FM 34-45

Tactics, Techniques, and Procedures

ELECTRONIC ATTACK

HEADQUARTERS, DEPARTMENT OF THE ARMY

FM 34-45

Field Manual
No. 34-45

Headquarters
Department of the Army
Washington, DC, 9 June 2000

TACTICS, TECHNIQUES, AND PROCEDURES FOR ELECTRONIC ATTACK

Contents

*This publication supersedes FM 34-40-7, 23 November 1992.

Page

Page

PREFACE

The purpose of this manual is to—

- Address the deployment and employment of electronic attack (EA) assets at division and brigade.
- Discuss concepts and principles unique to EA.
- Describe how to integrate EA into the targeting effort.
- Address specific tactics, techniques, and procedures (TTP) when applicable.

This manual is a guide for Army commanders, staffs, and operators who plan and/or execute EA. It applies equally to the Active Component (AC), US Army Reserve (USAR), and Army National Guard (ARNG).

This manual complies with FM 34-1 and is consistent with current joint doctrine. It assumes the user has a fundamental understanding of the doctrine in FM 100-5, FM 101-5, FM 34-1, FM 6-20-10, and FM 34-130.

The proponent for this publication is Headquarters, US Army Training and Doctrine Command (TRADOC). Send comments and recommendations on DA Form 2028 directly to Commander, US Army Intelligence Center and Ft Huachuca, ATTN: ATZS-FDC-D, Ft Huachuca, AZ 85613-6000.

This manual does not implement any International Standardization Agreements.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

Operations and Electronic Warfare

Division targeting teams and electronic warfare (EW) personnel work together to ensure that EW is integrated into targeting, is thoroughly planned, and is vigorously executed. The use of standard EW targets without thorough analysis and planning significantly limits the potential of EW as a true combat multiplier. Inadequate planning leads to the uncoordinated use of EW and limits the effects of both EW and fire support (FS) as a whole. On the other hand, if EW is adequately staffed, trained, integrated into targeting, planned, and executed, it helps the commander reach his targeting objectives by dominating the electromagnetic environment (EME).

EW can attack the threat when it is most vulnerable through a quick, accurate, timely, and responsive means that can also provide a fast assessment of the operation. Additionally, EW is important because it is a responsive tool to perform suppression of enemy air defenses (SEAD); it is also one of the integrated tools used to conduct information operations (IO). However, EW is effective only when the commander decides there is more value in conducting EA (for a specific high-payoff target [HPT] at a specific point) than performing additional collection in order to produce more intelligence.

THE POTENTIAL

1-1. The potential for EA is unlimited especially within the information age.

- **Offensive** operations often provide the friendly forces the element of surprise. Prior to units crossing the line of departure (LD), EA assets begin their missions. EA may focus on the scout or reconnaissance net to ensure intelligence indicating friendly forces attacking is not passed to the threat command post (CP). As units begin to engage the threat, EA assets then shift their effort onto the threat's counterbattery, command and control (C^2), and artillery. The suppression of these targets denies the enemy the ability to effectively control his forces and also disrupts the flow of information to his artillery and counterbattery, thus rendering them useless. At this point, EA systems engage specific targets. A unit near a bridge that was destroyed is jammed to prevent the requesting of engineer support. This will cause a delay in maneuvering an enemy unit that would protect a vulnerable flank.

- **Defensive** operations, conducted with the immediate purpose of causing an enemy attack to fail, often allow the friendly force to close off areas and create devastating engagement areas while denying the threat critical information. EA assets cover constricted terrain areas along the threat avenue of approach (AA). The engineers erect obstacles in order for maneuver and artillery units to create an engagement area. EA assets begin their mission as soon as the threat enters the area and no longer has direct contact with other units. At this time units engage with artillery and destroy threat forces. Because the threat has no communications, the engagement will be swift, with high casualties and lost momentum, thus ending the threat attack. EA also will be used in counterreconnaissance to deny threat scouts the ability to pass vital intelligence back to their commander.

METHODOLOGY

1-2. There is not a separate methodology to conduct EW. The best way to conduct EW is to effectively integrate EW within the targeting methodology and TTP. This manual and the flow of products are in accordance with FM 6-20-10. They provide a clear and relatively simple framework, terminology, and TTP to plan and conduct EA as a subset of EW. The framework begins with the targeting functions of DECIDE, DETECT, DELIVER, and ASSESS.

THE ENVIRONMENT

1-3. Operations are executed in an increasingly complex EME. Almost all military units use electromagnetic (EM) devices for communications, navigation, sensing, information storage, and processing. The increasing mobility and affordability of sophisticated EM equipment guarantees that the environment will become even more complex in the future. This environment creates vulnerabilities to and opportunities for EW for both friendly and threat forces. The threat and the friendly commanders depend on this flow of information to make informed decisions. EW can exploit this dependence. Appendix A further describes this environment.

1-4. The need to control the EM spectrum and the type of EW actions that can be used to control that spectrum depend on the operational environment. During peacetime, government bodies and international treaties and conventions control the use of the EM spectrum. However, standing rules of engagement (ROE) give joint commanders the authority in peacetime to take appropriate and necessary action to protect their forces. The type and level of EW actions appropriate to a particular operation depend on threat capabilities, threat vulnerabilities, and operational objectives.

ELECTRONIC WARFARE

1-5. EW includes three major subdivisions: electronic protection (EP), electronic warfare support (ES), and electronic attack (EA). EW is waged (through the use of EM or directed energy) within the EM spectrum to—

- Secure and maintain effective control and use of the spectrum for friendly forces.
- Attack the threat and to deny the use of the spectrum through damage, destruction, disruption, and deception.

ELECTRONIC PROTECTION

1-6. EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of EW that degrade, neutralize, or destroy friendly combat capability. This manual contains very little discussion of this subdivision of EW.

ELECTRONIC WARFARE SUPPORT

1-7. ES involves the search for, intercepts, identification, and location of sources of radiated EM energy (intentional and unintentional) in order to recognize and collect information on the threat. ES provides information necessary for immediate decisions involving EW operations and other tactical actions. Both EA and ES are critical and mutually supportive components.

ELECTRONIC ATTACK

1-8. EA involves the use of EM, directed energy (DE), or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered to be a form of fires. EA includes—

- Taking actions to prevent or reduce an enemy's effective use of the EM spectrum (for example, jamming and EM deception).
- Employing weapons that use either EM or DE to destroy EM equipment (for example, lasers, radio frequency [RF] weapons, or particle beams).

First Recorded Instance of Deliberate Radio Jamming

The first recorded instance of deliberate radio jamming took place in September 1901 in the US. Interestingly, it was aimed at securing commercial gain rather than military advantage. As now, there was considerable public interest in the America's Cup yacht races, and the newspaper first to reach the stands carrying each result stood to reap a large profit.... A third company...failed to get a sponsor but...used a transmitter more powerful than its competitors, and one of its engineers, John Pickard, worked out a method which allowed him to jam signals from the other companies while at the same time to report on the progress of the race from his boat.

Source: The History of US Electronic Warfare, Volume I

TACTICAL ELECTRONIC ATTACK

1-9. EA is best used as a combat multiplier in conjunction with other fires into an engagement area. Used alone, EA is only a delaying or disrupting fire—its effects are reduced. Additionally, the technique of using EA fires independently of other fires provides the enemy time and training to overcome the effects of future EA. While EA operations within a theater or joint task force area of operation (AO) are often complicated, tactical EA operations (to include division operations) are relatively simple.

1-10. The scope of tactical EA operations are limited by doctrine, organic and supporting capabilities, and realistic unit standing operating procedures (SOPs). However, when a tactical echelon lacks adequate organic or supporting capabilities, it can request support from a higher echelon. Sometimes a tactical echelon might not even know of an existing capability at a higher echelon. The US Air Force (USAF), US Marine Corps (USMC), and US Navy (USN) have the EA equipment for the SEAD. With the Army's dependence on aviation assets, the request for support from echelons above corps (EAC) in the joint arena for SEAD support will remain constant.

CURRENT AND FUTURE THREAT ELECTRONIC WARFARE CAPABILITIES

1-11. While allied forces are able to conduct EA, many threats, using off-the-shelf equipment, have the ability to conduct EA with greater distance and against targets conventionally safe against EA. The current communications environment provides many potential threats with a rich environment to conduct EW and exploit friendly communications. The more a unit relies on communications, the more vulnerable that unit is to threat ES and EA. In general, many threats currently have the capability to—

- Detect and locate friendly units because of our use of EM equipment.
- Monitor and exploit friendly unit's communications to include collecting information on a unit's mission, combat strength, logistics, morale, weakness, and other critical information.
- Deny a friendly unit's use of the EM spectrum, thereby degrading that unit's ability to plan operations, execute C^2, receive and process intelligence, and execute operations.

1-12. The future communications environment will provide threats with a target-rich environment for EW. In general, future threats will be able to—

- Detect, locate, and jam low probability of intercept (LPI) signals. The Army currently uses many types of LPIs (for example, Single-Channel Ground and Airborne Radio System [SINCGARS]).
- Use DE to destroy computer networks by using electromagnetic pulses (EMPs) to destroy silicon chips inside equipment.
- Use electronic deception to enter and control friendly voice and data nets.

Chapter 2

Electronic Attack in Information Operations

IO are actions taken to affect adversaries and to influence other audiences' military decisionmaking policies (MDMPs), information, and information systems, and defend friendly MDMPs, information, and information systems. EW is an integral part of IO; consequently, EA is closely tied to IO planning, integration, and execution.

INFORMATION OPERATIONS

2-1. IO consist of two supporting elements: offensive IO and defensive IO.

OFFENSIVE OPERATIONS

2-2. Offensive IO are the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers or to influence neutral audiences to achieve or promote specific objectives. The capabilities and activities include, but are not limited to, operations security (OPSEC), military deception, psychological operations (PSYOP), EW, physical destruction, special information operations, and computer network attack (CNA).

DEFENSIVE OPERATIONS

2-3. Defensive IO are the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems. Defensive IO are conducted through information assurance, physical security, OPSEC, counter-deception, counter-propaganda, counterintelligence, EW, and special IO.

2-4. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purpose. Although they are not integral components of IO, public affairs and civil affairs are enabling activities that may contribute in the execution of IO tasks and promote attaining specific IO objectives.

INFORMATION SUPERIORITY

2-5. The goal of Army IO is to achieve information superiority. Information superiority is a window of opportunity created by a focused effort that allows the actions or beliefs of the enemy commander to be influenced in support of decisive operations. It can be gained by the integration and synchronization of information management and IO. Information management is the directing of relevant information to the right person at the right time in a usable format to facilitate decisionmaking. It uses procedures and

information systems to collect, process, store, display, and disseminate data and information. (See Figure 2-1.)

2-6. One of the friendly commander's IO instruments to achieve or promote specific objectives is EW. EA is a valuable offensive IO tool. When planned, coordinated, synchronized, and integrated with the friendly FS plan, EA becomes a combat multiplier. EA can effectively confuse the threat and disrupt the threat commander's operation. The only difference between traditional EA planning and EA in support of IO involves the specific IO objectives and targets. Specific IO objectives may differ significantly from tactical military objectives. Additionally, the commander may use EA in support of IO and/or solely to complement supporting activities of IO. IO targets may include, but are not limited to, adversary perceptions, knowledge, personnel, equipment, information systems networks, or population.

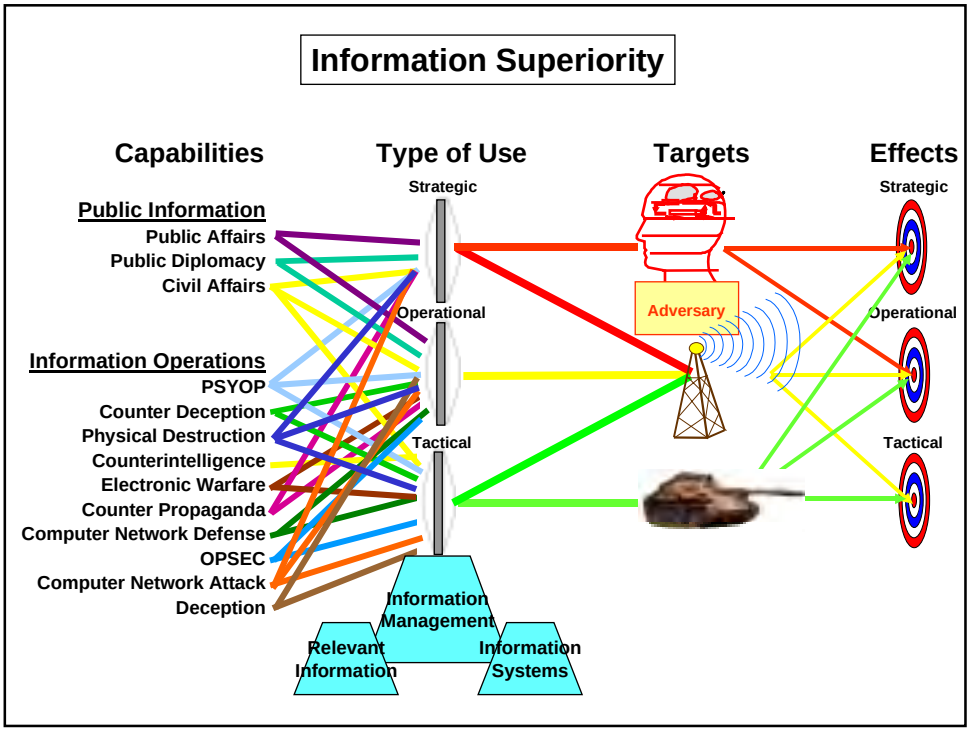


Figure 2-1. Information Superiority

2-7. The planning, coordination, and execution of electronic fires remains consistent with the same methodology (Decide, Detect, Deliver, and Assess) described in FM 6-20-10. During the DECIDE phase, the IO cell brings unique IO HVTs into the wargaming process. This results in unique IO HPTs that are integrated with all HPTs into the attack guidance matrix (AGM). The electronic warfare officer (EWO) provides the IO cell feedback on the outcome of EA, so that the IO cell can decide whether or not to nominate the target for reattack. Due to the nature of IO, however, feedback may not

be immediate and it may require a significantly longer period to make an assessment.

2-8. Successful application of EA in IO depends on IPB. Once the targets are identified, developed, and integrated in the targeting process, EA is applied as an effective IO tool. EA is synchronized and applied in conjunction with other IO elements and supporting activities to maximize the effect of these operations.

Chapter 3

Electronic Attack in Targeting: Key Personnel, Organizations, and Coordination

Targeting is the process of selecting targets and matching the appropriate response to them on the basis of operational requirements and capabilities. The DECIDE, DETECT, DELIVER, and ASSESS methodology directs friendly forces to attack the right target with the right asset at the right time.

The targeting process provides an effective method for matching the friendly force capabilities against a threat's targets. Another important part of the targeting process is to identify potential fratricide situations and perform the coordination necessary to positively manage and control the targeting effort. The targeting team and staff incorporate these measures into the coordinating instructions and appropriate annexes of the operations plans (OPLANs) and/or operations orders (OPORDs).

Targeting is a dynamic process; it must keep up with the changing face of the battlefield. The staff must continually update the tools and products described in this manual based on changing plans, situation development, and combat assessment. As a participant in the staff targeting process, the EWO ensures that EA is thoroughly integrated within targeting. This includes integrating EA into all the appropriate annexes and products.

ELECTRONIC ATTACK IN THE TARGETING METHODOLOGY

3-1. The modern battlefield presents many targets with different vulnerabilities exceeding the number of resources available to acquire and attack them. The commander must determine which targets are most important to the threat and, of those targets, which ones he must acquire and attack to accomplish his mission. Then as the operation unfolds friendly forces must identify, track, engage, and assess the results on priority threat targets.

DECIDE

3-2. DECIDE, as the first step in the targeting process, provides the overall focus, a targeting plan, and some of the priorities for intelligence collection. The targeting team must plan targeting priorities for each phase and critical event of an operation. Initially, the targeting team does not develop EA targets using any special technique or separately from targets for physical

destruction. However, as the process continues these targets are passed through intelligence organizations and further planned using collection management (CM) procedures. The EA plan (from DECIDE) is integrated into the standard targeting products (graphic or text-based). Some of the most critical products that involve EA are the—

- High-payoff target list (HPTL).
- AGM.
- EW annex.

3-3. Different personnel and organizations perform five processes as part of or in conjunction with the MDMP in order to plan EA:

- Intelligence Preparation of the Battlefield (IPB).
- Target Development.
- Requirements Management (RM).
- Mission Management (MM).
- Asset Management (AM).

DETECT

3-4. DETECT is a critical function in the targeting process. ES and EA assets deploy to detect HPTs (based on what the targeting team identified as HPTs during DECIDE). The intelligence operating system cross-queues assets based on a collection plan and the threat situation. It is critical that ES assets are deployed and work closely with EA assets. In order for EA assets to effectively perform EA, they need critical data like the location, signal strength, and frequency of the HPT. ES assets will find the "weak link" (with the support of the target assessment and signals intelligence [SIGINT] teams) in threat communications that the EA asset can attack.

DELIVER

3-5. DELIVER is the execution of EA against the targets identified in the HPTL, AGM, and EW annex once friendly forces identify, locate, and track HPTs. EA assets must satisfy the attack guidance developed during DECIDE. Executing EA requires close coordination between ES and EA assets when the EA asset is jamming the HPT. Recommend EA assets use maximum power based on mission, enemy, terrain and weather, troops, and time available-civilians (METT-TC). The commander makes the ultimate decision on how much power EA assets will use to accomplish the mission. Essential to this is the synchronization of lethal fires and nonlethal fires (EA). This synchronization is accomplished through AGMs, intelligence synchronization matrixes (ISMs), and EW annexes.

ASSESS

3-6. Combat assessment (CA) is the determination of the effectiveness of force employment during military operations. CA is composed of three elements:

- Munitions effects assessment (MEA).

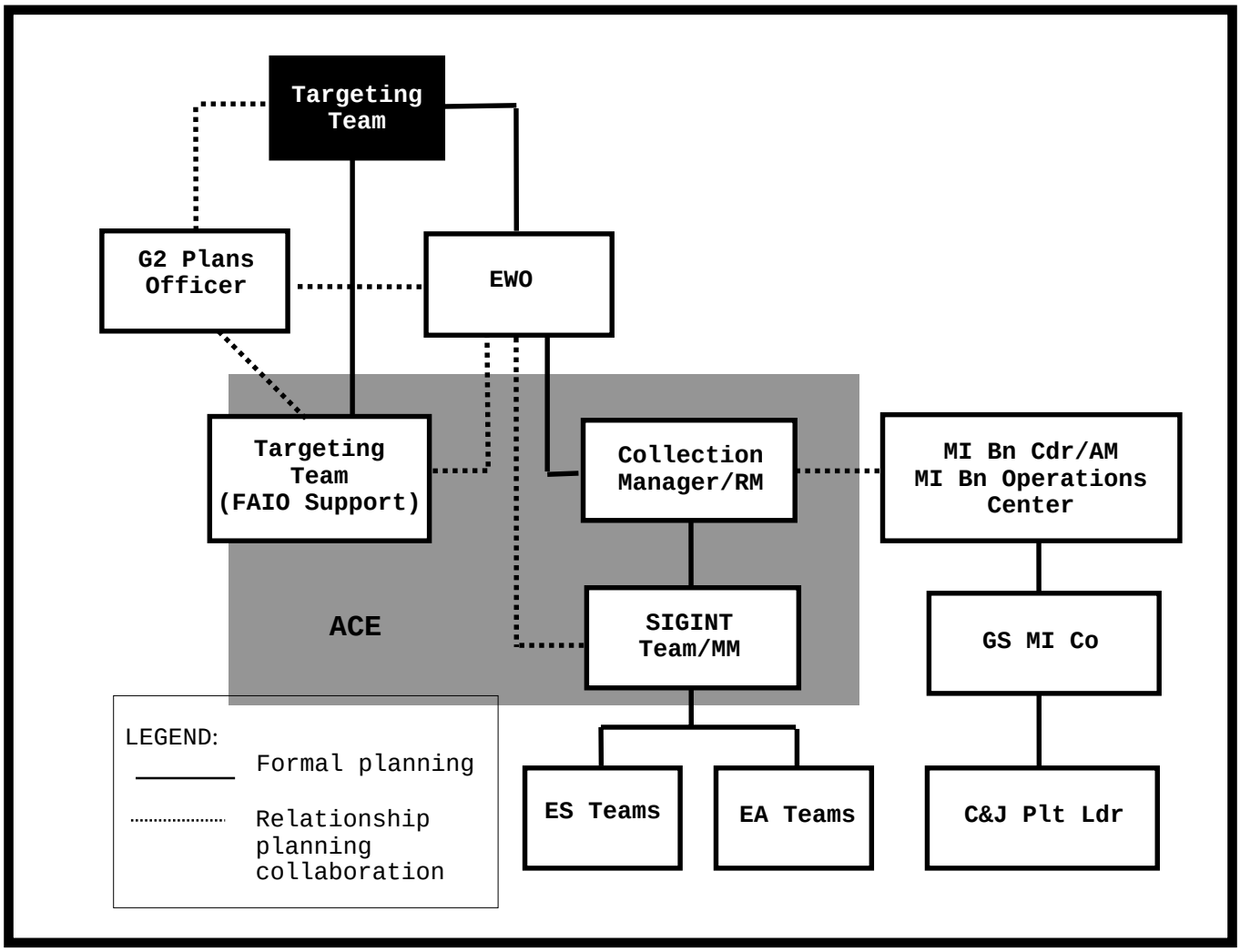
- Battle damage assessment (BDA).
- Reattack recommendations.

