeon:
  - Support medical humanitarian assistance and disaster relief operations.
  - Provide medical care of EPWs and civilians within the command's AO.
  - Coordinate medical laboratory access in AO.
  - Determine the nature of local health threats to the force through populace interviews.
  - Determine the identity of local or captured medical supplies.

- Veterinary Officer:
  - Determine source and suitability of local foods.
  - Assist the local population with veterinary service needs.

- Chemical Officer:
  - Identify threat force chemical weapons and equipment.
  - Communicate NBC risks to supported populations.

- Engineer Coordinator:
  - Procure proper local materials to support engineering mission.
  - Communicate engineering project requirements to contracted local work force.
  - Communicate engineering project impact on local landowners and other affected parties. Determine, in coordination with G2 (S2), suitability of local topographic maps and terrain products.
  - Assess environmental concerns of HN and local populations in combined operations.

- Provost Marshal:
  - Support dislocated and civilian straggler control activities.
  - Support internment and resettlement operations.
  - Communicate weapons bounty programs and payments to the local population.
  - Support counter-drug and customs activities.
  - Help foreign civil authorities maintain control when authorized.
  - Conduct liaison with local law enforcement authorities.

- PSYOP Officer:
  - Produce approved PSYOP propaganda and counter-propaganda media.
  - Evaluate PSYOP impact on target audience.

- Safety Officer:
  - Provide safety training to local labor force.
  - Communicate warnings of dangerous military operations and other hazards to local populace.

- Transportation Officer:
  - Coordinate commercial and local transportation needs.
  - Coordinate movement scheduling and routes with multinational forces and HN.

PERSONAL STAFF OFFICER RESPONSIBILITIES

E-14. Personal staff officers are under the immediate control of and have direct access to the commander. Most personal staff officers also perform special staff officer duties, working with a coordinating staff officer. These assignments are on a case-by-case basis, depending on the commander's guidance and the nature of the mission, and are very common in stability operations and support operations. Linguist requirements for special staff officers include but are not limited to the following:

- Chaplain:
  - Provide moral and spiritual leadership to the populace.
  - Coordinate religious support with coalition and multinational partners.

— Determine the impact of indigenous religious group faith and practices on military operations.
— Provide religious support to the community to include hospital patients, EPWs, refugees, and civilian detainees.
— Conduct liaison with indigenous religious leaders in close coordination with the G5.

- Public Affairs Office (PAO):

— Act as commander's spokesman for all communication with external media.
— Assess the accuracy of foreign media interpretation of PAO releases.

— Assess and recommend news, entertainment, and other information (assisting G5) for contracted services foreign nationals.

- Staff Judge Advocate:

— Translate foreign legal codes, Status of Forces Agreements (SOFAs), and international laws.
— Determine local environmental laws and treaties through translation services.
— Assess the treatment of EPW and civilian internees.
— Translate documents to support G4 in local contracts.

IDENTIFYING SOURCES OF LINGUISTS

E-15. Sources of linguist support include AC, non-MI Army linguists, RC, other Service linguists, US government civilian employees, US contract linguists, allied and coalition linguists, and local national contract linguists. It is vital to know the advantages and disadvantages of each type of linguist and to carefully match the available linguists to the operation.

ACTIVE COMPONENT

E-16. AC MI language dependent MOSs include MOS 97E (HUMINT Collector), 98G (Voice Intercept Operator), and their related warrant officer fields. Some soldiers in MOS 96B (All-Source Intelligence Analyst), MOS 97B (CI Agent), and MOS 98C (SIGINT Analyst) and their related warrant officer fields are trained in foreign languages.

E-17. There are many advantages to utilizing soldiers in the MOSs mentioned above. They are already trained in the military system, are not subject to deployment restrictions (a limiting factor with civilian linguists), have a security clearance and, as US personnel, support the command's interests.

E-18. The major disadvantage to using these individuals for general foreign language support is that in doing so, they are removed from their primary MI functions. They should be used only in linguistic duties that include intelligence potential. For example, an interrogator (97E) provides linguist support to a CA team as a method to provide access to the local population to determine their attitudes toward US Forces.

NON-MI ARMY LINGUISTS

E-19. Non-MI Army linguists include some enlisted and warrant officers in Career Management Field (CMF) 18 (Special Forces), CMF 37 (PSYOP), CMF 180A (Special Forces), and commissioned officers with a branch code 18 (Special

Forces) and functional areas 39 (PSYOP and CA) and 48 (Foreign Area Officer). Since the standards vary by field, pay attention to the recorded language proficiency and test date of these individuals.