3-7. MEA and BDA (when combined by the staff) inform the commander of effects against targets and target sets. Based on this information, the G2 continually analyzes the threat's ability to conduct and sustain operations (sometimes expressed in terms of the threat's centers of gravity). The bottomline is to either recommend reattack or not. The specific assessment of EA involves all three of the elements of CA as an integrated part of the targeting effort. One unique part of MEA for EA is the close coordination between ES and EA assets necessary to perform an operator evaluation (based upon the jamming effectiveness).

3-8. BDA is the timely and accurate estimate of damage resulting from the application of military force (either lethal or nonlethal) against a target. BDA in the targeting process pertains to the results of any attack. Producing BDA is primarily an intelligence responsibility, but requires coordination with operational elements to be effective. BDA requirements may be translated into priority intelligence requirements (PIR) or information requirements (IR) if it is linked to the commander's decisions. The G2 answers BDA requirements by providing the commander a series of timely and accurate “snapshots” of the effects on the threat. The “snapshots” include an estimate of the threat's combat effectiveness, capabilities, and intentions. This helps the commander determine if their targeting effort is accomplishing their objectives and if reattack is necessary.

KEY ELECTRONIC ATTACK PERSONNEL AND ORGANIZATIONS

3-9. The main CP is the critical location that plans and, to a large extent, controls EA for division operations. This CP is functionally organized to support the coordination needed to synchronize targeting (EA is thoroughly integrated within these operations). Tailoring the structure and relationship of the staff sections is necessary to ensure a cohesive coordinated targeting effort. Figure 3-1 shows the key EA personnel and organizations.



THE COMMANDER

3-10. The commander issues guidance on the concept of operations for close, deep, and rear operations as well as for future operations. He defines the mission, the concept of operations, his intent, and supporting tasks. His intent and targeting objectives guide the actions of the targeting team.

TARGETING TEAM

3-11. The targeting team is an ad hoc organization, which is driven by mission. Generally, the team will consist of the Deputy Fire Support Coordinator (FSCOORD), Air Liaison Officer (ALO), EWO, and representatives from the G2, G3, Air Defense Artillery (ADA), Engineers, and Army Airspace Command and Control (A^2C^2) element. The G3 adds additional members as necessary (for example, Deception, PSYOP, Civil Affairs, or IO).

3-12. Targeting team members go through the target list and decide (with the guidance of the G3 representative) which targets to attack and with what

type of fire (lethal and nonlethal). This task includes requesting support from higher echelons (for example, coordinating USAF support through the Battlefield Coordination Detachment (BCD) at the Air Operations Center [AOC]). The chief of staff is responsible for supervising the targeting processes, chairing targeting meetings, and leading the targeting team. The targeting team—

- Develops HPTs from the high-value targets (HVTs).
- Works with the G2 to perform target development.
- Develops the HPTL, AGM, and BDA requirements.
- Updates these products as the situation changes.

3-13. The Deputy FSCOORD is a key player in the targeting team. He provides the latest status of FS resources and plans their use in support of the operation. Specifically, he—

- Coordinates the functions of the targeting team.
- Recommends methods of attack for HPTs.
- Develops timelines and accuracy guidelines for the target selection standards (TSSs) (in coordination with the G2 section).
- Monitors changes in the situation and reassesses the HPTL, AGM, TSSs, and BDA requirements.
- Coordinates subordinate units' attack requirements.
- Receives BDA and determines if the desired effects were achieved or if additional attacks are required (with the G2 and G3).
- Ensures the air tasking order (ATO) supports target nomination in accordance with SOPs.

G2 PLANS OFFICER

3-14. The G2 Plans Officer—

- Maintains HVTs (with the targeting team analysis and control element [ACE] and field artillery intelligence officer [FAIO]).
- Uses the targeting team ACE to template potential HPTs.
- Recommends named areas of interest (NAIs) and target areas of interest (TAIs) to the G2 to support targeting.
- Coordinates with the collection manager to ensure adequate intelligence collection to support the targeting plan.

ELECTRONIC WARFARE OFFICER

3-15. The EWO—

- Helps the targeting team determine EA requirements against specific HPTs.
- Ensures EA can meet the targeting effect (in terms of the targeting objective).

- Coordinates with the SIGINT team (ACE) through the collection manager to satisfy ES and EA requirements.
- Prepares the EW annex.
- Provides EA MM for the division.
- Prepares and coordinates the EW annex for OPLANs and OPORDs.
- Determines and requests EAC EA support.
- Recommends to the G3/G2 whether a target should be engaged with EA.
- Expedites meaconing, intrusion, jamming, and interference (MIJI) reports to the ACE for targeting.

ANALYSIS AND CONTROL ELEMENT

3-16. The ACE provides support for EA missions through the collection manager, SIGINT team, targeting team, all-source team, and FAIO. This organization fuses intelligence to identify the best target inside a target set.

COLLECTION MANAGEMENT TEAM (ACE)

3-17. This team—

- Passes specific information requirements (SIR) that support EW to the SIGINT team.
- Works with the EWO, MI battalion, and SIGINT team to ensure that the collection plan and ISM are synchchronized with the AGM and EW annex.
- Either develops EW tasking for organic or supporting EW assets or requests EW support from a higher echelon (with the EWO and SIGINT team).

TARGETING TEAM (ACE)

3-18. This team—

- Interacts with the G2 Plans Officer, the FAIO, and the EWO to support EA as an integrated part of target development and targeting.
- Produces and compares target overlays to IPB products and current intelligence. (NOTE: This is a critical part of critical nodes analysis.)
- Nominates HPTs in support of the G2 Plans Officer.

FAIO

3-19. The FAIO—

- Collocates with the ACE specifically near the targeting team (ACE), collection management team, and all-source team.
- Supports the G2 Plans Officer (as necessary).
- Supports the targeting team (as necessary).
- Provides input concerning the threat, TSSs, attack guidance, and list of HPT types (as necessary).

- Is the threat artillery expert in the ACE.
- Provides feedback to the ACE, the targeting team, and artillery BDA via the division artillery S2.

SIGINT TEAM

3-20. This team—

- Identifies and tracks targets (to include EA targets).
- Performs MM and controls EA to include tasking EA and ES assets.
- Provides technical data to the ES and EA assets.
- Provides graphic depictions of line of sight (LOS) and threat target emitters.

DIVISIONAL MI BATTALION

3-21. The divisional MI battalion is responsible for conducting EW operations within the framework of the division commander's intent. To facilitate its mission, the G2 section provides the MI battalion the HPTL, AGM, EW annex, and the collection plan. The MI battalion is responsible to deploy the ES and EA assets and to provide training, maintenance, logistics, and AM. These ES and EA assets normally operate in general support (GS) to the division.

MI BATTALION COMMANDER

3-22. The MI battalion commander plans and directs the employment of his subordinate intelligence and intelligence and electronic warfare (IEW) assets. The commander—

- Coordinates with the G2, G3, and collection manager.
- Acts as the asset manager. Employs assets in accordance with the OPORD (to include the EW annex).

GS MI COMPANY COMMANDER

3-23. The company commander directs the employment of his ES and EA assets. The commander—

- Coordinates with the collection manager for the deployment of ES and EA assets for preplanned missions.
- Provides service support to ES and EA teams.
- Ensures the training of ES, EA, and target assessment teams.
- Conducts signals intelligence/electronic warfare (SIGINT/EW) operations in accordance with tasking.
- Performs rapid SIGINT analysis of collected data to determine which position will conduct tasking.

PLATOON OPERATIONS CENTER

3-24. The platoon operations center (POC) is the control point for ES and EA assets. The POC is comprised of a—

- Transcription and analysis (TA) team.
- Collection and jamming (C&J) platoon leader.

3-25. The POC is collocated with the brigade analysis and control team (ACT) and will assist the ACT in maintaining the enemy situation picture, MM, and AM of ES and EA.

C&J PLATOON LEADER

3-26. The C&J platoon leader is responsible for his ES and EA assets. The C&J platoon leader—

- Coordinates with the G2 and the G3 for movement and secure routes in a GS role. While in a direct support (DS) role coordinates with the commander and/or S2.
- Runs the POC which contains the TA team.
- Ensures that teams are resupplied and that their service support requirements are met.

EA TEAM

3-27. EA teams provide operators and equipment to perform the actual EA mission. They—

- Orient on targets and conduct EA.
- Monitor targets when tasked by the SIGINT team.

ES TEAM

3-28. ES teams provide operators and equipment to perform ES mission. They—

- Cue EA systems to targets.
- Develop targets for EA.
- Perform direction finding (DF) of targets for orientation of EA systems.

KEY ELECTRONIC ATTACK COORDINATION

3-29. The EWO coordinates with the following key staff members in order to plan and execute EA.

3-30. The G6—

- Performs spectrum management to include deconflicting EA (in the form of the restricted frequency list [RFL]).
- Coordinates closely with the Chief of Staff, G3, and other targeting team members to help develop the targeting plan.

DEEP OPERATIONS COORDINATION CELL

3-31. The Deep Operations Coordination Cell (DOCC) is an emerging organization that can be employed on a stand-alone or ad hoc basis. It is located at the main CP and plans, coordinates, and synchronizes the corps or division deep operations. Making deep operations work requires the full-time

efforts of several personnel (FSCOORD, G3 plans, G2, and aviation officer). Additional assistance from other staff agencies (Deputy FSCOORD, EWO, ADA officer, ALO, G3 air, and PSYOP) are included as required. The chief of staff directs the DOCC and approves all deep operations. The DOCC, which has robust communication links—

- Acts as the deep operations C^2 node in order to support the successful execution of deep operations.
- Stays abreast of the status of close and rear operations and continually assesses its relationship with deep operations.
- Is responsible to confirm and validate the original DECIDE criteria for a deep operation target.
- Allocates and controls the attack resource to engage the target.

3-32. With the DOCC in place, the C^2 process is continuous and interactive. The DOCC ensures the commander's intent, missions, and events drive the process.

3-33. The G3—

- Ensures the HPTL, AGM, and BDA requirements are integrated with the decision support template (DST) (by coordinating with the targeting team).
- Ensures the plan to include targeting reflects the commander's concept of operation.
- Determines if the desired effects were achieved or if reattack is required (with the Deputy FSCOORD and G2).

3-34. The G3 Air—

- Supervises the A^2C^2 element.
- Deconflicts the division's airspace. (NOTE: This is an important aspect of planning and execution if you plan to use EA from an air platform.)

Chapter 4

Decide

DECIDE, as the first step in the targeting process, provides the overall focus and sets priorities for fires (to include EA) and a portion of intelligence collection. Many key personnel and organizations are involved in DECIDE. They perform a number of structured processes against the framework of the MDMP to plan the use of lethal and nonlethal fires for each phase of the operation.

Based on targeting priorities, the targeting team and other organizations will produce graphics and text tools to maintain focus on the process and synchronize the effects. Planning EA within the MDMP framework as a portion of DECIDE is comprised of five interrelated processes as shown in Figure 4-1.

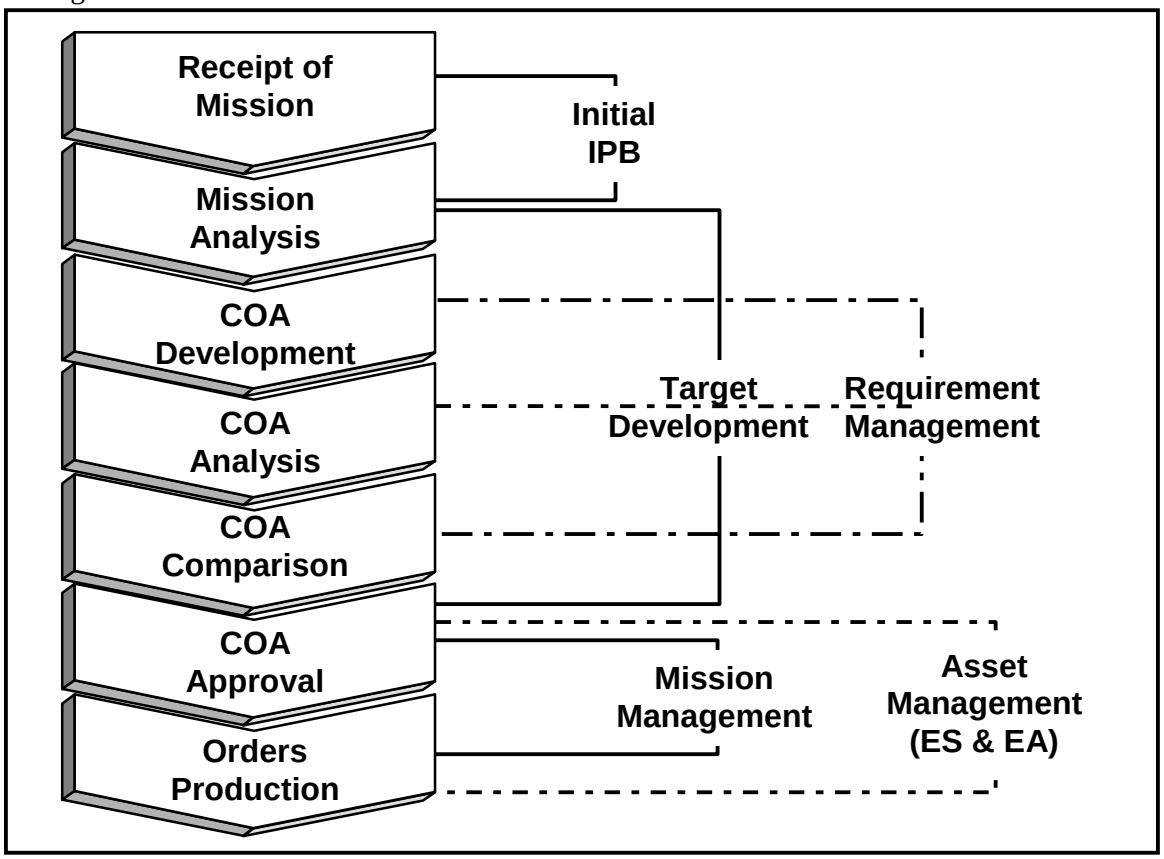


Figure 4-1. Planning EA.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

4-1. The initial IPB, as a subordinate step to mission analysis (the second step of the MDMP), starts the important analysis that eventually leads to EA planning. In terms of EA planning, the two most important products out of the IPB process (and into target development) are HVTs and EW analysis products. Figure 4-2 illustrates how IPB fits into EA planning.

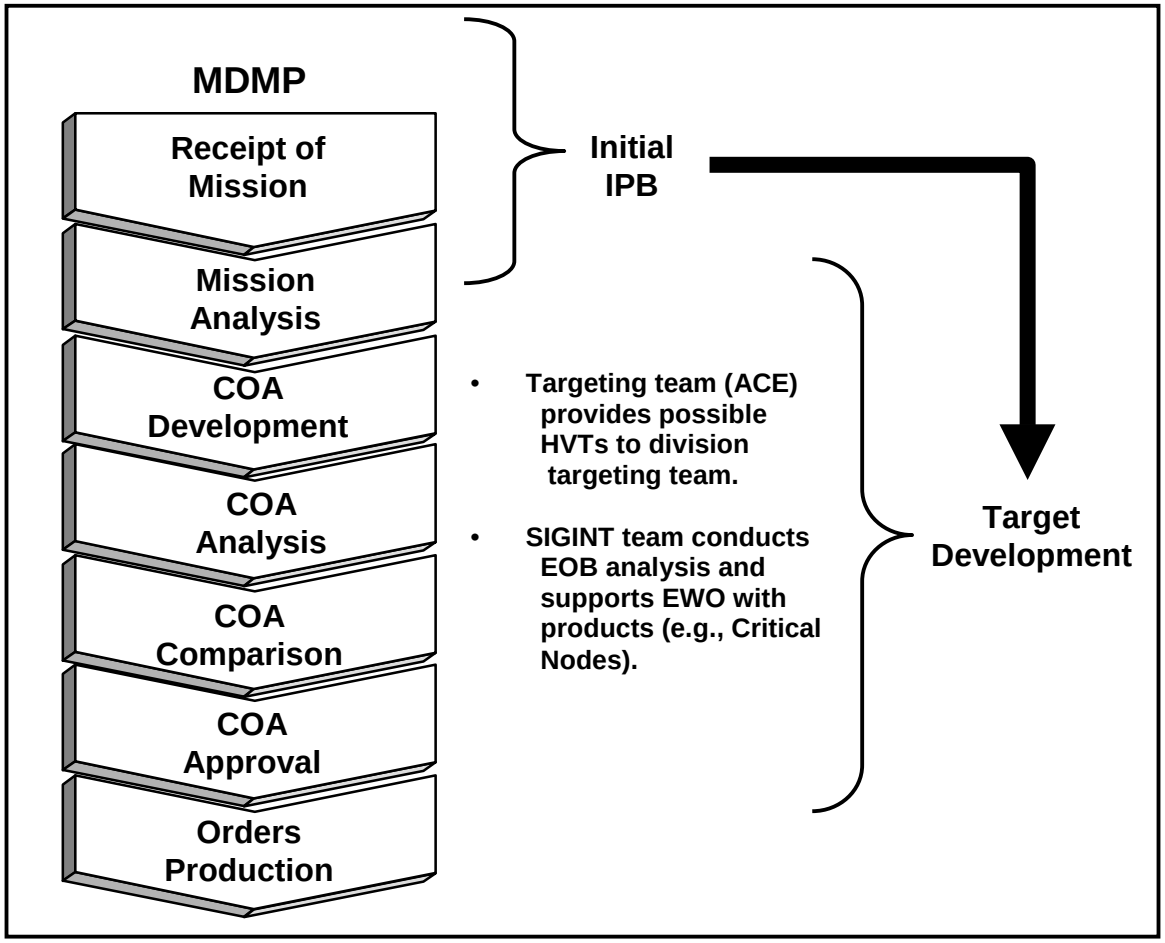


Figure 4-2. IPB in EA Planning.

HIGH-VALUE TARGETS

4-2. An important part of step 3 of the IPB process (evaluate the threat) is creating or updating threat models. A component of the threat model is generic HVTs. As the G2 Plans Officer provides the framework for the initial IPB (in order to support operational planning), the different portions of the ACE support the production of threat courses of action (COAs) and other IPB products. As the ACE develops threat COAs, the targeting team (ACE) analyzes the generic HVTs. Then they capture the most important HVTs for that particular threat COA into an HVTL. The targeting team (to include the

EWO) uses the HVTL to help develop HPTs after the wargame. HVTs are not specific or unique to EW; they support the entire targeting process.

EW ANALYSIS PRODUCTS

4-3. The SIGINT team, as part of both ongoing situation development and analytical support to IPB, uses the threat order of battle (OB) and HVTs (from the targeting team) to prepare net diagrams and other graphic planning and execution products. These products help the EWO identify critical communications nodes. These critical nodes are essential to the threat in order to use the EM spectrum. The EWO depends on assistance from the SIGINT team (through the collection manager) to ensure all HVT net diagrams are further broken down to show unique nodes that will disrupt the entire net if "jammed." These nodes become the initial candidates for EA targets.

TARGET DEVELOPMENT

4-4. During COA analysis (wargaming), threat COAs are analyzed in terms of their impact on friendly COAs. The wargame takes place using an action or reaction technique. The entire staff identifies the enemy battlefield functions that must be attacked. The commander and his staff analyze the criticality of friendly operating systems in the context of a specific COA. The G3 identifies the best places to attack HPTs in relation to the friendly COA; these places are designated TAIs. TAIs are points or areas where the friendly commander can influence the action by lethal or nonlethal fires and/or maneuvers. This manual discusses only those aspects that are most important to describing EA planning. FM 6-20-10 and FM 34-130 provide comprehensive doctrine for target development.

4-5. The targeting team uses two important products (besides threat COAs and the supporting products) from the IPB process for target development—HVTs and EW analysis products. After target development, the three most important products that flow into RM and MM are the HPTL, AGM, and EA portion of the battlefield operating system synchronization matrix. Figure 4-3 illustrates how target development fits into EA planning.