E-20. The Army also includes numerous soldiers who have proficiency in a foreign language but whose jobs do not require foreign language proficiency. They may have trained in a foreign language or may have acquired proficiency through their heritage. They have the advantage of being trained soldiers and are therefore readily deployable to all areas of the battlefield.

These soldiers may have the specific vocabulary and military skill knowledge for certain linguist support missions. For example, a supply sergeant who speaks the local language would be an invaluable asset to the G4.

E-21. The disadvantages are that they already have another job and units are reluctant to give up personnel, especially those in key positions, and their capabilities are difficult to assess. Since they are not required to take the DLPT, it is often difficult for the G1 (S1) to identify them as a linguist, or for a non-linguist to judge the level of their foreign language capability.

RESERVE COMPONENT

E-22. RC trained MI linguists include the MOSs listed above in the AC. RC MI linguists have the same set of advantages and disadvantages as listed above for AC MI linguists.

E-23. The RC also includes MI linguists in MOS 97L (Translator/Interpreter). The 97L's are specifically trained to be a translator and interpreter and have the advantages listed above. An added advantage is that, since their sole job is translation and interpretation, they do not have to be removed from another job in order to be used as linguists. The major disadvantage is that they might not have additional skills that give them dual functionality.

OTHER SERVICE LINGUISTS

E-24. Other service linguists have the advantage of deployability, loyalty, and clearance, but must often learn the Army system and specific Army vocabulary. They are also difficult to obtain, as their parent service is probably also short of trained linguists. Other Service linguists, however, will be valuable in joint operation centers and joint activities. When serving the JTF headquarters, Army commanders and staffs must be aware of the linguists in the other services in order to plan for their participation and optimize their employment.

US GOVERNMENT CIVILIAN EMPLOYEES

E-25. Civilians who have knowledge of a foreign language and are already employees of the US government in some capacity have the advantage of being in the system. They are difficult to obtain as they are already filling required positions and are usually not available for translator/interpreter use. They also are not as readily deployable as service members.

Civilians may have the advantage of extensive knowledge of the AO and extensive foreign language capability.

US CONTRACT LINGUISTS

E-26. US civilians can be contracted to provide linguist support. They have an advantage over local national hires in that their loyalty to the US is more readily evaluated and they can be more readily granted the necessary security clearance.

There may be severe limitations on their deployment and use and they must be carefully screened for foreign language ability. In many cases their use of the foreign language may be old fashioned or full of US idioms depending on their length of time in the US. If recent émigrés, their use in the country of their origin could be dangerous to them, or their loyalty may reside with the country of origin at odds with US interests.

ALLIED AND COALITION LINGUISTS

E-27. Allied and coalition linguists may be unfamiliar with the US system, and their loyalty is difficult to ascertain. MI linguists who speak the partner's language can be useful in determining reliability and loyalty of allied or coalition linguists.

LOCAL NATIONAL CONTRACT LINGUISTS

E-28. Local national hires will provide the bulk of your linguist support. They are usually cheaper to hire than US civilians and will know the local dialect and idioms. They can be selected for their expertise in particular areas or subject matter. A potential problem with local national hires is their ability to speak English, necessitating a screening interview or test to determine their ability to communicate in English.

E-29. For security reasons, CI personnel must carefully select and screen local nationals initially and periodically throughout their employment. Their loyalty can never be assumed. They may be affected by local prejudices and can be assumed to place their own interests above those of the US.

Appendix F

Stability Operations, Support Operations, and Intelligence Preparation Of The Battlefield

F-1. IPB analyzes the possibilities and limitations imposed by the AO and the threat's capabilities. It depicts the threat's possible COAs, and the probabilities of each COA occurring.

F-2. To make the IPB process relevant to stability operations and support operations, the S2 must go back to the basics: discern the intent of each step of the IPB process and interpret some doctrinal terms loosely. In this way your S2 can prevent trying to force a threat into a mold, which makes threat COAs and activities easier to express with familiar IPB products.

F-3. "Threat" describes the various challenges US forces can expect in stability operations and support operations. "Enemy" is too narrow a term for some of the challenges stability operations and support operations will encounter. Refugees, nongovernmental organizations, disaster victims, disease and environmental dangers, and many other challenges encountered during the types of operations brigades face today do not fit the definition of enemy, but they do pose a challenge to successfully accomplishing your mission.