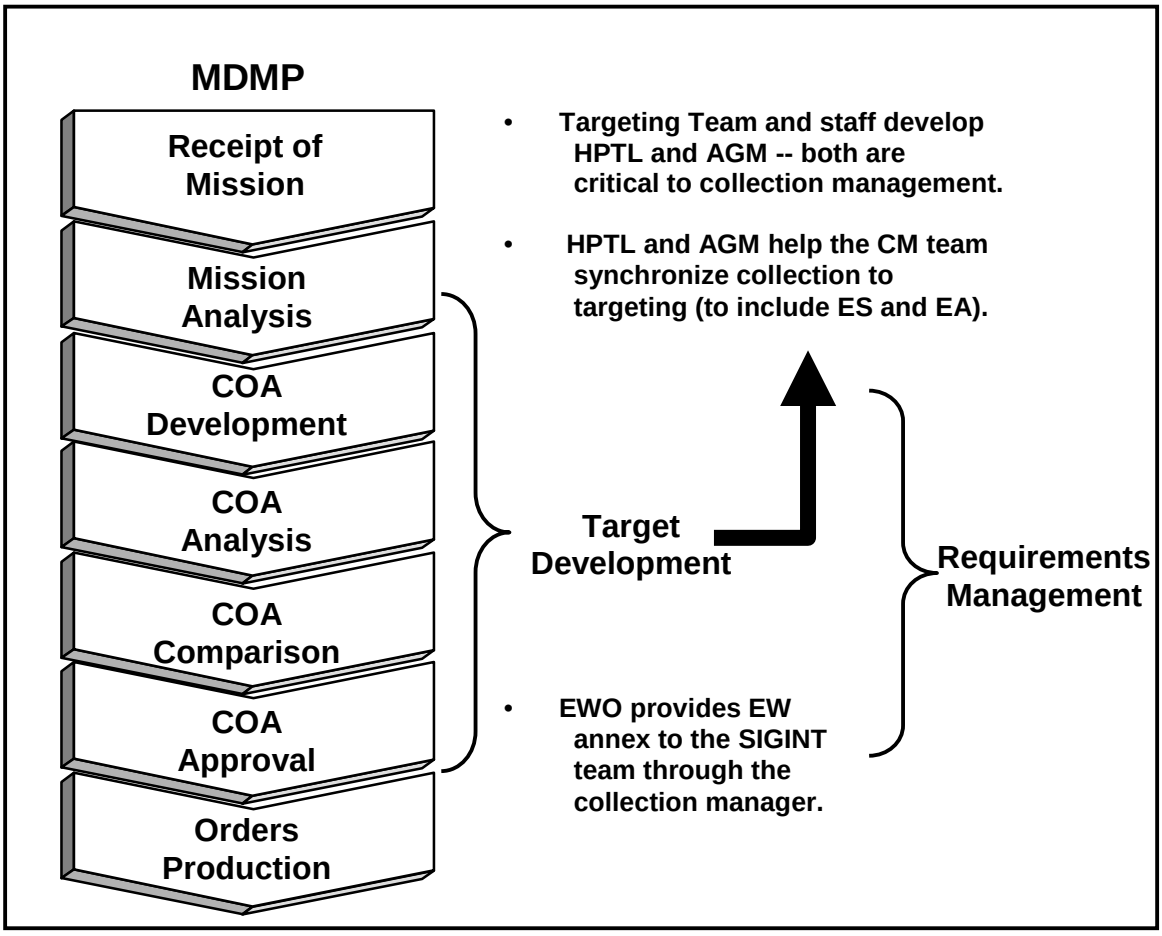


Figure 4-3. Target Development in EA Planning.

HIGH-PAYOFF TARGETS

4-6. Through wargaming the staff identifies the HPTs that must be acquired and attacked for the friendly mission to succeed. During COA analysis, the targeting team develops the HPTL, the targeting portion of the DST, and BOS synchronization matrixes. (This provides times for EA (non-lethal fire.)) For example, during the close fight, enemy artillery could be the priority for lethal and nonlethal fires. From this target set, specific HPTs (for example, an artillery battalion fire direction center [FDC]) is designated for lethal and nonlethal attack for a synergistic effect. The battalion FDC would be engaged with EA to disrupt coordination of fires by causing critical delays during the battle and would eventually be engaged by lethal attack (in accordance with the HPTL, AGM, and the TSS) for destruction. (For a more detailed discussion of the wargaming process, see FM 101-5.)

ATTACK GUIDANCE AND DAMAGE CRITERIA

4-7. Knowing target vulnerabilities and the effect an attack will have on enemy operations allows a staff to propose the most efficient available attack option. The commander provides critical guidance by stating that he wants to disrupt, delay, limit, damage, or destroy the threat.

4-8. The FSCOORD will provide the EWO with a desired level of damage or degradation. The EWO determines if current EA assets are able to range the target and achieve the mission, and how the mission will take place to achieve the desired effect.

EFFECTS OF FIRE

4-9. On the basis of the targeting team's guidance, the EWO recommends how each EA target should be engaged in terms of the effects of fire and attack options to use. The effects of fire can be to deny, disrupt, delay, and divert the target. The unique nature of EA, a non-lethal fire, and subjective use of these terms means the EWO must clearly communicate the intent of the terminology to both the targeting team and the collection manager. When applied to EA, these terms differ from when applied to describe physical destruction as defined in FM 6-20-10. The following criteria are captured in the AGM and EW annex.

Disrupt

4-10. Disrupt is designed to fragment the target's nets. This disruption will in turn cause the flow of information to slow, and in some cases stop the flow, until the net control stations can reinitiate the net and its users. When the enemy will attack, this tactic is effective as they move to LD. This tactic is simple to initiate and requires little coordination.

Delay

4-11. Delay is designed to fragment movements and deny the threat the ability to communicate in order to change routes. This tactic will necessitate the use of alternate forms of communication to continue movement (for example, hand-and-arm signals, runners). This effort will cause significant delays to the threat's movement, especially if tied in with obstacles. Denying the threat the ability to warn other units of obstacles will cause all follow-on units the same delay and could force the lead element to clear the obstacles without engineer support.

Divert

4-12. Divert is designed to prevent the target's use of critical resources. This method is used to jam combat support (CS) element's communication with combat units (for example, jamming combat service support [CSS] trucks on their way to an armor refueling or rearming point). Divert is a difficult task due to the intelligence required to pinpoint targets and upcoming events.

Deny

4-13. Deny is designed to control the EM spectrum and prevent the threat's use of that spectrum for any communications (whether voice or digital). This nonlethal fire is used at surge periods to act as a battlefield multiplier. The success of this fire denies the threat's ability to receive intelligence and to pass guidance. These actions in turn place a "stress" on EA assets and cannot be maintained for long periods.

EW TARGETS

4-14. The EWO helps develop the EW targets as an integrated portion of the HPTL. The three categories these targets fall into—planned, as acquired, and immediate—are discussed below.

Planned

4-15. For EW the actual target is the specific communication emitters that are critical to that target set during a specific military operation. The AGM as well as the BOS synchronization matrix will have these targets listed.

As Acquired

4-16. EA teams will engage these targets of opportunity upon detection.

Immediate

4-17. Targets (in the form of specific voice and data communications) are targets that the EWO did not or could not plan but that the targeting team identifies during the conduct of the operation and that require immediate EA.

ADDITIONAL ANALYSIS

4-18. The EWO then analyzes these requirements (in terms of effects and category) to further plan the EA necessary to service the target. He must determine the rough plan based on—

- Target vulnerability (in coordination with the SIGINT team). The EWO and SIGINT analysts use the electronic order of battle (EOB) to determine targets and use the electronic template to designate specific targets inside the target system. These targets will take into account redundant lines of communication (LOCs) and the advisability of engaging other communication links. An SA-8 battery may be identified as a critical target for EA, but due to its redundant communications and short link distance to its subordinate transporter or erector launchers, one can count on knocking out or degrading only one of its communications link. Therefore, the communication links would be "green" for targeting but the overall system would be "red" because it would still function despite the EA.

- System capability (in coordination with the SIGINT team).

- System reliability (in coordination with the SIGINT team).

- ROE. With the increasing technology of EW and dominance, the monitoring of ethical and humane issues is critical to ensure we do not deprive the local populace of critical casualty care, humanitarian support, and other life support through essential electronic communications.

4-19. The EWO analyzes whether organic assets can perform the mission. If not, the EWO requests support from higher through G3 and FS channels. He must also notify the collection manager when he requests support from higher in order to keep ES and EA synchronized between echelons.

TARGETING PRODUCTS (WITH EA FULLY INTEGRATED)

4-20. The EWO prepares documentation for the missions:

- EA targets on the HPTL.
- EA lines of the AGMs.
- The EA portion of the BOS synchronization matrix.

4-21. The EWO must prepare these documents to ensure the synchronization of lethal and nonlethal fires and the synchronization of EA with CM (this includes all three subprocesses—RM, MM, and AM). The end product of this process is the EW annex.

REQUIREMENTS MANAGEMENT

4-22. After target development, the most important products that flow **into** RM and MM are the HPTL and AGM. The most important products that flow **out of** RM into MM are the SIR (that the collection manager designates for ES) that support EA. Figure 4-4 illustrates how RM fits into EA planning.

4-23. During RM the collection manager performs a critical role by—

- Focusing the initial collection planning (as described in FM 34-2) to include synchronizing ES requirements to support EA tasks. This synchronization is accomplished when the CM team passes SIR to the SIGINT team.
- Ensuring that the EWO passes a clear articulation of the EA tasks (through the AGM) to the SIGINT team. The collection manager is the "middle man" and is the path for the EWO to request support from the SIGINT team. It is critical that the collection manager is a part of this process.

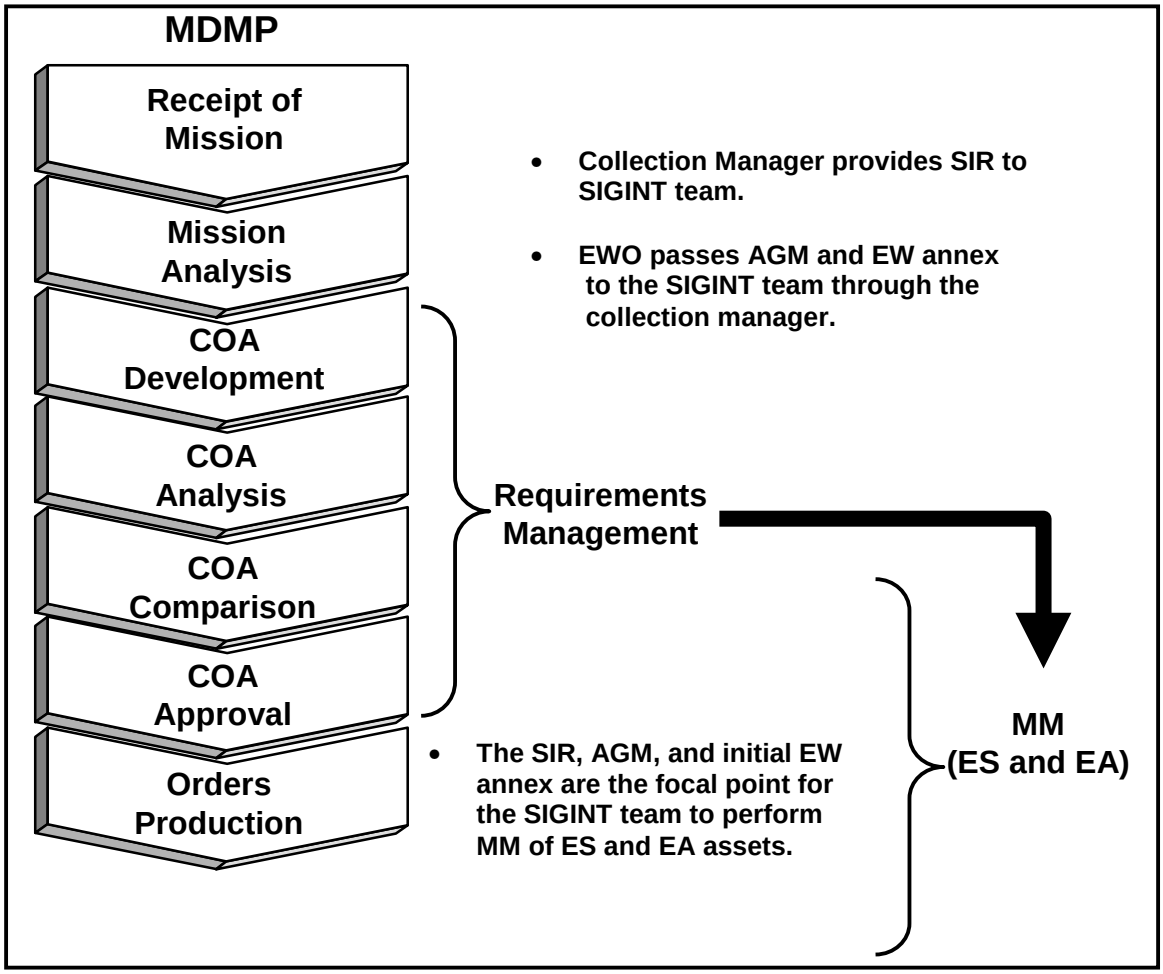


Figure 4-4. Requirements Management in EA Planning.

4-24. During wargaming the commander and entire staff determine decision points (DPs). When tied to targeting, the DPs ensure the decision to engage (or not to engage) occurs at the proper time. DPs and TAIs are recorded on the DST and are included in the intelligence collection plan. Wargaming helps finalize, among other products, the—

- Individual staff estimates.
- Scheme of maneuver and FS plan.
- DST and BOS synchronization matrix.
- PIR.

PRIORITY INTELLIGENCE REQUIREMENTS

4-25. The commander designates his PIR following the wargame. Generally, a PIR should support each HPT or TAI (if the staff plans to engage multiple HPTs within a TAI). This rule ensures that the commander prioritizes collection against HPTs. A latest time intelligence is of value (LTIOV) is a critical part of every PIR. This time (or event in certain circumstances) ensures that friendly collection does not occur after the point when that intelligence is not of use to the commander and friendly forces.

SPECIFIC INFORMATION REQUIREMENTS

4-26. The collection manager initially combines, validates, and prioritizes PIR and IR and prioritizes these sets of requirements. He then he refines these requirements into SIR that are clear, concise, and a "collectible" subset of the larger requirement. The collection manager takes the time to cross-check the HPT-related PIR against the SIR that support these HPTs. He ensures that there are adequate SIR (especially related to ES) to support the EA as captured on the AGM. The SIGINT team helps the collection manager perform this step because of their expertise in EW. Then the collection manager hands the ES-related SIR over to the SIGINT team. At the same time, the collection manager is capturing ES collection on the ISM.

MISSION MANAGEMENT

4-27. After RM, both MM and AM begin. In terms of MM, the most important products that are introduced into the process are the AGM (from target development) and the SIR (from RM). The most important products that flows out of MM are the specific taskings down to individual ES and EA assets. During MM the SIGINT team continues the CM process that started with RM. Figure 4-5 illustrates how MM fits into EA planning. FM 34-2 provides doctrine and TTP for MM.

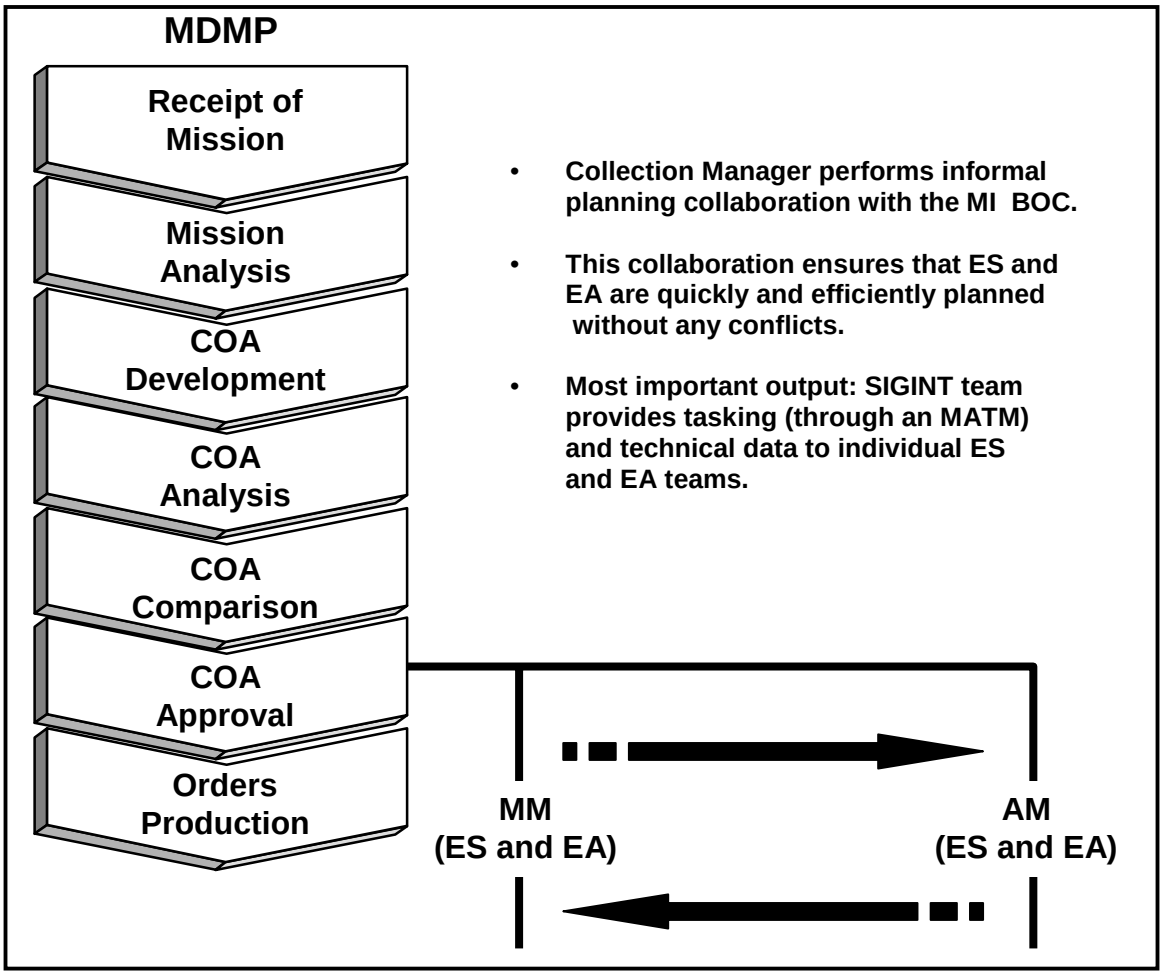


Figure 4-5. Mission Management in EA Planning.

REEVALUATE TARGET ANALYSIS AND IDENTIFY ADDITIONAL ES COLLECTION REQUIREMENTS

4-28. The G2 Plans Officer initially develops the sensor attack matrix, which is further developed during wargaming. The final signal attack matrix, which is developed by the SIGINT team, is used to determine the sensor to detect and locate targets. This matrix will also determine if the resources are available to detect, locate, and engage a specific target. The collection manager will use this matrix to task intelligence assets in locating targets.

4-29. The SIGINT team examines the analysis performed during target development and reevaluates if any subsequent analysis is necessary against the target. (NOTE: The SIGINT team continually provides intelligence in an easy-to-use format to ensure the EWO chooses valid EA targets during target development.)

4-30. The SIGINT team identifies (and later tasks) ES collection based on the SIR. In order to identify and track the critical communications nodes, the

SIGINT team uses its EW analysis (using All-Source Analysis System [ASAS] workstations) and the latest OB and situation development intelligence from the all-source team.

DETERMINE EA VIABILITY

4-31. The SIGINT team ensures that organic assets can perform the mission. If not, the EWO requests support from higher through G3 and FS channels. Additionally, the SIGINT team reviews the AGM, SIR, any guidance from the EWO, and the EWO's initial development of the EW annex. The EWO checks for any fragmentary orders (FRAGOs) that may have changed EA or ES missions. There are two important substeps to determine the viability of EA:

- Calculate EA effectiveness**.** The SIGINT team uses the signal-to-noise ratio (see Appendix B) to determine the effect of EA on targets at different ranges. ASAS provides a function to visualize electronic LOS. These two tools help the SIGINT team ensure that the EA targets are viable. (NOTE: The EWO, who is a subject matter expert on EW, knows the general ranges and capabilities of systems to ensure that the targeting team does not choose a target that EA could not service.)
- Assess technical data. The SIGINT team determines if sufficient data is available. This data will comprise operating frequencies, power output, distance between emitters and receivers, retransmission sites, and any historical information on threat reactions to EA. Additionally, the SIGINT team identifies (and later tasks) possible jump frequencies. The SIGINT team will task ES collection on these frequencies upon initiating EA.

ASSESS EA SYSTEM AVAILABILITY

4-32. The determination of availability is based upon three basic sets of information:

- Current mission tasking. The SIGINT team weighs each asset's current missions, alternate targets, and targets of opportunity against the EW targets and ES collection (in the form of SIR) to determine if the asset can add any missions to its current load.
- Current asset status. This step is based upon system performance. Performance is defined by the asset location (if the location is above targets with good LOS), sufficient power to achieve desired effect, and if the system can hit targets accurately.
- System performance (mechanical [the vehicle system] and technical [system and crew operations]). The SIGINT team maintains an informal record that indicates which systems require a higher degree of maintenance to remain operational.

DETERMINE ATTACK RESOURCES AND SELECT POINT OF ATTACK

4-33. Based on the attack guidance and effects of fire (as captured in the AGM and EW annex), the SIGINT team validates the target and the amount and type of EA necessary. The SIGINT team balances each target against the total workload on the EA and ES assets and determines the best assets to

perform missions (they will task these assets later). With guidance from the EWO, the SIGINT team prioritizes all missions and targets.

4-34. The SIGINT team creates alternate targets (at least one to each primary target). The SIGINT team designates the number of assets used on each target and any time coverage is necessary to jump assets forward. At this point, main targets are “locked in” while alternate targets are “plotted in” to ensure the mission is feasible.

EM SPECTRUM DECONFLICTION

4-35. The EWO and SIGINT team perform several actions with the support of the G6 to ensure that EA missions do not adversely affect friendly forces' use of the EM spectrum. The SIGINT team gathers data on higher and adjacent units' EW targets and assesses what impact (if any) these actions will have on organic missions and vice versa. This same step is performed with the tasking for EA. The SIGINT team will use the RFL to capture any conflicts between friendly communications and EA missions. Finally, the SIGINT team will determine if any interference will occur, taking into effect the harmonics from the EA mission and, if interference does occur, which task is the priority.

ESTABLISH JAMMING CONTROLS

4-36. The SIGINT team establishes both positive and negative controls on EA assets. It establishes a “stop jam” frequency and states procedures for “stop jam” in case of a loss of communications. The SIGINT team also ensures that the communication frequency is not in the harmonics of the target frequency (if using single channel).

TASK ES AND EA ASSETS

4-37. The SIGINT team tasks ES and EA assets through the multiple assets tasking message (MATM), which is sent digitally or by voice if the asset does not have the capability to receive digital tasking. The MATM for EA assets will contain technical and mission data necessary to accomplish the mission. Technical data will include callsigns, jargon, jump callsigns, signal strength (in Watts), stop jam frequency, and radio procedures to include threat procedures to follow in case of jamming. Mission data will include primary target, time of attack, alternate targets, and targets of opportunity. The MATM for ES assets will include technical data and mission data. The technical data for ES assets will mirror that for EA. Mission data for EA will include SIR, PIR, and the specific EA systems to cue on targets in accordance with the times detailed in the ISM.