F-4. To avoid overlooking serious challenges to mission success, we offer this definition of "threat" paraphrased from the Australian Army's definition: "**Threat** is any actor, agent, or environmental factor which endangers the commander's ability to accomplish his mission."

IPB MODIFICATIONS FOR STABILITY OPERATIONS AND SUPPORT OPERATIONS

STEP 1: DEFINE THE BATTLEFIELD ENVIRONMENT

F-5. Stability operations and support operations battlefield environments are not contiguous. For example, upon examining the AO assigned by a higher headquarters to an infantry battalion conducting a counterinsurgency operation, the S2 may be concerned about materiel and moral support for the insurgents coming from a refugee community. Although that community and its assets may have no direct ground connection to the battalion AO, activities in this physically separate region may impact insurgent activities and capabilities inside the battalion's AO. In this instance, you might recommend to the commander an AOI that does not include large areas between the AOI and the AO.

F-6. Stability operations and support operations IPB products need a greater level of detail. An excellent example is demographic analysis. In this stage of the IPB process, the S2 and analysts have to make an initial evaluation of what factors make a given population segment important to your mission and how to communicate this to you and your staffs.

F-7. Examine existing databases and collect intelligence needed to continue the IPB process. The significant difference is that many of those databases will be from open sources and cannot be tapped through normal intelligence channels. Often answers to basic questions of culture, history, and the perceptions they produce can be found by doing a little research using the nearest library or quality book store, in academic journals, and by going online and performing searches by topic, region, and country.

F-8. The intelligence community faces a challenge to produce timely, relevant, and updated reports on regions and issues of sporadic military interest. The academic community, travel industry, and international commercial activities study international regions daily. Their reports and assessments of local sentiments, current cultural taboos, and receptiveness to strangers, for example, are widely published and updated frequently. Rather than await an eventual response to an RFI on these basic intelligence issues, these nontraditional sources give you the information now.

STEP 2: DESCRIBE THE BATTLEFIELD'S EFFECTS

F-9. Revise your thinking for a new battlefield. As with the term "enemy," stability operations and support operations are often not conducted on anything resembling a battlefield. The environment may be lethal, and is usually challenging, but often does not look like a battlefield. Determine how the environment impacts everyone relevant to your operation. In recent years, we have relearned lessons of how civilians on the battlefield can add to the friction of battle and some attempts have been made to account for them. Primarily, these efforts take the form of plans to get refugees and others out of the way of the fighting, both to remove them from possible harm and to reduce the impact on our operations.

F-10. In a stability and support environment, the number and importance of population groups that could have important effects on the commander's mission expands. Classifying them all as civilians on the battlefield is not adequate. Even attempting to classify them as friendly, hostile, or neutral is only a start. For example, neutral refugees seeking relief supplies could spell disaster for an NEO if they flood helicopter LZs. With no hostile intent, they could make air extraction impossible as they head to the sound of rotors—a sound often associated with delivery of relief supplies. Clans or factions that express pro-US sentiments could violently attack relief workers if they assist their clan's perceived enemies. US forces could then become drawn into a larger, standing conflict as they attempt to defend the relief workers.

F-11. In this environment, your staff must do more than list and categorize groups. They must assess the goals and motivations of the groups, their leadership (or lack thereof), their beliefs, and their power bases. From all of these possibly important factors for further analysis, S2s must narrow the list to those with a direct effect on the commander's mission and his ability to accomplish it. The limited time, soldiers, and equipment available to S2s require focusing on the most important issues for detailed analysis.

STEP 3: EVALUATE THE THREAT

F-12. Evaluating the threat was once the easiest part of the IPB process; today, this step is more difficult. The threats are often not regular armies with well-defined doctrine and OB. Even during Operation DESERT STORM, against a threat the intelligence community thought it understood well, the threat did not fight as their doctrine said they would. In the final analysis, threats do the same thing US forces do—they use the means at their disposal to achieve their desired endstate. Cultural factors and economic and training restraints impact operations. Commander personalities also play an important

role. In the end, however, forces apply assets available to achieve what they want to accomplish and your S2 must take all of this into account. Conducting this step of IPB relies on the assessment of the threat's objective, and subsequent threat tactics are based on details of the specific operational environment in consideration.

F-13. Brigades and battalions depend on tactics descriptions, representative vignettes of threat activities, and modified templates packaged as threat models from higher headquarters. By applying basic operational principles to these skeletal products, S2s can modify threat models and assess preferred methods of operation for a given threat peculiar to your operation. By refining all of these, the staff produces a threat picture, which then can be turned into doctrinal templates and sketches. The important difference between these end products and what S2s received in the past is the amount of increased analysis required to turn the information into something useful for your planning and decisionmaking.

STEP 4: DETERMINE THREAT COAs

F-14. The S2 will begin by defining the likely threat objectives and developing threat COAs, bearing in mind that all threat COAs must be considered. The S2 will use the same procedures and tools he uses in conventional IPB (situaton templates, event templates, and event matrixes) to support his threat COA analysis.

F-15. The situation templates will graphically depict the threat's expected disposition should the threat adopt a particular COA. To construct a situation template, the S2 overlays the doctrinal template produced in step 3 on the environmental templates (to include the MCOO) developed in step 2. The threat is then adjusted on the doctrinal template to allow for the effects of the environment. Due to the potential complexity of a stability and support environment, some situation templates may be more suited to present in a matrix format.

F-16. The S2 will use event templates as guides for intelligence collection and ISR planning. These templates will depict where and when to collect the threat information. Some of the NAIs on the event template indicate the COA the threat will adopt. Consider the following when determining threat COAs relative to stability operations and support operations:

- A wider range of actions available to the threat.
- Historical, demographic, and cultural information is of importance in developing possible actions.
- The full set of unique COAs available to the threat.
- Objectives and COAs over a longer period of time.
- The threat will quickly incorporate lessons learned.
- Long-term political objectives; what the threat is willing to commit to at various stages.
- Imagery at a scale of 1:10,000 to 1:25,000 to accurately display detailed characteristics of the terrain.

URBAN OPERATIONS CONSIDERATIONS

F-17. Urban operations are a perfect example of a unique environment. Intelligence collection within the urban operations can be a complex and time-consuming process. Normally, your S2 must quickly focus on the key elements of the environment. The use of an abbreviated analytical process has the advantage of bringing environmental details into the IPB process. It also lays the groundwork for a more detailed analysis later as your operation matures.

F-18. Urban operations have an increased number and potential combination of variables. For example, an infantry battalion operating in a city's industrial park may not only encounter the threat during seasonal rains but also encounter flooding as well. Flooded buildings may in turn be full of damaged storage tanks that leak hazardous waste materials into the water. The battalion could suffer more casualties from the hazardous waste than from direct combat. In the confines of the urban environment there may be literally nowhere for the unit to go, and the situation will have to be addressed by a combination of combat, engineer, and chemical units.

F-19. Because of the diversity in the urban environment, your S2 may have difficulty identifying a starting point. The framework in Figure F-1 is a way for your S2 to start. It is a tool designed to facilitate an urban operation assessment and subsequently support your MDMP. The framework is structured around eleven steps, which may also be considered layers of the whole assessment. Your staff must address the first layer before reaching the second layer, and the third layer, and so on.