ASSET MANAGEMENT

4-38. After RM, both MM and AM begin. In terms of AM, the most important products that are produced are the chain of orders (normally an initial OPORD then subsequent FRAGOs) that deploy and provide the framework for ES and EA operations. Figure 4-6 illustrates how AM fits into EA planning. FM 34-2 provides doctrine and TTP for MM. (Refer to Appendix D for message formats.)

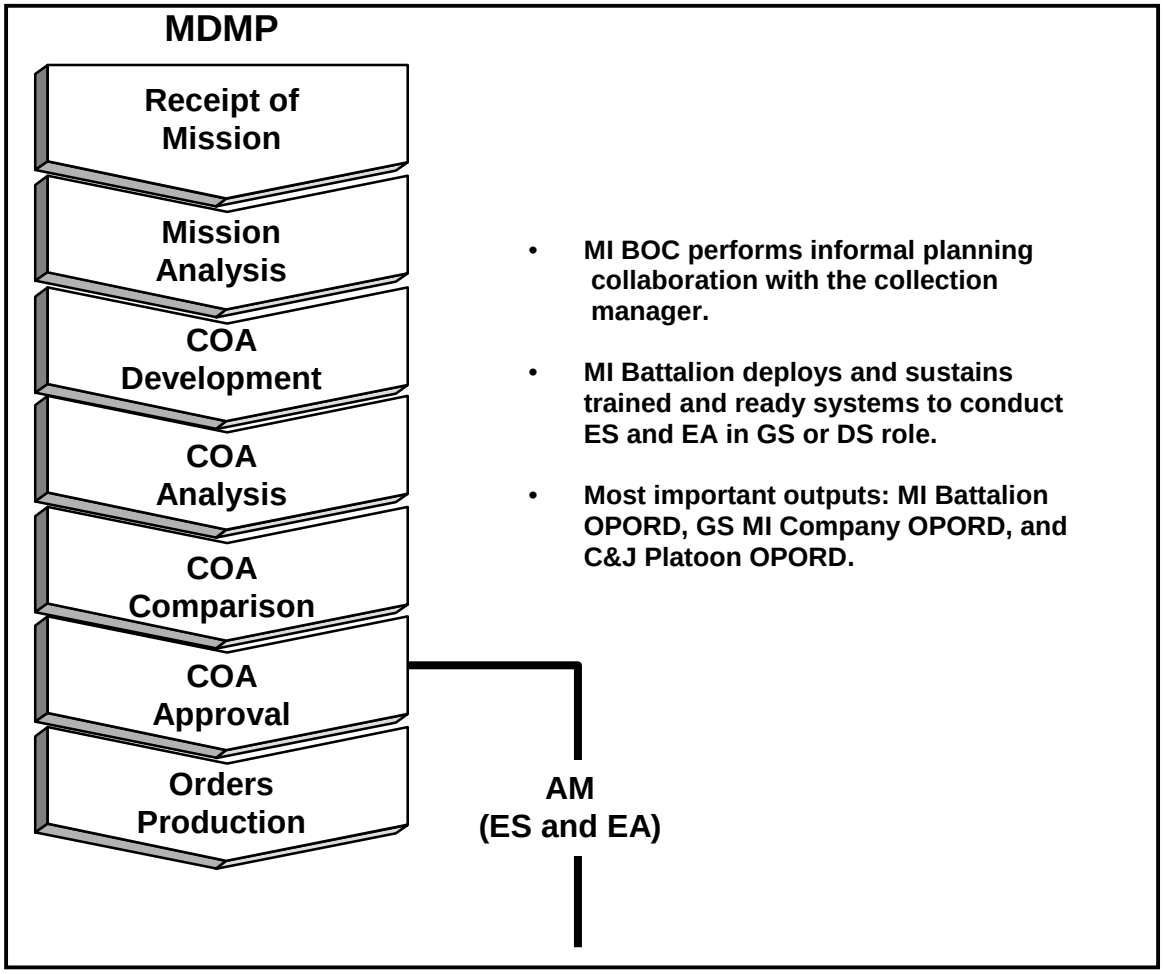


Figure 4-6. Asset Management in EA Planning.

4-39. The MI battalion commander and his Battalion Operations Center (BOC) (coordinating with the collection manager) task organizes EA and ES assets and coordinates the movement of EA and ES systems in order to support EA and ES tasking as developed by the SIGINT team during MM. This task includes planning to provide continuous coverage on the targets while other EA and ES systems move.

Chapter 5

Detect

This chapter discusses the deployment of ES systems and the collection and dissemination of ES data in support of EA. For EA to be successful on the battlefield, the commander must understand the role of ES and how to coordinate the ES effort in support of EA.

ELECTRONIC SUPPORT DATA

5-1. ES assets collect information for three purposes:

- To provide intelligence.
- To develop the database in the SIGINT team to aid the DECIDE function.
- To cue the EA assets to active targets.

5-2. Currently database development relies heavily on exploiting signal internals, which include what is said that specifically identifies the target and gives target intent. Future ES systems, like PROPHET, will detect and collect signal externals. Signal externals only identify that an emitter is active and is located at a specific grid coordinate. If the ES system is designed to identify what kind of unit is associated with the peculiar characteristics of the emitter, then you will know a little about the unit but not the specifics of its purpose, capabilities, and intent. More detailed analysis, often at echelons higher than that supporting the EA asset, is required to provide this information.

5-3. DETECT is composed of three functions:

- Deploy ES and EA assets.
- Collect ES data.
- Process SIGINT data.

DEPLOY ELECTRONIC SUPPORT AND ELECTRONIC ATTACK ASSETS

5-4. Deploying assets is naturally divided into the three basic categories of platforms:

- Ground vehicle platforms.
- Ground manpack platforms.
- Airborne platforms.

5-5. ES assets are not deployed in the same manner as EA systems. ES systems deploy in various formations to create a baseline which will provide area coverage for specific missions. For example, the "Lazy W" configuration is used for a wide coverage along a front where enemy positions are unknown. Systems will deploy to high ground for best LOS, while still remaining in proximity to adjacent systems in order to maintain system parameters and good baseline for DF and cueing operations. Targets from the HPTL will be found, identified, located, and targeted for a predesignated mission. In the defensive, ES assets are used primarily to identify targets on AAs into the AO.

5-6. EA assets deploy to cover specific areas in response to targeting requirements. EA assets will move to high ground to achieve optimal LOS; generally valleys, passes, roads, and bridges are ideal target areas because they create choke points in which EA is most effective. EA assets will not deploy in the same area unless a high number of targets require two systems or more to cover them.

GROUND AND AIR ASSETS CAPABILITIES

5-7. Air and ground assets have unique capabilities to consider when employing. Employ air and ground assets to complement their capabilities. The collection manager must ensure that the ISM is configured to efficiently fulfill the requirements. Use of EAC assets should never be the sole source of ES. Because EAC ES assets are not organic to the ground commander, they lack the responsiveness and flexibility to collect within a specific area and cross-cue other sensors.

Ground Capabilities

- Advantages:
  - Ability to continue long-term collection and EA regardless of the weather.
  - Can quickly respond to changes in requirements.
- Disadvantages:
  - Assets limited in LOS considerations will shut down to jump forward in battle.
  - Terrain limited.

Air Capabilities

- Advantages:
  - Ability to overcome the LOS problems encountered by ground assets.
  - Has a standoff capability.
  - Has minimized terrain interference.
- Disadvantages:
  - The depth of planning needed to employ air assets due to the short duration of missions and maintenance requirements.

- Air assets are extremely weather dependent and are easily found with DF when using EA.

AIRBORNE PLATFORMS

5-8. Airborne deployment falls into three functions. These assets are heavy maintenance items and are generally used during specified periods to provide EA capability on targets not in range of ground assets.

Select Restricted Operation Zone (ROZ)

5-9. The ROZ determines the flight path from which the airborne platform will perform its mission. This function has five steps:

- **Step 1. Determine target LOS.** This step entails the analysis of LOS by the pilot, the senior operator, and the MI battalion S3. They will analyze the LOS and choose the best possible ROZ to hit the target considering elevation, range, terrain (for example, mountains, bodies of water).
- **Step 2. Determine communications LOS.** This step, which is performed after the selection of the primary ROZ, ensures communications with the ACE.
- **Step 3. Determine area coverage.** This step outlines the possible areas of effects for EA. During this step possible ROZs are identified and each is countered against terrain masking. Those ROZs with a high degree of terrain masking are eliminated.
- **Step 4. Determine cover and concealment.** During this step the pilots will determine the altitude of their aircraft in correspondence to the nearest cover (for example, mountains, ridgelines) for quick evasion of threat's air defense.
- **Step 5. Determine ingress and egress routes.** This step provides entry into the ROZ and exit points out of the ROZ for coordination with the BCD. This step is continuously updated as intelligence from the MI battalion S2 brings to light new air threats.

Coordinate ROZ Selection

5-10. This function covers the coordination for air space with the BCD. Pilots will request a ROZ with the MI battalion S3. This request will specify the air space and request it 72 hours in advance. The S3 will then coordinate the request with the Joint Forces Air Component Commander (JFLAC)/A^2C^2 for the ROZ. This JFLAC/A^2C^2 at the Corps will then pass the request onto the BCD. The BCD will coordinate with air space managers who decide whether this request is acceptable or if an alternate ROZ is granted due to air space limitations.

Review Air Threat Report

5-11. The pilots and crew perform this step. The aviation brigade will receive intelligence on the current threat to air assets and confirm the intelligence with the ACE. The pilots and crew will review this report before the mission. This report may cause the use of alternate ROZs because of a

high threat. New intelligence and requirements update steps 2 and 3 continuously.

GROUND MANPACK PLATFORMS

5-12. Manpack collection teams can be deployed alone or in conjunction with other elements. Independently deployed assets will have the additional responsibility of team security and added supply considerations.

Ground Manpack System

5-13. Manpack collection systems provide the commander with unique capabilities when conducting initial entry, stability operations, and support operations. Found in both light and special operations forces (SOF) units, manpack systems have characteristics not found in vehicle systems. Manpack systems are characterized by the following:

- Deployable in areas that are normally not accessible or usable. This access can be constrained by threat forces and/or routes to site. The manpack allows the commander to place teams in areas where vehicle-mounted equipment would present too large of a footprint and terrain is too restrictive for air assets. Due to this, manpack systems are often close to or past the forward line of own troops (FLOT).
- Manpack systems also have a lower battlefield signature due to placement and equipment. Thus they can be used in more low-profile operations and are especially helpful in urban situations.

5-14. Limitations of manpack systems:

- Very limited mobility of collection teams.
- Teams may have to rely on outside assets (airlift in most cases) to deploy on the battlefield.
- Manpackable systems are usually not netted, so DF will be limited to lines of bearing (LOBs) from each system.
- Collection teams will be limited on mission duration (normally 3 to 5 days) and METT-TC dependent.
- Current reporting may be limited to voice communications or short data bursts depending on equipment.
- Limited communication link, high security requirements, difficult resupply, and deployment asset.

Special Considerations

5-15. Special considerations must be made for small low-level voice intercept (LLVI) teams which will be deployed close to the FLOT if not beyond it. These teams are dependent upon stealth for battlefield survival. The teams will usually be inserted by air, either air assaulted in or jumped in. Slow movement due to the weight of these small systems will make security escorts hard to plan and coordinate. For these sites, situational awareness is imperative. Evasion plans are briefed and planned with rally points and

extract points fully detailed. If contact is made, team members will move as a group or as individuals back to the predesignated points.

GROUND PLATFORMS

5-16. Current ground systems have to completely shut down in order to change position. The commander must decide on how much of the baseline he is willing to lose for the duration of the movement. A commander can move all or part of the assets. Jumping a part of the baseline at a time allows the commander to maintain coverage of the targets, but this is a slow process.

5-17. In the case of the "Lazy W" configuration, a commander can start movement by jumping the two rear operating systems. Once these systems are in place and operational, the commander would then jump the other three systems. The other option is to move all systems at the same time. The commander can negate the loss of target coverage by coordinating with other assets.

Ground Systems Augmented With Air Assets

5-18. The commander must carefully plan and coordinate for the use of organic aerial assets. The aerial assets add tremendous flexibility to the baseline. Aerial assets—

- Can extend the width and depth of the ES ground baseline.
- Can provide coverage on targets while part or all of the ground systems are in movement.
- Provide the commander with on-the-move capability. This becomes the critical issue when the battlefield tempo exceeds the movement capability of the ground systems.

5-19. Deploying ground platforms consists of three interrelated functions:

- Coordinate ES and EA position selection.
- Select ES and EA operational sites.
- Occupy and prepare selected ES sites.

5-20. **Coordinate ES and EA Position Selection.** This function is comprised of three actions:

- **Select general deployment areas (GDAs).** This step consist of five sequential tasks to determine possible sites and their overall advantages and disadvantages.
  - **Review maneuver unit's scheme of fire and maneuver.** Under some circumstances, the GS MI commander may attach ES and EA assets under the direct control of the DS company. The DS company will provide a situation report (SITREP) on the AO to the GS commander for team movement. Upon arrival, the DS company commander will take control of the asset and, with assistance from the GS commander, provide logistical and related support. There are several techniques for site security (for

example, attached security force such as a fire team, collocation of ES and EA assets, or providing your own security with internal assets).

- **Conduct map reconnaissance.** In this task the team leader and the POC leader assess possible site locations and routes to and from the sites. The POC leader will indicate each team TAI to ensure focus on each particular AO.
- **Select potential operational sites.** From the map reconnaissance the team leader, with input from the POC leader and input from the IPB process, will select the best sites from the potential site list. Elevation, multiple egress routes, LOS of surrounding areas, and minimal terrain masking to surrounding areas are essential for EA/ES.
- **Confirm current security in AO.** In this task the team leader coordinates with the POC to ensure that the site selected is secure. The POC will determine if there are indications of enemy activity in the AO, or if there are electronic signatures of enemy transmitters at the potential sites as indicated by DF results collected by friendly ES assets. The POC will ensure the site is not expected to have threat movement through the area or to have strategic importance to the threat.
- **Conduct site reconnaissance.** In this task the team leader performs a site reconnaissance on the ground. Several sites will be reconnoitered for use as primary, secondary, or alternate sites. With the rapid flow of the battlefield, there may only be the opportunity to do this only initially or during a defensive phase of the operation. In an early entry force this step will not be performed, and IPB and map reconnaissance will give the best possible site. Under these circumstances OPSEC is paramount.

- **Coordinate with maneuver unit commander.** This step is composed of five tasks which are sequential in nature. These tasks outline the process of coordinating instructions (the fourth paragraph in the OPORD).
  - **Coordinate times and routes for deployment.** This task is conducted by the POC leader, who coordinates with the MI battalion S3 (who then coordinates with the G3) through the GS MI company commander for movement and routes. If a POC leader is part of the DS company, he should coordinate through the DS company commander with the S2 and S3 of the unit that owns the terrain (usually a maneuver brigade) and inform the MI battalion S3. This information is passed to the team leader in a FRAGO from the POC leader.
  - **Coordinate operational sites.** This task is also conducted by the POC leader to ensure sites are available for use by ES and EA assets, and there is no confliction. Confliction can take place with other assets and nearby assets such as signal assets causing disturbance in EM environment or being hampered in turn by EA operations. Terrain deconfliction must be addressed during the

orders process and at the highest level possible. It is not uncommon for conflicts to arise with signal, mortars, scouts, and EW—assets all vying for the same piece of ground. The POC leader must ensure these steps have been performed before teams move to these sites.

- **Coordinate security.** This task is performed by both the MI company commander and MI battalion S3 who coordinate security for EW assets. The team leader and the POC noncommissioned officer in charge (NCOIC) make the coordination between the ES or EA asset and the maneuver asset that will provide security en route to the predetermined ES or EA site. For example, an ES or EA asset would deploy with scouts who are conducting a reconnaissance mission. Upon reaching the ES or EA site, the scouts will continue with their reconnaissance mission. A security force will not always accompany assets during movement, but it is desirable if possible.
- **Coordinate communications procedures.** This task is performed by the team leader during the POC leader's OPORD. The team leader will receive procedures and frequencies during the OPORD, which he will disseminate to the team before movement.
- **Coordinate CSS requirements.** The team leader at this point will coordinate any service support requirements for the systems, vehicles, and radios.

- **Obtain approval of general deployment area.** This step is composed of three tasks to obtain approval for ES and EA systems.
  - **Integrate ES mission with host maneuver unit.** This task is initiated by the GS MI company commander to ensure the movement and mission of ES and EA assets remain synchronized with the maneuver element.
  - **Gain clearance for ES and EA operational areas and sites.** The POC will gain clearance from the company commander for operational sites for ES and EA. Some considerations will be the possible duplication of efforts from adjacent units and required baselines for collection. The required baselines will make the ES site selection difficult since the sites must fit into an overall scheme while also having good LOS at each site. EA considerations are units in the line of electronic fire that may experience a communication loss during EA missions. Examples of four possible ES baseline configurations are listed below.
    - Standalone, which provides an LOB from the ES asset to the target (Figure 5-1).
    - Convex, which provides good LOBs against targets that are located to the sides of the baseline of systems (Figure 5-2).
    - Concave, which is best, is used when the targets are straight in front of the baseline (Figure 5-3).

- "Lazy-W," which is the most often used configuration because it offers good DF when the target's location in relation to the baseline is unknown (Figure 5-4).

▪ **Gain clearance for ES and EA systems movements.** This task is the final coordination done with maneuver element before the asset pushes out to its site. This final clearance will give team leaders a green or red status for movement along predetermined routes.

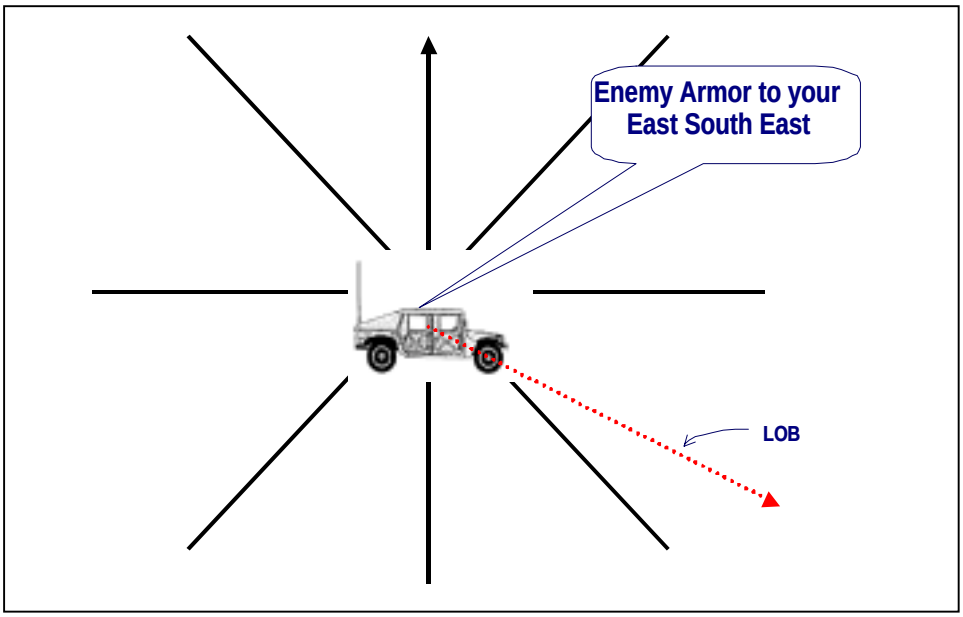


Figure 5-1. Stand Alone Operations

5-21. **Select ES and EA Operational Sites.** This function identifies **primary**, **alternate**, and **supplementary** sites as well as provides for preparing site sketches. Communication, target LOS, and range of targets are essential to operations and are part of site selection. Range will always be dependent upon terrain, vegetation, emitter power, distance between receiver and collector, and numerous other factors. The SIGINT team will use the signal-to-noise ratio to ensure EA systems are within range of their respective targets. Also considerations for baselines are imperative in choosing these sites. All possible sites must provide support for the baseline to effect accurate locations and overall coverage of the battlefield.