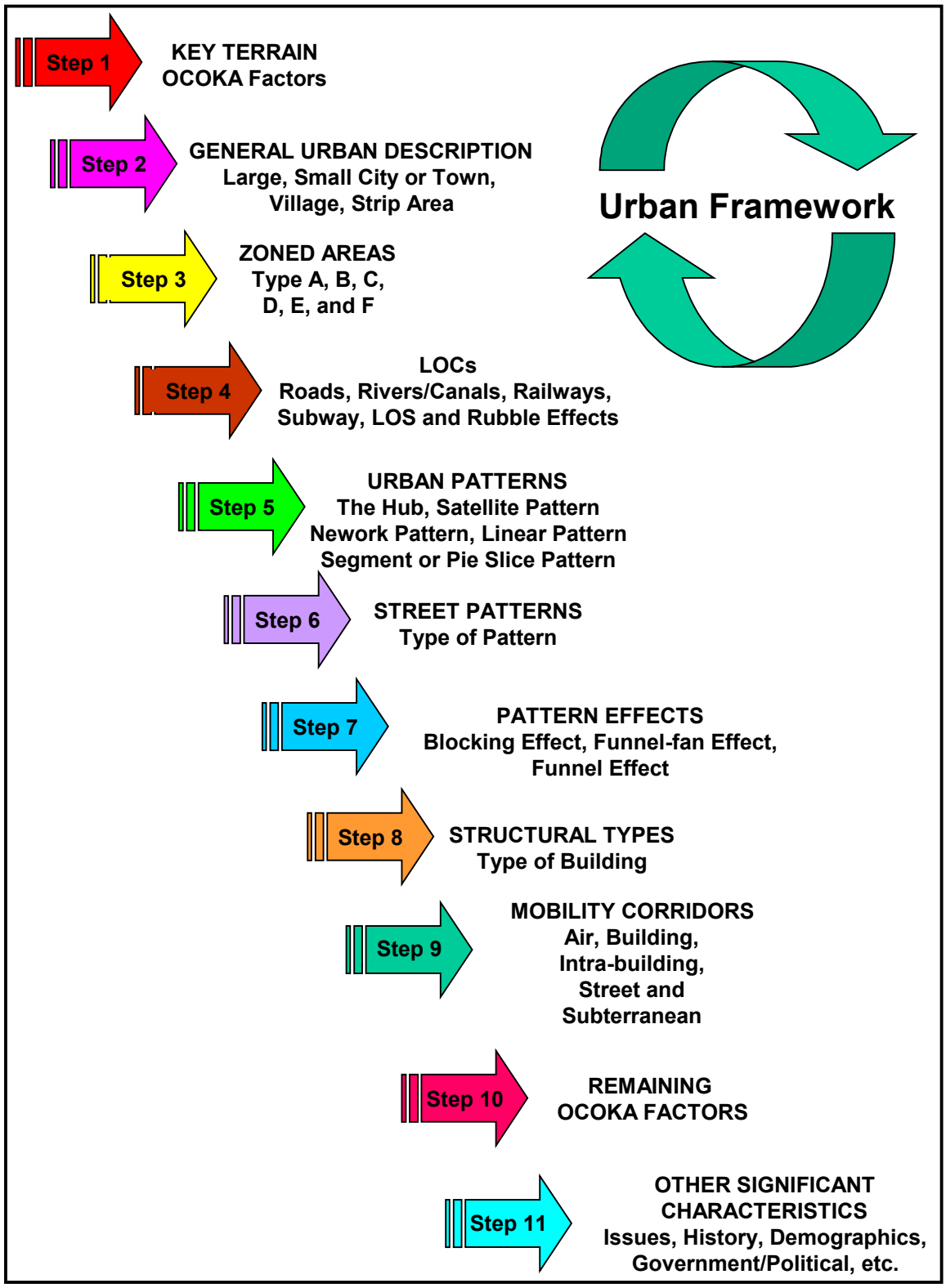


Figure F-1. Urban Operations

GLOSSARY

A

AC	Active Component
ACE	analysis and control element
ACR	armored cavalry regiment
ACT	analysis and control team
ADA	air defense artillery
ADRG	Arc Digitized Roster Graphics
AEB	aerial exploitation battalion
AG	advance guard
AGMB	advance guard main body
AO	area of operation
AOI	area of interest
ARFOR	Army force
ARL-M	airborne reconnaissance low-multifunction
ASARS	Advanced Synthetic Aperture Radar System
AT	anti-tank
ATGM	anti-tank guided missile
ATK	attack
attrit	attrition

B

BCT	brigade combat team
BDA	battle damage assessment
BLUFOR	Blue forces
BMP	infantry fighting vehicle (Soviet origin)
BN	battalion
BOS	battlefield operating system
BP	battle position
BRDM	infantry fighting vehicle (Soviet origin)
BTRY	battery

C

C^2	command and control
C^3	command, control, and communications
CA	Civil Affairs
CATK	counterattack
CCIR	commander's critical information requirements
CFSO	counterintelligence force protection source operations
CGS	common ground station
C-HUMINT	counter-human intelligence
CI	counterintelligence
CMF	career management field
co	company
CofS	Chief of Staff
COMINT	communications intelligence
COP	common operational picture
CO/TM	company/team
COA	course of action

CRP	combat reconnaissance patrol
CS	combat support
CSS	combat service support
CWT	combat weather team

D

DA	Department of the Army
DF	direction finding
DLPT	Defense Language Proficiency Test
DOCEX	document exploitation
DOD	Department of Defense
DP	decision point
DRT	dismounted reconnaissance team
DS	direct support
dsmt	dismount
DST	decision support template
DTED	digital terrain elevation data
DZ	drop zone

E

EA	electronic attack
EEFI	essential elements of friendly information
EENT	end of evening nautical twilight
ENY	enemy
E-O	electro-optical
EP	electronic protection
EPW	enemy prisoner of war
ES	electronic warfare support
ELINT	electronic intellligence
EW	electronic warfare
EWO	electronic warfare officer
EWTL	electronic warfare target list