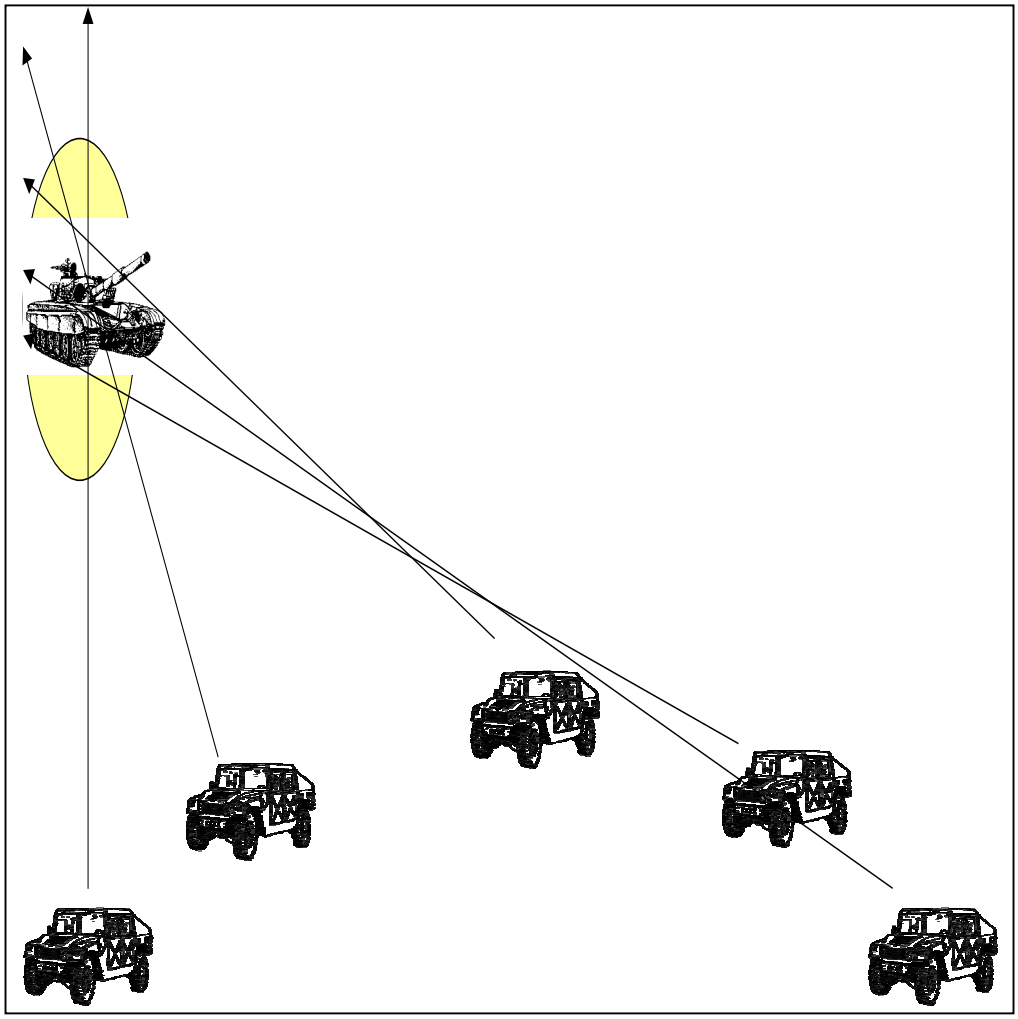


Figure 5-2. Convex Baseline

- Select primary ES and EA positions. This step is composed of five tasks to determine specific site locations:
  - **Determine communications LOS.** This task is performed upon reaching the site but before setting up the ES and EA system. Communication LOS is critical. Without communications the system will move to a point where communications are reestablished (for example, after one hour without communications, the system will move to reestablish communications).
  - **Determine target LOS.** The team leader performs this task. He performs LOS analysis based on recommendations of the ACE through its use of the ASAS for LOS determination. This analysis will consider terrain to include mineral deposits, vegetation,

elevation, large manmade features, and bodies of water. (For more information, refer to FM 34-130.)

- **Determine area coverage.** The team leader maps, either informally or formally on paper, the possible area upon which the system can provide ES and EA. This mapping should be a 360-degree picture from the system with shade in the areas that are masked by terrain and thus are not generally collectible or attackable by the system. Map utilities' field of view (FOV) function on ASAS can provide general information on terrain coverage and is used to assist in identifying and eliminating primary and alternate sites.
- **Determine cover and concealment.** This task is performed upon reaching the site. The team leader will position the system on the military crest of the terrain with the antenna rising above the ridgeline. If possible, use higher terrain behind the system to avoid silhouetting the antenna against a lighter background such as the sky. Attempt to use natural cover for the system, while keeping the system at the best possible site. The ES system will use camouflage, but will also make optimal use of natural vegetation. EA systems will not use camouflage due to the repositioning of the system after mission EA assets depend on natural concealment and positioning. The use of vegetation on the system is desirable as long as it does not interfere with quick site egress or system capabilities. Small LLVI teams will find terrain, which provides good LOS but is of little or no tactical value because of their proximity to the FLOT. LLVI teams depend upon natural concealment and vegetation for site concealment.
- **Determine ingress and egress routes.** If possible, the team leader will designate both a primary ingress route into the site and egress route moving away from the FLOT. These routes should use a high degree of concealment and cover ensuring no observation of movement can occur from the direction of the FLOT.

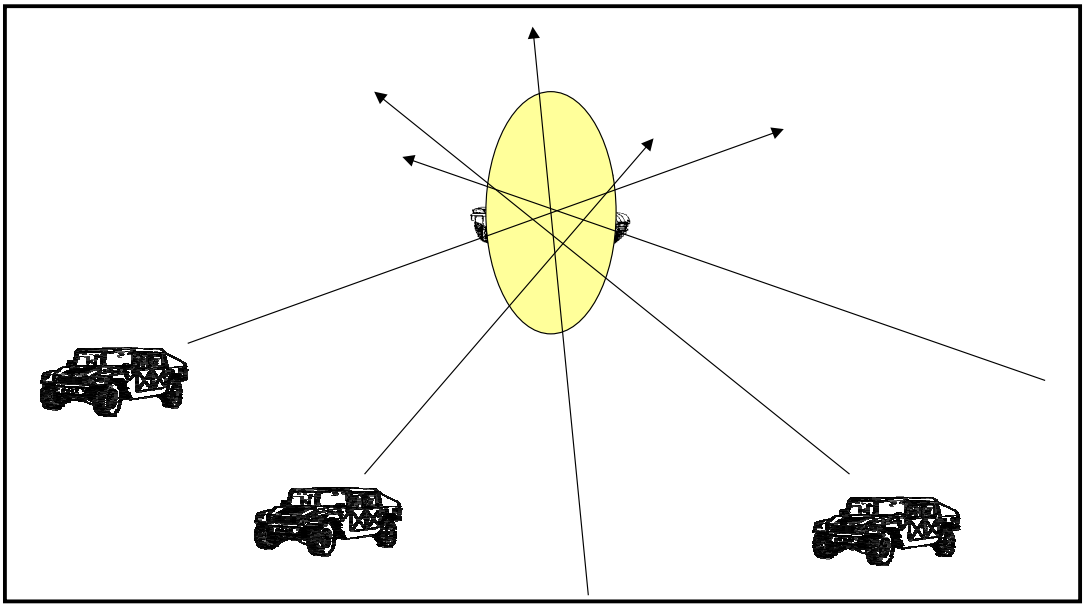


Figure 5-3. Concave Baseline

- **Select alternate ES positions.** This step is composed of five tasks, which are identical to the task of selecting the primary ES and EA positions. The target will remain identical to the targets of the primary ES or EA site. Use these tasks to evaluate and choose the next best site. This site will be used if the first site is compromised or deemed unsuitable for the mission. An example would be friendly intelligence indicating that the enemy is nominating the primary site for artillery or an enemy axis of advance. If contact is ever made, the system must relocate due to its limited small arms fire capacity. If security is added, weigh the benefits of added firepower versus the larger footprint created by security force.
- **Select supplementary position.** This position has the same requirements as above. This site will be the last formally selected site in the AO and used as a last resort. All above-mentioned factors will be considered in this step.
- **Prepare site sketches.** This step is comprised of three tasks. The team leader will sketch these tasks on a sector sketch. The team leader will also brief team members on specifics of the sector sketch (for example, fighting positions, egress routes, and rally points).

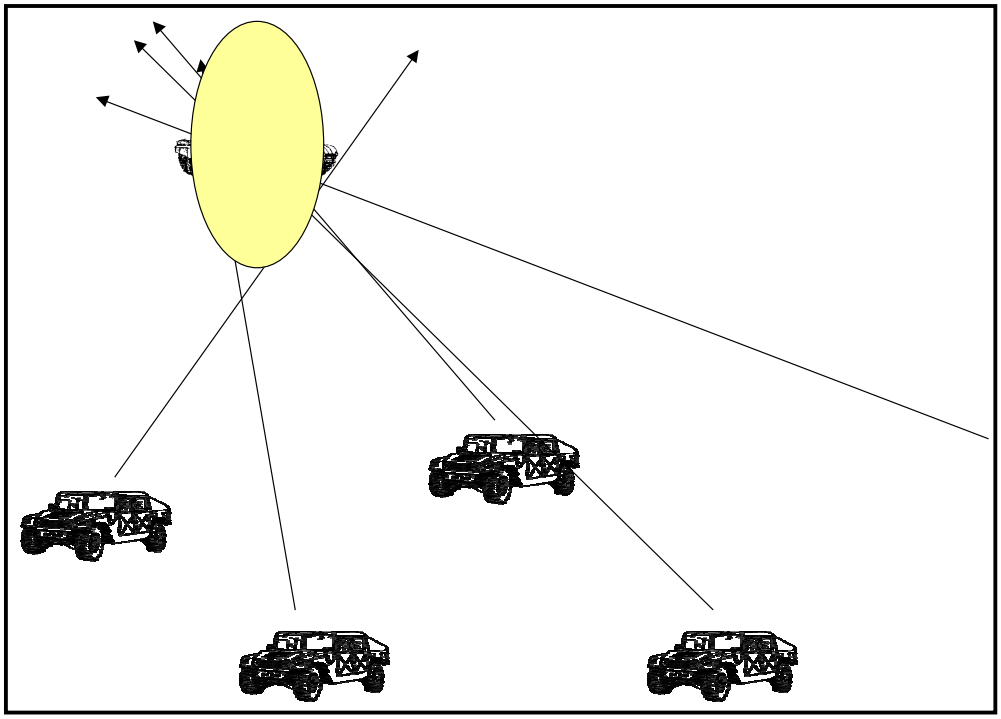


Figure 5-4. "Lazy W" Baseline

- **Fighting position sketch.** This task provides a sector sketch, which includes sectors of fire, dead space, and alternate fighting positions. These fighting positions are hasty at first and later, if time permits, are developed into fighting positions. Due to time considerations and the high amount of movement occurring with ES and EA systems, this decision will be mission dependent. LLVI teams will make hasty fighting positions but if contact occurs, they will break contact and move back to rally points. LLVI teams do not have the capability to sustain engagements. Stealth and concealment are the two best security tools for LLVI teams.
- **Ingress and egress sketches.** These sketches provide routes to and from the site, giving specific routes for specific contact (for example, if contact occurs to the east the team moves out on the egress route to the west). The team leader will designate vehicles and ground rally points.
- **Administrative sketch.** This sketch lays out the location of the system and chases vehicles along with fire, fuel, and crew rest points. (NOTE: This requirement is impractical for LLVI teams.)

5-22. **Occupy and Prepare Selected ES Sites.** This step is comprised of five tasks:

- **Move to site via entry point.** This task will begin the movement from the GS MI company AO or the controlling element to the ES or EA site. Using tactical road march procedures the team will move out

along secure routes, if possible, to the site. If the chase vehicle is available, it will move out in front of the system 100 meters to act as security for the system and to determine road conditions for the system. The engaged ES or EA system will evade and use the chase vehicle to provide cover for system movement if the chase vehicle is available. The team will not approach the site from a vantage point observable from the FLOT.

- **Establish security.** The chase vehicle personnel perform this task upon reaching the site. The chase vehicle will confirm or establish the security of the site before the system moves onto the site. When the system arrives, communications are established and security will remain in force until the end of the mission. LLVI teams will typically send one man forward to the site to ensure security and then move the entire team to the site for system and antenna set-up.
- **Confirm LOS to target area.** After establishing security, the team leader will place the target on the terrain and ensure that he still has LOS to target. The EA team leader will orient the system on the targeted area before set-up, either using terrain reference or getting an azimuth on target from the SIGINT team.
- **Conduct system set-up.** After communications are initiated and site location is confirmed along with target location, the team leader will begin system set-up procedures. The unit SOP will regulate system set-up, and security will remain in effect during system set-up.
- **Minimize antenna masking by obstructions.** Performing this task will not significantly delay the team in relocation. Techniques for this task include—
  - Using high terrain behind antenna to prevent sky lining.
  - Using trees and vegetation to conceal the antenna if they do not have a high water content.
  - Using the military crest of the hill to keep the antenna concealed as much as possible.

COLLECT ELECTRONIC SUPPORT DATA

5-23. Collection of ES (communications intelligence [COMINT]) data falls into two categories: voice and digital or analog data. This data will be used to identify and target receivers for EA.

COLLECT VOICE DATA

5-24. This function has six subfunctions that when combined and analyzed provide intelligence on targets and nodes for the effective use of EA against these nodes.

Intercept Signal

5-25. ES systems will search across the spectrum for enemy communications (either voice encrypted or clear).

Target Acquisition

5-26. Collection for target acquisition is the process where the ES system has been given specific tasking to locate a particular target. It can be as simple as finding a particular frequency to provide orientation data for an EA system. Or it can be as complex as searching the full spectrum for a particular entity that has met the criteria for EA. The ES system then tips that frequency and location to an EA system for attack. The length of time that it takes the ES system to fulfill the tasking is directly tied to the amount of technical data that is supplied with the tasking. The ES system that has been tasked to provide tip-off data is also usually tasked to monitor the effectiveness of the attack. The tasking for this type of mission originates in the ACE and is refined by the GS or DS company POC prior to being sent to the system.

Gist Signal

5-27. The operator will provide the gist of the communication; callsign, ID nets (for example, artillery, infantry).

Locate Target

5-28. This subfunction will be performed either by the system which is netted or by the POC team using numerous LOBs.

Analyze the Signal and Build a Database

5-29. This subfunction will be performed primarily in POC and above by 98Cs to build net diagrams for the precise delivery of EA to delay, disrupt, divert, or deny spectrum to enemy.

Report Collection Results

5-30. Operators will report collection data as soon as possible to expand the SIGINT base.

COLLECT DIGITAL OR ANALOG DATA

5-31. This function has seven steps that somewhat mirror the subfunctions of collecting communications data.

Intercept Digital Analog Signal

5-32. Operator will scan and identify signal (for example, digital artillery nets).

Record Digital/Analog Signal

5-33. Operator will record the signal and make notes about the type of signal.

Identify Emitter Parametrics

5-34. Operators identify signal strength and width.

Identify Emitter Function

5-35. This step is completed by the POC team or higher through enemy historical data and threat models.

Locate Digital or Analog Target or Build Digital or Analog Database

5-36. This step is also performed by analyzing data at the SIGINT team level.

Report Digital or Analog Collection Results

5-37. This step is performed by the operator along with sending the recording back to the SIGINT team.

COLLECTION FOR DATABASE DEVELOPMENT

5-38. The collection manager develops clear, precise, and valid tasking to support targeting. In order to maximize collection, the EWO will coordinate with the collection manager to ensure the EW target annex is integrated into the collection plan for ES. Information obtained from this collection will help update local and national databases in order to perform situation development.

5-39. Collection will be geared to support the PIR and IR and the current operation. The collection manager can follow one of several methodologies when developing the EW target list (EWTL). These methodologies vary from EW support to targeting to collection for threat database development.

5-40. The collection manager can focus tasking by threat operating systems. The collection manager plans collection based on the operating system that he feels will be most beneficial to support PIR (for example, artillery, maneuver units, reconnaissance units).

5-41. Tasking is based on known frequency, callsign, net characteristics, or signal characteristics. Characteristics can determine the importance of a net. Example: If an artillery command observation post (COP) were known to operate on a specific frequency, that frequency is included in the tasking. Tasking is based on geographical location. Signals may be of particular interest if DF places it in an area that is of specific interest.

SEARCH TECHNIQUES

5-42. There are three main techniques of acquiring target emitters. They are **spectrum searche**s, **band or sector searches**, and **point searches**. These techniques are best used combined, not independently. The techniques employed will depend on the mission, the number of assets, and their capabilities.

SPECTRUM SEARCH

5-43. A spectrum search entails a detailed mapping of the entire spectrum that is exploited by a particular system. This search provides an overview of the amount and type of activity and where in the spectrum it is located. No detailed processing is done on signals. The amount of time to identify the

signal and produce an LOB or fix is kept to a minimum. This search technique is best used to first establish what activity to exploit. Spectrum search allows a single asset to locate and exploit emitters to fulfill mission requirements. In a multiple asset system, one position should always conduct a spectrum search to acquire new targets.

BAND OR SECTOR SEARCH

5-44. A band or sector search follows the same guidelines as a spectrum search but is limited to a particular segment of the exploitable spectrum. By limiting the size of the search band, the asset can improve the odds of acquiring a signal. This technique is used only in multiple asset or position systems. This search will allow for the development of new targets.

POINT SEARCH

5-45. The point search technique is used when a list of specific targets is provided for monitoring or exploitation. This technique allows for in-depth, long-term exploitation of signals in a defined environment. Point search should be used only after a thorough map of the environment is completed and in conjunction with a spectrum, band, or sector search. This technique is used to tip-off preplanned targets to EA assets.

CROSS CUE

5-46. When an ES asset acquires an EA target (for example, preplanned or target of opportunity), the ES asset is responsible for tipping the target information to the EA asset.

5-47. The EA ground systems have the capability to use either an omnidirectional antenna or a log periodic antenna (LPA). The difference is that the LPA increases the effective radiated power and the power is focused along a general azimuth. In order to use the LPA, the EA system operator must know the approximate target location prior to the start of the EA mission. This is one way the ES system supports EA missions.

5-48. The EA aerial systems have only omnidirectional antennas. With both types of EA systems, the ES assets provide support by providing target acquisition, target tip off, target monitoring, and jamming effectiveness.

TA TEAM

5-49. The TA team will verify and assist the ES assets in target detection. The TA team will take the notification of a target from the ES asset and verify the target with the AGM or EWTL. If it is a valid target, the TA team will notify the ES asset in order to pass the target to the EA assets.

5-50. Along with tasking the EA assets, the ES assets are tasked to monitor the target in order to quickly identify information that would lead to valid targeting. Because information is time sensitive, quick reporting is vital.

5-51. The minimum information that needs to be passed to the EA assets are frequency, location of target, and signal characteristics (if available). This enables the EA assets to acquire the target and position their antennas in the correct azimuth.

PROCESS SIGNALS INTELLIGENCE DATA

5-52. The processing of SIGINT data will create and redefine the baseline of intelligence necessary for the commander to envision the threat, both current and future. The data produced by this process will provide support to targeting, SIR, and numerous other products to the commander. The processing of SIGINT data takes place at all levels of ES, from the ES asset operator to the SIGINT team and collection manager. The focus of the manual is on EA but it provides a brief overview of the process of intelligence as it applies to EA.

5-53. ES assets will transmit collection data via tactical reports (TACREPs) to the TA team. The data will include signal type, target identification, and gist of target activity.

5-54. The TA team will process the ES data, fusing the data to develop a battlefield picture and provide support in either a GS or DS mode. The TA team will provide limited processing using support from the SIGINT team via ASAS, doing limited work on simple voice matrixes, and using the OB and the EOB. These tools, along with intelligence disseminated by the ACE, provide a source for intelligence support to units supported in a DS mode.

5-55. The SIGINT team will further process ES data, having feeds from both the TA teams and, under certain circumstances, the ES assets. The data processed will depend upon numerous factors. Upon support from higher to decrypt communications data and intelligence feeds, the SIGINT team will also use the OB, EOB, and doctrinal templates to determine threat intent and actions.

5-56. The SIGINT team and the TA team will provide target data to FS channels. Using the ISM, these teams provide priority to targeting requirements to ensure intelligence is provided in a timely manner to engage HPTs. These targets may be engaged by either lethal or nonlethal fires.

SITUATION DEVELOPMENT

5-57. It is crucial that information pass between elements as quickly and as accurately as possible. Information development data will be passed from the ACE, down to the ES and EA assets, in the form of technical data and tasking. Technical information that is developed at the ES asset is also passed directly to the EA asset (as well as to the ACE) to help with database development.

5-58. Once the ES system has acquired the target, the operator must disseminate the information to the EA system. This is done most frequently with voice communications. The data needs to include the frequency, location, and signal characteristics. The ES system operator also notifies higher headquarters that the target was acquired and that the necessary data was transmitted to the EA system. If the ES system fails to acquire the target, the ES system operator must notify higher so that the tasking can be shifted or changed.

ELECTRONIC ATTACK EFFECTIVENESS

5-59. During an EA mission, the ES asset will monitor the target to provide feedback to the EA asset and to provide the analytical element with an effectiveness report. The purpose of feedback is to keep the EA asset apprised of the status of the target. The immediate notice of changes to the frequency, location, or signal characteristic is vital to the success of the EA mission.

5-60. When a mission is completed, the ES or EA asset will send the analytical element a detailed effectiveness report in the form of a jamming effectiveness report (JER) or multiple assets effectiveness report (MAER), which will be sent digitally or by voice. This report will include the effects on the target from the perspective of that ES or EA asset. It includes but is not limited to frequency, location, signal characteristics, effects observed, and duration. (See Appendix D.)

Chapter 6

Deliver

The DELIVER function of the targeting process executes the target attack guidance and supports the operation once the HPTs are located and identified. The attack of targets must satisfy the attack guidance developed in the DECIDE function. This guidance is divided into two categories: tactical and technical decisions. Throughout this chapter we will refer to the tasker agency; generally this refers to the TA team at the brigade TOC. Other tasking agencies can be the General Support Operations Center (GSOC), G3, and ACE.

TACTICAL DECISIONS

6-1. Tactical decisions determine the—

- Time of the attack.
- Desired effect.
- Degree of damage, or both.
- Attack system to be used.

6-2. On the basis of these tactical decisions, the technical decisions describe the—

- Number and type of munitions.
- Units to conduct the attack.
- Response time of the attacking unit.

6-3. These decisions result in the physical attack of the targets by lethal and/or nonlethal means. For more information on targeting methodology, see FM 6-20-10, Chapter 2.

TECHNICAL DECISIONS

6-4. In the DELIVER phase EA includes conducting and reporting EA functions. This process is linear and continuous; each step is vital to the overall effectiveness of EA. EA cannot be a battlefield multiplier if it does not have continuous ES along with SIGINT team intelligence support. Different techniques against different units will give varying results. Terrain will influence these results; it is critical to use terrain to augment the mission of EA. In defense operations the ability to deny communication when a unit arrives at an obstacle is an overwhelming battlefield multiplier. The necessity of reporting the techniques and the threat reaction also will provide

a baseline for future missions. In an environment rich with signals, it is imperative that EA is delivered with precision and overpowering force. Figure 6-1 shows an example of using ingress routes into division or brigade AOs.

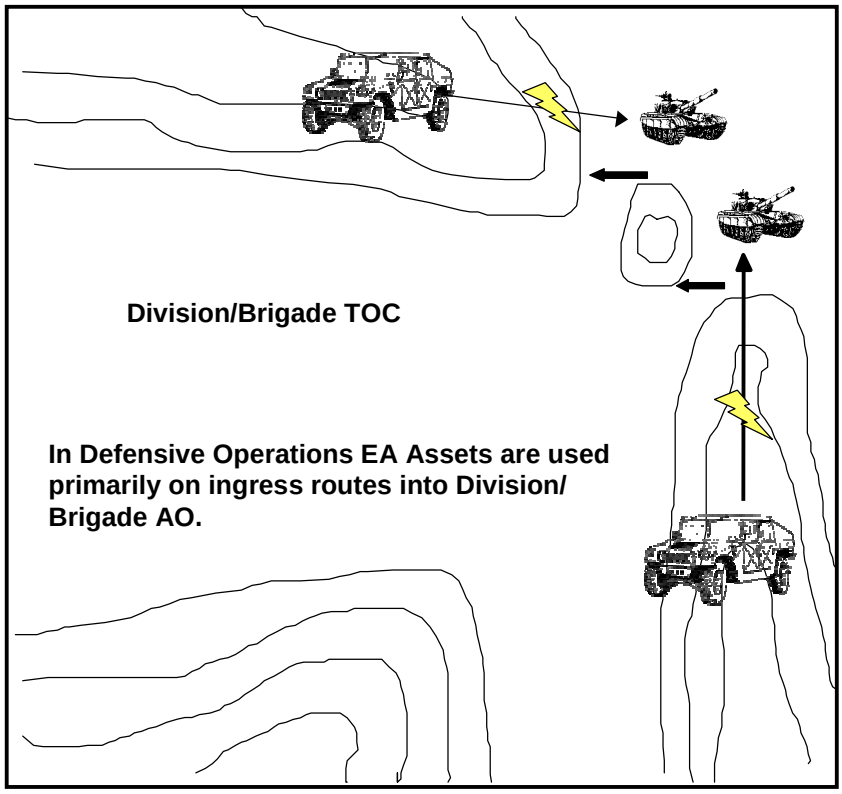


Figure 6-1. Division or Brigade TOCs

CONDUCT ELECTRONIC ATTACK

6-5. This operation has three functions. **Acquire target**, **reappraise and apply jamming equation**, and **jam target**.

ACQUIRE TARGET

6-6. This function has three steps: **Confirm target technical parameters**, **monitor target frequency**, and **confirm target acquisition**.

Confirm Target Technical Parameters

6-7. This step consists of three tasks:

- Confirm target frequency. The team leader will confirm with the TA team or POC the specific target frequency and ensure if jump frequencies were used that they were provided with jump sequence and correct jump frequencies.

- Confirm spectrum scan segments. The team leader will next use the scan function on the system to determine the exact frequency. This process is done because recalibration of a system is rare and the frequency may not correspond exactly.
- Confirm continued monitoring of target. The operator or team leader will confirm with the TA team the continued monitoring of targets.

Monitor Target Frequency

6-8. This step has three interrelated steps:

- Monitor designated frequency. The operator will monitor the frequency.
- Monitor designated scan sectors. The operator will monitor the particular sectors to ensure the system is still on target for the exact frequency.
- Revisit target frequency. The operator will periodically check on the target. How often the asset revisits the target is determined by the number of targets and the SIGINT team.

Confirm Target Acquisition

6-9. This step has four sequential steps:

- Acquire signal. This task is covered in the previous section.
- Identify signal. The operator will identify the particular signals with data passed by the SIGINT team.
- Confirm signal is designated target. The operator will use this data to confirm that the target is the same target passed by the SIGINT team. Examples of this confirmation would be callsigns, jargon, language, and essential elements of information.
- Confirm signal is preplanned target or target of opportunity. The operator will confirm that the target is either a preplanned target or a target of opportunity. This task is the last confirmation that the target is the correct target.

REAPPRAISE AND APPLY JAMMING EQUATION

6-10. This function will be performed by the SIGINT team to ensure that the EA asset can acquire the target and the target will be within range of the EA asset. The jamming equation will give the SIGINT team a range of each EA system with regard to particular emitters and receivers. Doctrine and equipment capabilities dictate quick and overpowering EA attack; therefore, this equation is not used for minimum power. An example of this are targets of opportunity. The EA team will not have the time to perform the equation and fine-tune the EA asset to hit the target with minimum power (minimize the asset's signature). The requirement for this technique is no longer valid because these assets deliver quick overpowering attacks.

JAM TARGET

6-11. This function has four steps.

Review Jamming Control

6-12. This step will ensure that there is a "stop jam" frequency being monitored by the system.

Program Jamming Power Output

6-13. This step will pass from the tasker to the jammer the power output for the system. This step is usually bypassed with the assumption that maximum power for precise overpowering EA will be used.

Jam Target Using Predetermined Techniques

6-14. This step will direct the EA system in the particular techniques to use. There are four basic techniques: **deception**, **jamming**, **masking**, and **DE**.

6-15. **Deception.** EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. There are three primary types of EM deception:

- Manipulative EM deception, which involves actions to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces.
- Simulative EM deception, which involves actions to simulate friendly, notional, or actual capabilities to mislead enemy forces.
- Imitative EM deception, which introduces EM energy into enemy systems that imitate enemy emissions.

6-16. **Jamming**. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EM spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. Jamming falls into two categories, voice and digital (analog) data. Communications jamming is targeted against hostile voice systems for multiple purposes:

- To introduce delays into the enemy's C^2 system that allows the friendly commander to fully exploit his options.
- To delay hostile time-sensitive information until it is no longer useful.
- To force the enemy (in conjunction with ES) into actions that are useful to friendly operations. There are three primary types of EM jamming:

An example of EA forcing the enemy into action useful to friendly operations out of encrypted communications through jamming allows ES to gather intelligence from this otherwise secure net and further develops an intelligence baseline.

  - Spot Jamming. Spot jamming may be directed at a single frequency or multiple frequency through sequential spot jamming and involves jamming various frequencies one at a time in

sequence. Simultaneous multispot jamming involves jamming several frequencies at the same time. In both spot and sequential spot jamming, the full power of the jammer is directed against one frequency at a time, increasing the effectiveness and range of jammer. Spot jamming is less likely to interfere with friendly communications because receivers and transmitters can easily avoid it by slightly changing (detuning) the frequency they are receiving.

- Sweep Jamming. In sweep jamming, the jammer goes through a frequency range, then repeats the sweep continuously. All frequencies in the range are jammed. Friendly frequencies may be affected unless protected by the Joint Restricted Frequency List (JRFL).
- Barrage Jamming. Barrage jamming, unlike spot jamming, simultaneously spreads the jammer's power over a larger portion of the frequency spectrum, thereby reducing radiated power directed at any single target frequency. Barrage jamming is similar to sweep jamming, since all frequencies are jammed within the targeted portion of the spectrum.

6-17. **Masking**. Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES without significantly degrading the operation of friendly systems.

6-18. **Directed Energy.** DE is an umbrella term covering technologies that relate to the production of a beam of concentrated EM energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to damage or destroy enemy equipment facilities and personnel. Directed energy warfare (DEW) is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel; or to determine, exploit, reduce, or prevent hostile use of EM spectrum through damage, destruction, and disruption. (See Appendix A for more information on DE in EW.)

Report Inability to Locate Target

6-19. The operator reports the inability to locate the target and therefore to queue ES assets to search for the target or to pass targets to other EA assets.

JUMPING EA ASSETS AFTER EA MISSIONS

6-20. Dependent upon METT-TC, the commander must review the advantages and disadvantages of moving EA systems after EA missions. This decision becomes more critical as threat technology increases.

- Advantages: Jumping systems after each mission increases survivability due to the strong EM signature produced during jamming missions. These signatures are easily located if in the VHF range. When located, ES assets can DF these signatures and provide support

to targeting for lethal fires and various other means to destroy the EA asset.

- Disadvantages: Jumping systems after each mission will dramatically decrease the amount of EA missions which can be accomplished. The tear-down, set-up, and movement time will use up critical resources, specifically time. Due to the necessity of locating EA assets near the FLOT, movement will also expose systems to threat forces in the area of movement. Therefore, the decision to move is balanced against missions and resources.

REPORT ELECTRONIC ATTACK RESULTS

6-21. This operation has two functions: **determine effectiveness** and **prepare and transmit EA report**.

DETERMINE EFFECTIVENESS

6-22. This function has three steps.

Determine Degree of Disruption to Threat Communications

6-23. This step has four tasks:

- Monitor target reaction. In this task the team leader will record and analyze the reaction of the target. The team leader records the specific reaction of enemy forces with the support of an ES asset such as communication phrases (for example, "we are being jammed" "say again," "repeat all after,") or no verbal recognition of voice communications or contradictory acknowledgement. Contradictory acknowledgment (for example, "go to assembly area Bravo" when the original message was assembly area Golf). These statements would mark the conclusion of a successful EA mission.
- Estimate degree of degradation to maneuver. The team leader would once again listen for phrases, which would provide information. The team leader will also look for phrases that indicate delay, disruption, and diversion of maneuver elements (for example, "Mike 14 you are off line," "Mike 14 move back into formation.") If these phrases are repeated to several different units in the element, the EA is effective.
- Estimate degree of degradation of fires. This task can be analyzed if the target is a voice net. With the digital artillery nets, the team leader will not be able to assess effectiveness, but ES systems will be able to monitor the net to see if the jamming is overpowering the signal to the receiver. Also, assessment of the battlefield will reveal if the enemy forces initiated any artillery missions. A forward observer (FO) calling for fire and adjusting fire—
  - Has to repeat coordinate.
  - Is delayed passing adjustments.
  - Adjustments are delayed in firing.

6-24. The team leader will look to see if the mission is performed and the degree of effectiveness. If multiple adjustments over several minutes are not made and the unit moves out of the area, but the FO cannot walk the rounds onto the unit, the EA mission is successful.

- Estimate degree of degradation. The team leader performs this task. This effectiveness is determined by multiple means. Voice analysis identifies similar phrases in the monitoring of target reaction. Also, the team leader will look for indicators that actions are not followed or performed. Another way to estimate degradation is for the ES assets to report the splintering of the net. Throughout these tasks, the ES systems must support the EA personnel orienting the EA systems. It is also critical to support EA assets for effectiveness. For EA systems using encrypted communications channels, the ES system will monitor the net to see if EA overpowers the system and if the voice net drops into the "red." These actions are clear indications of the effectiveness of EA. Many nets will assume bad encryption and simply go "red" to communicate. If this happens, EA may cease and ES begins to gather intelligence until the SIGINT team tasks the EA team to reattack the target.

Prepare EA Rating Table

6-25. This step has two tasks.

- Estimate mission success. The team leader, in conjunction with the ES assets, performs this task to estimate the degree of degradation of communication and noncommunications nets. This will determine the success of mission.
- Describe threat reaction to EA. This reaction is recorded in the determine degree of disruption to threat communications. These reactions are compiled by the tasking agency to give overall enemy reaction to EA.

Prepare to Continue Mission or Begin New Mission

6-26. The SIGINT team will decide whether to continue the mission based upon the EW annex. If the mission is ineffective, the SIGINT team may task the EA asset to employ a different technique or it may pass the mission to other EA assets. If the mission is successful, a determination will be made if the net is still a viable target or to move onto another mission.

PREPARE AND TRANSMIT EA REPORT

6-27. This function has two steps. These steps conclude DELIVER, although this is truly a continuous cycle.

- Transmit effectiveness report. A MAER is sent by the team leader to the tasker to report the overall effectiveness and status (a basic summary) of the missions performed by the EA asset. The MAER—
  - Will queue the SIGINT team for additional missions and any specific reports needed before new missions are begun.

  - Will also provide details on the target, target reaction, mission success, and techniques employed.
  - Is not only a report on the effectiveness of EA but also upon the reaction of enemy forces to particular techniques.
  - Is used to build a database on the use of EA against specific units and their specific reactions and provide EA assets and EWOs more concrete expectations when delivering EA.
- Summarize significant EA mission technical parameters. These technical parameters summarize the frequencies and power used on specific targets.

SUMMARIZE STATUS OF ELECTRONIC ATTACK ASSETS

6-28. This task will provide a basic system status report. The EA system will send a multiple assets status report (MASTR) to the SIGINT team detailing the team status. This will provide the exact status of each EA asset to include the fuel, water, food, and ammunition. When combined with the system status, they give the SIGINT team a complete understanding of the system and its ability to perform additional missions.

Chapter 7

ASSESS

EW operators constantly evaluate the effectiveness of EA missions and report this information to the supported unit. The supported unit in turn incorporates these EA effectiveness reports into their combat assessment of the targeting effort. The combat assessment is the final function in the targeting process. The assessment represents the staff's determination of the effects of fires (lethal and nonlethal) on the enemy and whether these effects are accomplishing the commander's targeting objectives. The combat assessment forms the basis for the staff's reattack recommendations to the commander and future weapon system selection and employment. Assessing EA begins with the operators.

OPERATOR EVALUATION

7-1. It is important for the operator to evaluate EA effectiveness based upon the desired effects contained in the attack guidance. This technique provides the operator with a quantifiable measure of EA effectiveness. The use of percentages or other numerical formulas at the operator level are not accurate and add little to the assessment of EA effectiveness on the battlefield. The EA system operator and operators of the supporting ES systems execute the following steps to evaluate the effectiveness of EA missions.

RECORD JAMMING EFFECTIVENESS

7-2. During jamming missions, ES operators monitor the target to determine if the jamming is overpowering the signal to the receiver and affecting the target operator's ability to communicate.

RECORD EFFECTS ON THE TARGET SIGNAL

7-3. This is particularly important when attacking targets such as encrypted voice and data networks. EA and ES operators cannot access or exploit the internals of these communications systems and must judge the effects of jamming on the signal itself. Understanding the effects of the jamming signal on the target signal is also important when using EA and ES operators that are untrained in the target language. If the jamming is overpowering the signal, then the ES system will hear the noise of the EA system override that of the target transmitting station. The operator will also see a "spike" on the oscilloscope when the EA system signal is active. If these indicators occur, then the EA operator can assume the attack is effectively disrupting the target's ability to communicate.

RECORD OPERATOR COMMENTS

7-4. Listen for operator comments about difficulty communicating or executing operations. Phrases such as "I can't hear you, say again," "we are being jammed," and "repeat all after" indicate that the jamming power and technique are disrupting communications. Record instances where the operator repeats movement instructions, firing data, and situation reports. Note incidents where operators do not acknowledge a transmission and messages or give contradictory acknowledgments. An example of a contradictory acknowledgement would be when the operator confirms "assembly area Bravo" when the original message was "assembly area Golf." Additionally, the operator should listen for changes in attitude, rate of speech, and use of obscenities that reflect the operator's emotional response to the effects of EA. Operator comments provide important information about the EA technique employed and whether the EA mission achieved the targeting objective.

RECORD COUNTERMEASURES TO JAMMING

7-5. The ability of the operator to recognize and react to EA varies based on his training, experience, and discipline. An inexperienced operator may attribute the noise or broken communications to nature or equipment rather than to EA. This type of operator will attempt to work through the EA rather than to take countermeasures such as switching to an alternate frequency or mode of communications. The more experienced and trained operator will recognize EA and initiate some form of countermeasure to defeat or minimize the effects of EA. Noting how long it takes the operator to recognize EA and to take action are important pieces of information for future EA mission on the target or similar targets.

DETERMINE JAMMING EFFECTIVENESS

7-6. The level of accuracy in this subjective evaluation depends upon the training and experience of the EA operator. The assessment begins with the operator reviewing the EA guidance contained in the tasking message or OPORD. The operator considers the jamming mission successful if the mission occurred on time, against the correct target, and achieved the desired EA targeting effect.

REPORT JAMMING EFFECTIVENESS

7-7. The EA operator provides a JER to the TA team, which in turn compiles these reports into a MAER for the SIGINT team that addresses the effectiveness of the mission. The SIGINT team will forward this information in a signal summary (SIGSUM) to the EWO for MEA. This report gives details on the target, target reaction, and techniques employed. This report is not only a report on the effectiveness of jamming but also on the effectiveness of the particular techniques against a target type. Targeting and planning personnel use this information to ensure EA assets are employed to their fullest potential against appropriate targets.

REPORT DECEPTION EFFECTIVENESS

7-8. Assessing the effectiveness of deception occurs at the ACE as they fuse intelligence to discern the threat's reaction to the deception operation. Deception assessment occurs seldomly at the operator level. Indicators for operators of a successful deception operation are threat forces attempting to communicate, to gather data, and to coordinate movement if using imitative deception. (See Appendix D for more information on electronic deception.)

UNIT COMBAT ASSESSMENT

7-9. The unit staff builds the combat assessment from BDA and MEA. BDA describes the effects of targeting (lethal and nonlethal fires) on the target and forms the basis for reattack recommendations. MEA addresses the effectiveness of munitions, weapons systems, and tactics. Together, BDA and MEA help the unit understand the impact of the current FS plan on the threat and improve the targeting effort in future operations.

BATTLE DAMAGE ASSESSMENT

7-10. The G2 is primarily responsible for developing the BDA within the unit staff. During DECIDE, the G2 assists the commander in setting BDA requirements for HPTs. The G2 incorporates these BDA-related PIR into the collection plan and orders to subordinate units. This supports the timely collection and reporting of BDA information to the G2. For EA missions, this ensures ES systems are tasked to collect and report on the effectiveness of EA missions.

7-11. In addition to intelligence reports and operator evaluation, the G2 also uses target development and FS planning products to develop the BDA. The DECIDE phase products provide the G2 with the target descriptions, attack rationale, and desired effects that the targeting team used to develop the HPTL and concept of fires. The G2 should refer to the following documents during BDA development. The staff should also update these and other documents (for example, situation template, target synchronization matrix, collection plan, and FS plan) based on the results of the BDA.

- Concept of fires provides the task, purpose, method, and desired effects required to support the commander's scheme of maneuver.
- HPTL provides a mechanism for prioritizing the analysis effort with the targeting priorities. The EA effectiveness report should include the target number to assist in associating reports to targets.
- Target spreadsheet provides the analytic yardstick for comparing the desired effect contained in the concept of fires and HPLT with the actual effects. In the case of EA targets, situation templates reflecting the threat EOB and critical nodes should be present in the spreadsheet or as a separate electronic preparation of the battlefield product.

7-12. With the raw data such as the EA effectiveness report and reference material in hand, the G2 begins the task of sorting and analyzing the data to develop an all-source intelligence BDA of the effects on the target. To further aid in this task, each BDA is broken down into three components. Each component allows the G2 to scrutinize and record the effects on the target

from a number of perspectives. These three different assessments also require different sensors, analytical elements, and timelines. They are not necessarily subcomponents of each BDA report. The four components are physical damage assessment (PDA), functional damage assessment (FDA), target system assessment (TSA), and MEA.

Physical Damage Assessment

7-13. PDA estimates the quantitative extent of physical damage through munition blast, fragmentation, and/or fire damage effects to a target. This assessment is based on observed or interpreted damage. While EA is not traditionally thought of as physical damage, the EWO can develop an immediate assessment of the effectiveness of EA through "observed or interpreted damage."

7-14. **Observed Damage.** Much like lethal fires, EA can be either observed or unobserved nonlethal fire. Observed EA requires an ES asset to "observe" or monitor the effects of the EA on the frequency of the system under attack. The EWO must identify EA targets requiring ES collection during the DECIDE function of the targeting process. If the requirement becomes a PIR, the collection manager will then request or task support for monitoring the EA target. The ES asset will then monitor the target and provide feedback to the EA asset on the effects of the attack. At the end of the EA mission, the EA and ES will send a MAER to the EWO and collection manager on the results of the mission.

7-15. **Interpreted Damage.** If an ES asset cannot monitor the EA mission, then the operator must interpret the effectiveness of the attack based on the asset's proximity to the target, ability to acquire the target, technical factors (for example, signal-to-noise ratios), and operator experience. The EA asset and SIGINT team cannot quantitatively interpret the effectiveness of unobserved EA. Unlike the physical signs of the effects of lethal fires, the effects of unobserved EA cannot be evaluated based on post-strike reconnaissance.

Functional Damage Assessment

7-16. The FDA estimates the degree of degradation caused by EA against the target compared to the operational objective established against the target. This assessment is inferred on the basis of all-source intelligence and includes an estimate of the time needed to replace the target function. An FDA is a temporary assessment (compared to TSA) used for specific missions.

Target System Assessment

7-17. The TSA is a broad assessment of the overall impact and effectiveness of all types of attack against an entire target system's capability (for example, threat air defense systems). It may also be applied against threat unit combat effectiveness. A TSA may also look at subdivisions of the system compared to the commander's stated operational objectives. It is a relatively permanent assessment (compared to an FDA) that will be used for more than one mission.

Munitions Effects Assessment

7-18. The FS staff (or G3/S3 through the targeting team in accordance with FM 6-20-10) is responsible for developing the MEA concurrently and collaboratively with the BDA. For EA systems, the team depends upon the information in the EA effectiveness report to determine the effectiveness of the EA system against a particular target. The assessment forms the basis of recommendations for changes to increase the effectiveness of the following:

- EA tactics (system selection, positioning, deployment, and redeployment).
- EA techniques (spot jamming, imitative deception, intrusion).
- EA procedures (tasking and reporting channels, ES and EA system tip-off, technical data).
- EA systems (system capability, operator qualifications, mobility).