F

FA	field artillery
FASCAM	family of artillery scatterable mines
FSCOORD	fire support coordinator
FD	forward detachment
FFIR	friendly forces information requirments
FIS	foreign intelligence services
FISINT	foreign instrumentation signals intelligence
FLOT	forward line of own troops
FRAGO	fragmentary order
FSE	fire support element
FSO	fire support officer
FWD	forward

G

GD	advance guard
GRCS	GUARDRAIL common sensor

GS	general support
GSR	ground surveillance radar

H

H	hour
HN	host nation
HPT	high payoff target
HPTL	high payoff target list
HQ	headquarters
HUMINT	human intelligence
HVT	high value target
HVTL	high value target list

I

IBCT	initial brigade combat team
I&W	indications and warnings
IEW	intelligence and electronic warfare
IMINT	imagery intelligence
inf	infantry
IO	information operations
IPB	intelligence preparation of the battlefield
IR	information requirements
ISM	intelligence synchronization matrix
ISR	intelligence, surveillance, and reconnaissance

J

Joint STARS	Joint Surveillance Target Attack Radar System
JTF	joint task force

K

km	kilometer

L

LOC	lines of communication
LRS	long-range surveillance
LTIOV	latest time information is of value
LZ	landing zone

M

MASINT	measurements and signature intelligence
MCOO	modified combined obstacle overlay
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops, time available and civilians
MFR	memorandum for record
MI	military intelligence
MOD	mobile obstacle detachment
MOS	Military Occupational Specialty

MRB	motorized rifle battalion
MRD	motorized rifle detachment
MRR	motorized rifle regiment
MSR	main supply route

N

N	north
NAI	named area of interest
NBC	nuclear, biological, and chemical
NE	northeast
NEO	noncombatant evacuation operation
NP	nonpresistant (chemicals)
NRT	near-real time

O

OB	order of battle
OBJ	objective
OCOKA	observation and fields of fire, concealment and cover, obstacles, key terrain, avenue of approach
OMT	operational management team
O/O	on order
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPS	operations
OPSEC	operations security

P

PAO	public affairs office
PCHEM	presistant chemical
PIR	priority intelligence requirements
PL	phase line
POL	petroleum, oils, and lubricants
PSN	position
PSYOP	psychological operations
pt	point
PZ	pickup zone

R

RC	Reserve Components
R&S	reconnaissance and surveillance
recon	reconnaissance
REGT	regiment
REMBRASS	Remotely Monitored Battlefield Sensor System
RFI	request for information
RKH	chemical
RSTA	reconnaissance, surveillance, and target acquisition

S

S	south
S&TI	scientific and technical intelligence
SBF	support by fire
SIDPERS	Standard Installation Division Personnel System
SIGINT	signals intelligence
SIR	specific information requirement
SOFA	Status of Forces Agreement
SOR	specific orders and requests
SPT	support
SSO	special security officer
STANAG	standardization agreement (NATO)
STM	standard tactical mission
SWO	staff weather officer

T

TAC	tactical command post
TAI	target area of interest
TDAM	tank division
TEB	tactical exploitation battalion
TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities
TF	task force
TGT	target
tm	team
TOC	tactical operations center
TROJAN Spirit	Special Purpose Intelligence Remote Integrated Terminal
TTP	tactics, techniques, and procedures

U

UAV	unmanned aerial vehicle
UTP	urban tactical planner
U2R	Advance Synthetic Aperture Radar

V

vic	vicinity

W

W	west
WARNO	warning order
WMD	weapon of mass destruction
wpns	weapons

X

XO	executive officer

REFERENCES

FM 2-0 (FM 34-1)	Intelligence and Electronic Warfare Operations, 27 Sep 94
FM 2-01.3 (FM 34-130)	Intelligence Preparation of the Battlefield, 8 Jul 94
FM 3-0/FM 6-0 (FM l00-5)	Operations
FM 34-5(S)	Human Intelligence and Related Counterintelligence Operations, 29 Jul 94
FM 2-22.3 (FM 34-52)	Intelligence Interrogation, 28 Sep 92
FM 2-50.1 (FM 34-25-1)	Joint Surveillance Target Attack Radar System, 3 Oct 95
FM 3-55.1 (FM 34-25-2)	
FM 2-00.10 (FM 34-10-1)	Tactics, Techniques, and Procedures for the Remotely Monitored Battlefield Sensor System (REMBASS), 18 Jun 91
FM 2-01.2 (FM 34-60)	Counterintelligence, 3 Oct 95
FM 3-34.330 (FM 5-33)	Terrain Analysis, 11 Jul 90