REATTACK RECOMMENDATION

7-19. Based on the BDA, the staff determines if the targeting objectives were met and if reattack is necessary. MEA helps the staff to select the best weapon system to execute the reattack. Both BDA and MEA give the staff the information needed to develop a complete reattack recommendation for the commander. In some cases, BDA and MEA may indicate that EA is not capable of meeting the targeting objective. The combat assessment process allows the staff to—

- Recognize that shortcoming in the FS plan.
- Select an alternate weapon system (lethal or nonlethal).
- Reattack the target.
- Achieve the targeting and operational objectives. (See Joint Publication 2-01.1 and FM 6-20-10 for more information on combat assessment.)

7-20. See Appendixes E, F, and G for more information on target reports, DS, and military operations on urbanized terrain (MOUT).

Appendix A

The Electromagnetic Environment

EM energy is both a natural and manmade occurrence. This energy, in the form of EM radiation, is made up of oscillating electric and magnetic fields and is propagated at the speed of light. EM radiation is measured by the frequency of its wave pattern's repetition with a set unit of time. The standard term for the measurement of EM radiation is the hertz (Hz), the number of repetitions (cycles) per second. The term **"**electromagnetic spectrum**"** refers to the range of frequencies of EM radiation from zero to infinity. The spectrum is divided into 26 alphabetically designated bands.

MILITARY ELECTROMAGNETIC SPECTRUM

A-1. Figure A-1 shows the principal military segment of the EM spectrum with the corresponding EW frequency bands and radar designations and why there is occasionally confusion when discussing frequency bands, which share names in different designation systems. The EME is the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted EM emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. The EME is the sum of—

- EM interference.
- EM pulse.
- Hazards of EM radiation to personnel, ordnance, and volatile materials.
- Natural phenomena effects of lightning and precipitation static (p-static).

A-2. P-static is created by charged precipitation particles that strike antennas and gradually charge the antenna, which ultimately discharges across the insulator, causing a burst of static.

MILITARY OPERATIONS AND ELECTROMAGNETIC ENVIRONMENT

A-3. The impact of the EME upon the operational capability of military forces, equipment, systems, and platforms is referred to as EME effects. EME effects encompass all EM disciplines, including—

- EM compatibility (EMC) and EM interference (EMI).
- EP.
- Hazards of EM radiation to personnel, ordnance (HERO).
- Volatile materials such as fuels.

- Natural phenomena effects of lightning and p-static.

A-4. Equipment and systems which operate on the principles of electromagnetism are characterized by electromagnetic vulnerability which cause them to suffer a definite degradation (incapability to perform the designated mission).

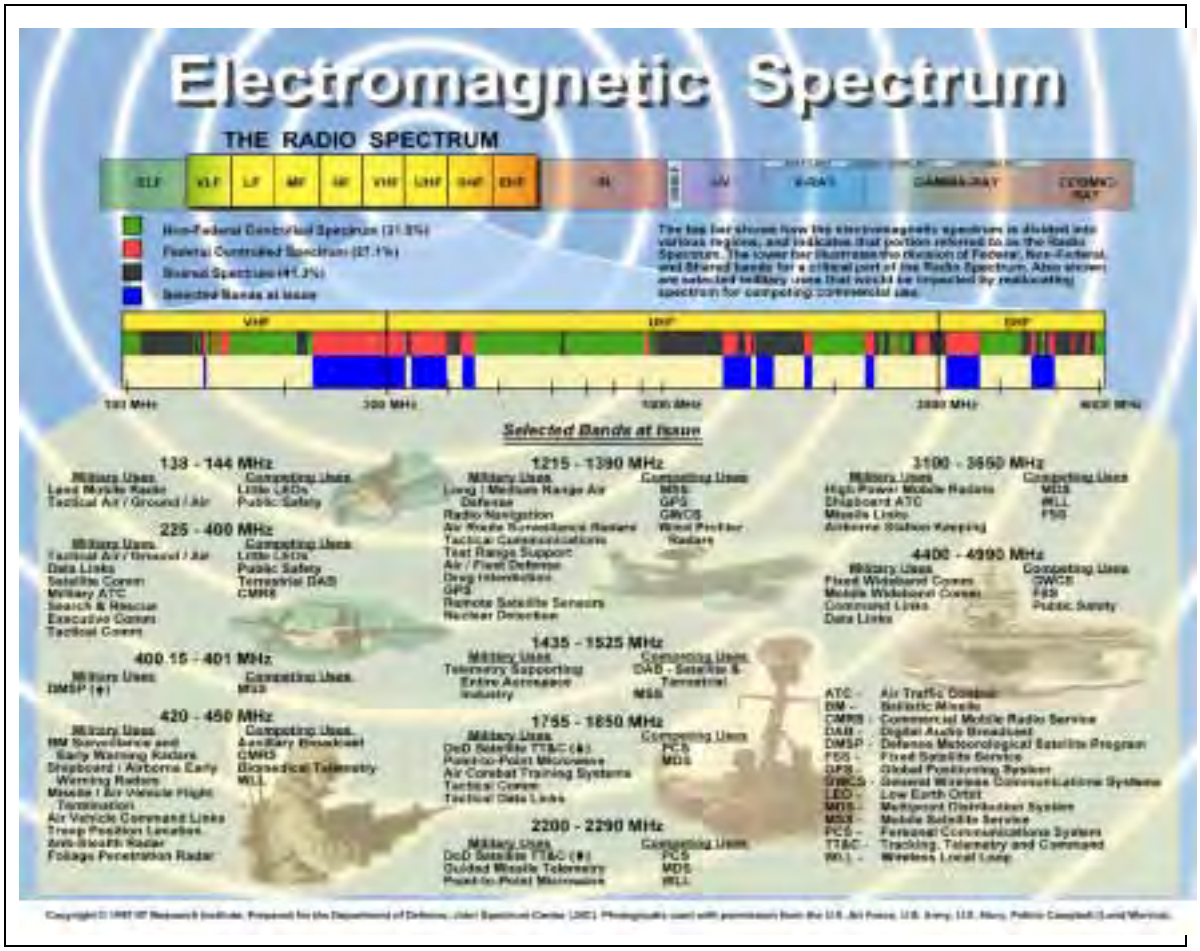


Figure A-1. Electromagnetic Spectrum

DIRECTED ENERGY IN EW

A-5. DE includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the EM spectrum. Possible applications include lasers, RF weapons, and particle beam weapons. As the development of DEW evolves, TTP must also evolve to ensure their safe, effective employment. Although some DE applications will easily fit into traditional EW roles, others will not. For example, in EW terms—

- A laser designed to blind or disrupt optical sensors is ES.

- A laser-warning receiver designed to detect and analyze a laser signal is ES.
- A visor or goggle designed to filter out the harmful wavelength of laser light is EP.

A-6. The potential for the threat's use of destructive DE weapons and other destructive RF weapons is also growing. Intelligence assets must be tasked to collect information about this threat, and joint planning must include the development of operational procedures and COAs to mitigate the effects on these weapons.

PRINCIPAL ELECTRONIC WARFARE ACTIVITIES

A-7. The principal activities used in EW have been developed over time to exploit the opportunities and vulnerabilities, which are inherent in the physics of EM energy. Although new equipment and new tactics continue to be developed, the physics of EM energy remains constant. This physical constant is the reason that the basic activities of EW remain effective despite changes in hardware and tactics. The principal activities used in EW follow.

ELECTROMAGNETIC COMPATIBILITY

A-8. EMC is the ability of systems, equipment, and devices that use the EM spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of EM radiation or response. EMC involves the application of sound EM spectrum management:

- System, equipment, and device design configuration that ensure interference.
- Free operation.
- Clear concepts and doctrines that maximize operational effectiveness.

ELECTROMAGNETIC DECEPTION

A-9. EM deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Types of EM deception are discussed below.

Manipulative EM Deception

A-10. This type of deception involves actions to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces.

Simulative EM Deception

A-11. This type of deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

Imitative EM Deception

A-12. This type of deception introduces EM energy into enemy systems that imitates enemy emissions.

EM Hardening

A-13. EM hardening consists of actions taken to protect personnel, facilities, and/or equipment by filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of EM energy.

EM Interference

A-14. EMI is any EM disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like.

EM Intrusion

A-15. EM intrusion is the intentional insertion of EM energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion.

EM Jamming

A-16. EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EM spectrum, and with the intent of degrading or neutralizing the enemy's combat capability.

Electromagnetic Pulse

A-17. EMP is the EM radiation from a nuclear explosion caused by Compton-recoil electrons and photoelectrons from photons scattered in the materials of the nuclear device or in a surrounding medium. The resulting electric and magnetic fields may couple with electrical and electronic systems to produce damaging current and voltage surges. EMP may also be caused by nonnuclear means.

Electronic Masking

A-18. Electronic masking is the controlled radiation of EM energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy ES or SIGINT, without significantly degrading the operation of friendly systems.

Electronic Probing

A-19. Electronic probing is the intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems.

Electronic Reconnaissance

A-20. Electronic reconnaissance is the detection, identification, evaluation, and location of foreign EM radiations emanating from other than nuclear detonations or radioactive sources.

Electronic Intelligence

A-21. Electronic intelligence (ELINT) is the technical and geolocational intelligence derived from foreign noncommunications EM radiations emanating from other than nuclear detonations or radioactive sources.

Electronics Security

A-22. Electronics security (ELSEC) is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications EM radiations (for example, radar).

EW Reprogramming

A-23. EW reprogramming is the deliberate alteration or modification of EW or target sensing systems or the TTP that employ them, in response to validated changes in equipment, tactics, or the EME. These changes may be the result of deliberate actions on the part of friendly, adversary, or third parties; or they may be brought about by EMI or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and target sensing systems equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems.

Emission Control

A-24. Emission control (EMCON) is the selective and controlled use of EM, acoustic, or other emitters to optimize C^2 capabilities while minimizing for OPSEC detection by enemy sensors; mutual interference among friendly systems; and/or execution of a military deception plan.

Spectrum Management

A-25. Spectrum management involves planning, coordination, and managing joint use of the EM spectrum through operational, engineering, and administrative procedure**s**, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Wartime Reserve Modes

A-26. Wartime reserve modes (WARMs) are characteristics and operating procedures of sensors, communications, navigation aids (NAVAIDs), threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. WARMs are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

IEW Support

A-27. Electronic forms of intelligence gathering (for example, SIGINT, measurement and signature intelligence [MASINT]) comprise a significant portion of the day-to-day activities of the intelligence community. The

distinction between intelligence and ES is determined by who tasks or controls the intelligence assets, what they are tasked to provide, and for what purpose they are tasked.

A-28. ES is achieved by intelligence collection, processing, and exploitation assets tasked or controlled by an operational commander. These assets are tasked to search for, intercept, identify, locate, and report sources of intentional or unintentional radiated EM energy.

A-29. The purpose of ES tasking is immediate threat recognition and other tactical actions such as threat avoidance, targeting, and homing. ES is intended to respond to an immediate operational requirement. However, the same assets and resources, which are tasked with ES, can also collect intelligence at the same time that meets other collection requirements. Intelligence collected for ES purposes normally are also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met.

Appendix B

Signal-to-Noise Ratio Reference

Signal-to-noise ratio formulas provide personnel involved in EA the tools that are necessary to compute jamming power outputs and distances. These products are necessary to fully plan and/or execute EA operations

RATIO FORMULA

B-1. The ratio formula is used to compute the maximum distance a jammer can be from a target and still be effective (Figure B-1).

$$dj = dt \sqrt[n]{\frac{Pj}{Pt\ K\left(\frac{ht}{hj}\right)^2}}$$

f	Frequency (50 MHz)
dt	Enemy transmitter location to target receiver location distance in km (9 km)
Pt	Power output of enemy transmitter in watts (5 watts)
hj	Height of jammer antenna above sear level in meters (386 meters)
Pj	Power output of the jammer in watts (1,500 watts)
ht	Height of enemy transmitting antenna above sea level (ASL) in meters (385 meters)
JSR	Jamming to signal ratio (JSR) (8:1 (9dB))
dj	Jammer location to target receiver location distance in kilometers (solve)
n	Terrain and conductivity Factor (4) 2 = Level terrain (over water, lakes, and ponds) good conductivity for a JSR of at least 2:1 3 = Rolling hills (farmland type terrain), good conductivity for a JSR of at least 4:1 4 = Moderately rough terrain (high hills), fair to good conductivity for a JSR of at least 8:1 5 = Very rough terrain (mountains or desert terrain) poor conductivity for a JSR of at least 16:1
K	Jammer tuning accuracy factor (2) 2 = For jamming FM receivers operating in the VHF range 3 = For jamming continuous wave (CW) or amplitude modulated receivers operating in the very high frequency (VHF) range

Figure B-1. Signal-to-Noise Ratio Formula

B-2. The use of this formula will provide for the creation of a range fan which, when plotted for different radios and signal strengths and broken down into varying ranges between transmitters and receivers, will allow for a

general range fan. This range fan will in turn provide the SIGINT teams with the means to effectively place teams and to determine which target areas can be affected by specific locations.

FUTURE TRENDS

B-3. The shortcoming of this formula is in its lack of any relationship to vegetation or signal frequency. These two factors affect the signal-to-noise ratio to such a degree that only a rough estimate as to a true range fan is determined. One possible solution to this problem is a system developed and designed by the Electronic Proving Ground (EPG). The Virtual Electromagnetic C4I Analysis Tool (VECAT) is designed to provide different users with powerful command, control, communications, computers, and intelligence (C4I) system analysis capabilities embedded in a user-friendly graphical user interface (GUI) environment. For example:

- A communications engineer or spectrum manager can use VECAT to plan specific communication links or perform area site analysis.
- An intelligence tester may use VECAT to plan evaluations of a sensor system immersed in a battlefield environment which would be impractical to duplicate in a field test situation.

B-4. VECAT employs terrain integrated rough earth model (TIREM) as its core EM propagation analytical engine. TIREM was developed by the Joint Spectrum Center (JSC) in the 1970s and is used for calculating EM-wave propagation loss between antennas above a point-by-point representation of the terrain elevations along an irregular profile of the earth.

B-5. TIREM evaluates the geometry of the defined path, determines appropriate modes of propagation, and applies suitable algorithms to calculate the path loss for the dominant mode. As a legacy model, TIREM suffers from lack of modern user amenities, such as GUI input interfaces and graphical output formats.

B-6. In VECAT, a powerful graphics interface is used to display the TIREM results. This allows the user to view either two- or three- dimensional (2D or 3D) data in a variety of combinations and styles. To facilitate its use, VECAT employs a Geographic Information System (GIS) and an Relational Database Management System (RDBMS) back-end. The GIS allows the user to place equipment in realistic positions. The equipment can be chosen from a database of known equipment and its deployment configuration can be stored in a database. The user can customize the calculations, thus accounting for a multitude of equipment characteristics and physical phenomena.

B-7. An important part of VECAT is the C4I standard, which is essentially the Army doctrinal dispersion of C4I assets in a geographic area of interest. With VECAT, the user can create and edit deployments and view communication links and their terrain profiles and area elevation data. VECAT provides a visual selection system, allowing the user to easily access the equipment in the deployment; the selection system permits the user to work with only those pieces of equipment satisfying specific criteria. The user can evaluate any subset of deployment. For instance, a user can

evaluate the area coverage of a specific EA asset against specific targets in the EM spectrum.

B-8. For decades, communicators have been concerned with RF propagation path loss through foliage. EPG has developed, implemented, and integrated into VECAT the EM Wave Attenuation in a Forest (EWAF) propagation model, which uses conventional inputs to estimate plausible foliage losses. The EWAF is an elementary, heuristically based foliage propagation path loss model that represents a forest as a dissipative dielectric slab lying in a more loosely half-spaced representation of the ground. Modeling the foliage by a dielectric slab provides an estimate of foliage excess-path-loss (EPL) expected in situations where meager information is available regarding wood density, conductivity, and other electrical parameters of the forest.

B-9. The EWAF model uses empirical foliage path-loss information as a basis and is therefore closely coupled to actual path-losses encountered in real-world situations. The EWAF model is not a rigorous attempt to solve the EM wave equations at the boundaries of the different representative dielectric slabs. EWAF is essentially a family of curve-fitting algorithms based on previously measured data for sparse and dense forests in the United States and Germany, as well as a very dense forest in India, where the mean annual rainfall is about 3 meters.

B-10. Features of the EWAF model include the effects of antennas within the forest, outside the forest, and above the forest; wave polarization; forest density; canopy, trunk, and undergrowth losses; antenna beamwidth; wet foliage; lush foliage; and other physical or forest conditions. The model provides a good estimator for EPL due to foliage anywhere in the world.

B-11. VECAT provides a powerful, flexible C^4I analysis tool for a wide range of users. The interface is user-friendly and provides output customized to the user's needs. VECAT is expandable and well documented. It is developed to contemporary standards and uses and reuses existing software when practical. VECAT is a modern system, available now to meet a wide variety of user's needs. VECAT will provide an easy medium in which to perform engineering analyses, evaluations, and planning studies in the following functional areas:

- Fundamental EM wave propagation analyses over digital terrain.
- Receive signal level (RSL), often incorporating 3D antenna patterns.
- LOS and terrain masking effects.
- Path profile terrain evaluations.
- Signal-to-interference ratio (S/1) and bit error rate (BER) studies.
- Electromagnetic environmental effects (E3) electric field distributions.
- Spectrum usage and signal modulation.
- Co-site EMI, remote interferer, and jammer studies.
- Fade-and-noise modeling.
- EM wave propagation through foliage.

Appendix C

Electronic Deception

Electronic Deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information and to deny valid information to an enemy or to enemy electronic dependent weapons. Electronic deception is both parts of EW and military deceptions. Normally, an electronic deception is conducted as part of a larger deception, and are seldom conducted alone. Division is the lowest level at which a deception plan can be initiated, and the commander must approve all deception plans. Historically, deception operations originate from EAC.

TYPES OF ELECTRONIC DECEPTION

C-1. Among the types of electronic deception are—

- **Manipulative Electronic Deception (MED).** Actions to eliminate, reveal, or convey misleading, telltale indicators that may be used by hostile forces.
- **Simulative Electronic Deception (SED).** Actions to represent friendly, notional, or actual capabilities to mislead hostile forces.
- **Imitative Electronic Deception (IED)**. The introduction of EM energy into enemy systems that imitates enemy emissions.

C-2. Although electronic deception is usually thought of in terms of communications, electronic deception is also conducted using digital (analog) emissions. The signals could mimic the data flows issuing from a TOC when in reality it is a jammer putting out a signal pre-recorded for this mission.

MANIPULATIVE ELECTRONIC DECEPTION

C-3. MED uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it is actually going to withdraw, the unit might transmit false FS plans and requests for ammunition.

C-4. MED is used to cause the enemy to splinter his intelligence and EW efforts to the point that they lose effectiveness. It is used to cause the enemy to misdirect his EA and ES assets and therefore cause fewer problems with friendly communications. Used in these ways, MED is an EP technique.

SIMULATIVE ELECTRONIC DECEPTION

C-5. SED uses communication and noncommunication signals to mislead hostile forces as to friendly units and/or the capabilities of friendly units. There are three types of SEDs:

- **Unit Simulation.** The use of actual equipment or specially designed simulators to indicate that a unit is in a certain location during a specified period.
- **System Simulation.** The use of systems that give off emissions peculiar to a particular organization. A countermortar or counterbattery radar is peculiar to an artillery unit; therefore, by turning on that type of radar you can indicate the probable location of an artillery unit.
- **Activity Simulation.** The operation of noncommunication emitters to imply a type or change of activity by a unit. For example, placing surveillance radars in a typical defensive array when, in fact, the intention is an attack.

IMITATIVE ELECTRONIC DECEPTION

C-6. In IED, the enemy's EM emissions are imitated to mislead the enemy. Examples include entering the enemy communication nets by using his callsigns and radio procedures, and then giving enemy commanders instructions to initiate actions which are to our advantage. Targets for IED include any enemy receiver and range from cryptographic systems to very simple, plain-language tactical nets. IED can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts are intended to cause decisions based on false information that appears to the enemy to have come from his own side.

C-7. Properly used, IED can be decisive on the battlefield. However, to be effective, IED requires electronic equipment capable of convincingly duplicating the functions of enemy equipment. IED is done if—

- (The transmitter) is compatible with the intended receiver station equipment.
- (The transmitter) has sufficient power to transmit to the receiver station.
- A proficient linguist (if voice transmissions are used).
- An operator capable of imitating the transmitting style of the enemy manual Morse operator (if continuous wave is used).

C-8. If available, however, captured enemy equipment (CEE) should be used to ensure that the technical characteristics of signals are authentic.

ELECTRONIC DECEPTION PLANNING

C-9. Electronic deception planning determines how to use EM equipment to mislead the enemy and cause him to do something to our advantage. Each

piece of electronic and associated equipment has its own electronic signature. These signatures are exploited in deception.

C-10. The G3 usually plans and supervises deceptions. The EWO is usually responsible to the G3 for the electronic deception plan. All of these personnel work with the G2 to determine the electronic activities most likely to be intercepted by enemy SIGINT.

C-11. Careful integration of electronic deception with visual, sonic, and olfactory actions is critical. What the enemy detects electronically must remain consistent with other sources of intelligence reports. Because of the reliance placed on EM radiation (for example, communication, surveillance, navigation) this aspect of deception requires close attention. Although electronic deception can be the sole act of deception, the effect is often of short duration.

C-12. The enemy's success depends upon his knowledge of your emitters. Success in MED and SED depends on understanding how your emitters appear to the enemy. The SIGINT team should keep a profile (database) of a command's voice and digital (analog) emitters. This is to determine how best to electronically portray a desired portion of that command. When planning MED and SED, it is usually necessary to consider all the command's EM emitters. It is necessary to consider what is occurring and what should occur with all EM emitters in the unit's area.

C-13. Similarly, when planning an electronic deception, consider all unit electronic activities, such as—

- Actions that support the current operation as well as those that will support the deception operation.
- All actions which must be integrated and deconflicted to prevent one activity interfering with another.

C-14. Some considerations for planning are—

- Close control and coordination will be necessary, especially during MED.
- The staff plans to avoid confusing friendly operators with deception communications or with unique returns on digital (analog) equipment.

C-15. Time is critical. Given sufficient time, the enemy can discover even the most complex electronic deception. A deception intended to deceive the enemy for two or three days must include a well-coordinated electronic deception that covers all electronic emitters.

- Adequate for a deception for only a short period just before an attack.
- The electronic deception plan can be relatively simple.
- Enemy capabilities are critical. If the enemy cannot detect your electronic emitters, the electronic deception will fail.

C-16. The commander can perform MED and SED as long as he uses only equipment under his control. IED can only be done with permission of the appropriate commander—within a division, this is usually the division commander. This restriction is to ensure that IED does not jeopardize the SIGINT effort. IED, if recognized by the enemy, will provide data concerning

the friendly ES effort. This could cause the enemy to improve his communications security (COMSEC) and procedures to reduce the effectiveness of the friendly SIGINT efforts. Coordination with higher will always occur before any MED or SED operations begin.

C-17. False emanations must be—

- On signals strong enough to reach the enemy.
- On a frequency the enemy can intercept.
- In a modulation the enemy can intercept.

ELECTRONIC DECEPTION TECHNIQUES

C-18. The following are electronic deception techniques:

- Leave a significant sample of regimental or battalion headquarters communication in place while the headquarters moves to another location.
- Broadcast false information with the intention of having the enemy receive the message and commit his forces into an area of our choosing.
- Broadcast false unit strengths, dispositions, or locations to confuse the enemy.
- Exchange operators among units or overload one unit with operators whose characteristics are probably known to the enemy.
- Place multichannel communications in a battalion area to show a larger force.
- Pad traffic on secure links to deceptively show a buildup for an attack. This technique applies to both voice and message traffic when encrypted.
- Use callsigns and frequencies to lead the enemy to incorrect net structures.

Appendix D

Message Formats

The three message types that must used in conjunction with EA are MATM (Figure D-1), MAER (Figure D-2), and MASTR (Figure D-3). These formats will vary with equipment, either voice or datalink.

MULTIPLE ASSETS TASKING MESSAGE (MATM)

(X014)

MESSAGE MAP

MESSAGE NUMBER: X014

TITLE: MULTIPLE ASSETS TASKING MESSAGE [MATM]
12345678901234567890123456789012345678901234567890123456789012
3456789

HEADING/RELOC//
1
KPOST/STA:AANNXXXXXX/ASOFDAT:NNNNNNNNA/ETRO:NNNNN
NNNA
1 2 3

/RELOC:NNAAANNNNNNNN/-/-/AZM:NNN//
4 5 6 7

AMPN/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
1
END-OF-SET MARKER//

HEADING/COMINT TASKING//
1
1KTASK
/DE/STA /TSKACT/MSNNO/IMT /PRY/ON-TIME/OFFTIME
/NN/AANNXXXXXX/AAA /AANNXX/AAAA/

Figure D-1. Example of an MATM

```
    1       2       3       4       5       6       7       8

1KCOMACT
/DE/CONOT /OCRNFREQ/DT/CN  /ACTTYP/ECH-LVL
/NN/XXXXXX/AAAAAAAA/NN/XXXXXXXXXXXXXXX/AAAAAA/A
AAAAAA//
    1       2       3       4       5       6       7

AMPN/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
    1
END-OF-SET MARKER//

1KCOMPRM
/DE/TGT-CALL-SIGN   /R-FREQ      /HIGHRF      /MOD/UK      /SIG//
/NN/XXXXXXXXXXXXXXXXX/XXXXXXXXXXX/XXXXXXXXXXX/
AAA/NNAAANNNN/A//
    1       2       3       4       5       6       7

NARR/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
    1
END-OF-SET MARKER//

    RECORD MESSAGE EXAMPLE

MESSAGE NUMBER:  X014

TITLE:  MULTIPLE ASSETS TASKING MESSAGE [MATM]

C O N F I D E N T I A L*

EXER/BLUE KNIGHT//

MSGID/MATM/ASAS 9 ID/0723/JUN//

HEADING/RELOC//

KPOST/STA:D00901A/ASOFDAT:06251900Z/ETRO:06252300Z
/RELOC:16MAB76214955/-/-/AZM:062//
```

Figure D-1. Example of an MATM (continued)

```
AMPN/CONTACT HQ WHEN TEAM IS FULLY OPERATIONAL//

HEADING/COMINT TASKING//

1KTASK
/DE/STA        /TSKACT/MSNNO /IMT /PRY/ON-TIME/OFFTIME
/01/Q15101A     /ADD   /362491/CDF /  3/252330Z/260000Z
/02/Q15101B     /ADD   /362521/CDF /  2/260400Z/260430Z//

1KCOMACT
/DE/CONOT /OCRNFREQ/DT/CN       /ACTTYP/ECH-LVL
/01/XXXXXX/ONCE    /30/XXXXXXXXX      /RVRCRS/RGT
/02/XXXXXX/ONCE    /30/XXXX        /WITHDR/DIV//

AMPN/ENSURE ANY NEW ENTITIES ARE IDENTIFIED//

1KCOMPRM
/DE/TGT-CALL-SIGN    /R-FREQ    /HIGHRF    /MOD/UK      /SIG
/01/VB262          /  23.254GHZ/        -/SSB/16MAB7429/S
/02/AK794          /  241.6 MHz/        -/CW /16MAB7926/W//

NARR/IF ANY NEW TARGETS ARE LOCATED DURING THE
SEARCH, REPORT THEM IMMEDIATELY//

HEADING/ELINT TASKING//  MESSAGE MAP (CONTINUED)
    1

1KTASK
/DE/STA   /TSKACT/MSNNO /IMT /PRY/ON-TIME/OFFTIME
/NN/XXXXXXXXXX/AAA   /XXXXXX/AAAA/
N/NNNNNNA/NNNNNNA//
    1       2       3       4       5       6       7       8

1KELACT
/DE/ELNOT       /OCRNFREQ /DT/R-FREQ           /HIGHRF
    /EFC/TGT-EQUIP-NAME
/NN/XXXXX/AAAAAAAA/NN/XXXXXXXXXXX/XXXXXXXXXXX/A
A /XXXXXXXXXXXXXXXXX//
    1       2       3       4       5       6       7       8

1KELPRM
```

Figure D-1. Example of an MATM (continued)

```
/DE/PRFPRI        /PULSDUR /SCAN-TYPE
/NN/AAAXXXXXXXXXXX/NNNNNNN/AAAA//
    1        2        3        4

NARR/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
    1
END-OF-SET MARKER//

HEADING/EA TASKING//
    1
1KTASK
/DE/STA             /TSKACT/MSNNO /IMT /PRY/ON-TIME/OFFTIME
/NN/AANNXXXXXX/AAA   /AANNXX/AAAA/
N/NNNNNNA/NNNNNNA//
    1        2        3        4        5        6        7        8

1KTGTJAM
/DE/OCRNFREQ/DT/RF-
BANDWIDTH/RMOD/TMOD/AZM/POLTGT/ERP/ACTTYP/ECH-LVL
/NN/AAAAAAAA/NN/    NNNNNNNN/AAA /AAA /NNN/AAAAA /NN
/AAAAAA/AAAAAAA//
    1        2        3        4        5        6        7        8        9        10
    11

5KJAMFRQ
/DE/LOWRF     /HIGHRF     /R-FREQ     /TGT-CALL-SIGN    /SIG
/NN/XXXXXXXXXAAA/XXXXXXXXXAAA/XXXXXXXXXAAA/XXXXXX
XXXXXXXXXXX/A//
    1        2        3        4        5        6

5KGUARD
/DE/LOWRF     /HIGHRF     /R-FREQ
/NN/XXXXXXXXXAAA/XXXXXXXXXAAA/XXXXXXXXXAAA//
    1        2        3        4

AMPN/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
    1
END-OF-SET MARKER//
```

Figure D-1. Example of an MATM (continued)

```
NARR/FREE-TEXT INFORMATION OF UNLIMITED LENGTH
FOLLOWED BY AN
    1
END-OF-SET MARKER//

HEADING/ELINT TASKING//

1KTASK
/DE/STA       /TSKACT/MSNNO /IMT /PRY/ON-TIME/OFFTIME
/01/D00901A   /ADD  /386111/DF  /  3/260730Z/260900Z
/02/D00903D   /ADD  /386142/COL /  2/261430Z/261730Z//

1KELACT
/DE/ELNOT/OCRNFREQ/DT/R-FREQ    /HIGHRF     /EFC/TGT-EQUIP-
NAME
/01/XXXX /HOURLY  /90/   27.60MHz/          -/PW /FC RADAR
/02/XXXX /HOURLY  /60/    830MHz/          -/PW /EW RADAR//

1KELPRM
/DE/PRFPRI       /PULSDUR /SCAN-TYPE
/01/PRF18.5      /   0.005/CON
/02/PRF80        /  55.700/CIR//

NARR/IF ANY NEW TARGETS ARE LOCATED DURING THE
SEARCH, REPORT THEM IMMEDIATELY//

HEADING/EA TASKING//

1KTASK
/DE/STA       /TSKACT/MSNNO/IMT /PRY/ON-TIME/OFFTIME
/01/Q15101A   /ADD  /3210A/EA /  3/261415Z/261430Z
/02/Q15106B   /ADD  /3225A/EA /  3/261830Z/261900Z//

1KTGTJAM
/DE/OCRNFREQ/DT/RF-
BANDWIDTH/RMOD/TMOD/AZM/POLTGT/ERP/ACTTYP/ECH-LVL
/01/ONCE   /15/    9624.20/MCW /MCW /274/ELIPL / 62/COMM  /RGT
/02/ONCE   /30/    4762.55/ASB /ASB /169/HORIZ / 46/SEARCH/DIV//

5KJAMFRQ
/DE/LOWRF     /HIGHRF     /R-FREQ     /TGT-CALL-SIGN    /SIG
```

Figure D-1. Example of an MATM (continued)

/01/ 156.25MHz/ 826.75MHz/ 425.70MHz/MN724 /R
/02/ 725.80MHz/ 270.50MHz/ 195.60MHz/AB265 /R//

5KGUARD
/DE/LOWRF /HIGHRF /R-FREQ
/01/ 255.70MHz/ 1988.75MHz/ 395.25MHz//

AMPN/TIP ANY NEW TARGETS FOUND TO DF//

NARR/REPORT ALL TARGETS THAT COULD NOT BE JAMMED//

Figure D-1. Example of an MATM (concluded)

MULTIPLE ASSETS EFFECTIVENESS REPORT (MAER)

UNCLASSIFIED
APPENDIX I ACCS-A3-500-004
Printed: 20-AUG-1999 25-OCT-1993
(U) INDEX REFERENCE NUMBER : S301 STATUS: AGREED DATE: 22-JAN-1993
---------- ------ ----
MTF IDENTIFIER : MAER

MESSAGE TEXT FORMAT NAME : MULTIPLE ASSETS EFFECTIVENESS REPORT

FUNCTION OR PURPOSE : THE MAER IS USED TO REPORT THE EXTENT OF MISSION EFFECTIVENESS
---------- (POSITIVE OR NEGATIVE) TO THE TASKING AUTHORITY.

SPONSORS :

RELATED DOCUMENTS :

Figure D-2. Example of an MAER

MESSAGE TEXT FORMAT :

SEG RPT OCC SETID SEQ FIELD OCCURRENCE SET FORMAT NAME

--- --- --- ----- --- ---------- ----------

© EXER 1 /M/O// EXERCISE IDENTIFICATION

(O) OPER 2 /M/O/O/O// OPERATION IDENTIFICATION DATA

(M) MSGID 3 /M/M/O/O/O/O// MESSAGE IDENTIFICATION

(O) REF 4 /M/M/M/M/O/O/*O// REFERENCE

© AMPN 5 /M// AMPLIFICATION

© NARR 6 /M// NARRATIVE INFORMATION

(M) HEADING 7 /M// EA, EP, COMINT, ELINT, IMINT,

(M) KASDEG 8 /M/O// ASSET DESIGNATOR

(M) RMKS 9 /M// REMARKS

(O) DECL 10 /M// MESSAGE DOWNGRADING OR

NATURAL LANGUAGE EQUIVALENT: THE FOLLOWING CONDITIONAL SETS/FIELDS ARE MANDATORY AS INDICATED:

---------- EXER: IF MESSAGE IS IN SUPPORT OF AN EXERCISE THAT HAS A DESIGNATED CODE NAME OR NICKNAME. USE OF SETS EXER AND OPER ARE MUTUALLY EXCLUSIVE, I.E., IF CONDITIONS FOR SET EXER ARE SATISFIED, SET OPER CANNOT BE USED IN THIS MESSAGE. IF CONDITIONS FOR NEITHER SETS EXER OR OPER ARE SATISFIED, NEITHER SET WILL BE USED IN THIS MESSAGE.

AMPN: IF FLD 2 OF SET REF IS COMMUNICATION TYPE AND ONLY ONE REFERENCE IS USED, OR ADDITIONAL INFO RELATING TO SET REF IS REQUIRED.

NARR: IF SET REF IS REPEATED ONE OR MORE TIMES AND FLD 2 OF ONE OR MORE SETS REF CITES COMMUNICATION TYPE, OR ADDITIONAL INFORMATION RELATING TO SETS REF IS REQUIRED.

Figure D-2. Example of an MAER (continued)

REVISION DATE : 22-JAN-1993

UNCLASSIFIED MSG MAP-S301-1

Figure D-2. Example of an MAER (concluded)

MULTIPLE ASSETS STATUS REPORT (MASTR)

UNCLASSIFIED
APPENDIX I ACCS-A3-500-004
Printed: 20-AUG-1999 25-OCT-1993
(U) INDEX REFERENCE NUMBER : S304 STATUS: AGREED DATE: 22-JAN-1993

MTF IDENTIFIER : MASTR

MESSAGE TEXT FORMAT NAME : MULTIPLE ASSETS STATUS REPORT

FUNCTION OR PURPOSE : THE MASTR IS THE VEHICLE BY WHICH CORPS AND DIVISION ASSETS REPORT OPERATIONAL STATUS OR ANY CHANGES IN CAPABILITY TO THE ASAC.

SPONSORS :

RELATED DOCUMENTS :

MESSAGE TEXT FORMAT :

Figure D-3. Example of an MASTR

```
SEG RPT OCC SETID     SEQ FIELD OCCURRENCE              SET
FORMAT NAME
--- --- --- -----     --- ----------------              ---------------
     (C) EXER       1 /M/O//                    EXERCISE
IDENTIFICATION
     (O) OPER       2 /M/O/O/O//                OPERATION
IDENTIFICATION DATA
     (M) MSGID      3 /M/M/O/O/O/O//            MESSAGE
IDENTIFICATION
     (O) REF        4 /M/M/M/M/O/O/*O//         REFERENCE
     (C) AMPN       5 /M//                      AMPLIFICATION
     (C) NARR       6 /M//                      NARRATIVE INFORMATION
     (C) HEADING    7 /M//                      COMINT, ELINT OR EA
ASSET STATUS
   * (C) KPOSTM     8 /M/M/M/C/C/C/C//          COMINT, ELINT
OR EA ASSET STATUS
     (C) AMPN       9 /M//                      AMPLIFICATION
     (O) HEADING   10 /M//                      IMINT ASSET STATUS
     (C) AMPN      11 /M//                      AMPLIFICATION
     (C) HEADING   12 /M//                      REMBASS ASSET
STATUS
   * (C) KSTAT     13 /M/M/M/M/M/M/C/C/C//     REMBASS
ASSET STATUS
     (C) AMPN      14 /M//                      AMPLIFICATION
     (C) HEADING   15 /M//                      HUMINT ASSET STATUS
   * (C) KHSTAT    16 /M/M/M/C/C//             HUMINT ASSET
STATUS
     (C) AMPN      17 /M//                      AMPLIFICATION
     (O) HEADING   18 /M//                      OPSEC ASSET STATUS
     (C) AMPN      19 /M//                      AMPLIFICATION
     (O) DECL      20 /M//                      MESSAGE DOWNGRADING
OR


 NATURAL LANGUAGE EQUIVALENT:  THE FOLLOWING
CONDITIONAL SETS/FIELDS ARE MANDATORY AS INDICATED:
EXER: IF MESSAGE IS IN SUPPORT OF AN EXERCISE THAT HAS A
DESIGNATED CODE NAME  OR NICKNAME. USE OF SETS EXER
AND OPER ARE MUTUALLY EXCLUSIVE, I.E., IF CONDITIONS FOR
SET EXER ARE SATISFIED, SET OPER CANNOT BE USED IN THIS
MESSAGE.   IF CONDITIONS FOR NEITHER SETS EXER OR OPER
ARE SATISFIED, NEITHER SET WILL BE USED IN THIS MESSAGE
```

Figure D-3. Example of an MASTR (concluded)

Appendix E

Example Formats and Target Report

The targeting products developed during the targeting process are actually tools. They are used by the commander, the targeting team, and supporting and supported units. The products allow them to control and synchronize targeting effectively and efficiently. As such, there are no prescribed formats. Each unit will develop tools that work best for that unit. Factors to consider in developing formats:

- Type and level of the command.
- Operating environment.
- Assets available.
- Missions.
- SOPs.

GENERAL

E-1. Regardless of the formats used, the **decide, detect, deliver,** and **assess** methodology associated with the command decision cycle must be followed.

E-2. The purpose of this appendix is to provide a menu of formats. They may be copied and used as is, or the targeting team can modify them to suit the needs of the command. Also provided is a sample target report format which can be used or modified as desired.

E-3. These formats are not yet integrated into supporting C^4I systems such as tactical fire (TACFIRE) direction system, Advanced Field Artillery Tactical Data System (AFATDS), Warrior, and ASAS. The need for automation support is apparent and emerging. C^4I systems will be asked to incorporate similar targeting formats.

HIGH-PAYOFF TARGET LIST

E-4. The modified HPTL at Figure E-1 is the basic format described in Chapter 4.

EVENT OR PHASE: _____		
PRIORITY	CATEGORY	TARGET

Figure E-1. High Payoff Target List

TARGET SELECTION STANDARDS

E-5. TSSs are comprised of the essential elements as shown in the sample entries in Figure E-2. HPT refers to the designated HPTs which the collection manager is tasked to acquire.

HPT	TIMELINESS	ACCURACY
COPs	3 hrs	150 m
RSTA	30 min	150 m
2S3	30 min	500 m
M-46	30 min	500 m
ADA	15 min	500 m
CPs	3 hrs	500 m
Ammunition	6 hrs	1 km
Maneuver	1 hr	150 m

Figure E-2. Example TSS

ATTACK GUIDANCE MATRIX

E-6. The AGM (Figure E-3) provides guidance on what HPTs should be attacked and when and how. The AGM consists of the following.

- HPTL. A prioritized list of HPTs by phase of the operation.
- WHEN. The time the target should be engaged.
- HOW. The attack system that will engage the target.
- EFFECT. The desired effects on the target or target system.
- REMARKS. Remarks concerning whether or not BDA is required, whether coordination must take place, and so forth.

PHASE/EVENT: Attack through the security zone				
HPTL	**WHEN**	**HOW**	**EFFECT**	**REMARKS**
COPs	P	GS arty	N	Plan in initial prep
RSTA and COPs	P	GS arty	N	Plan in initial prep
2S1 and 2S3	P	MLRS	N	Plan in initial prep
2S6, SA9, and SA13	P	GS arty	S	SEAD for aviation operations
Regiment CP	A	MLRS	N	
Reserve Battalion	P	Avn Bde	D	Intent to attack reserve battalion in EA HOT
C^2	P	TLQ-17	EW	Deny communications to C^2
LEGEND: I = IMMEDIATE A = AS ACQUIRED P = PLANNED Prep = Include in preparation fires			S = SUPPRESS N = NEUTRALIZE D = DESTROY EW = JAMMING or other OFFENSIVE EW	

Figure E-3. Example AGM

SENSOR OR ATTACK MATRIX

E-7. The sensor or attack matrix is a tool used to determine if organic sensors and attack systems can acquire and attack the HVTs for each critical event or phase of the battle (Figure E-4). Use additional sheets as necessary.

EVENT: ATTACK THROUGH SECURITY ZONE							
HVT	COPs RSTA	M46	2S3	MAIN FWD CPs	AMMO	MANEUVER	HVT
SENSOR							ATK SYSTEM
EPW team					S	A	Mnvr brigade
CI team			S		S		AHB
LRSD	S/A						D/A 155-mm SP
TRQ-32	S	A	A	S			D/A MLRS
ALQ-151		A	A	S			C/A MLRS
PPS-5				A			EW: TLQ-17
OH-58D	S			A			
TRQ-32				S/A			TLQ-17
Q36 CMR			S			A	CAS: 20/day

S = SENSOR with capability to acquire target A = ATTACK system with capability to engage target.
D/A = Division/Artillery C/A = Corps/Artillery

Figure E-4. Example Sensor or Attack Matrix

OPTIONAL HIGH PAYOFF TARGET LIST AND ATTACK GUIDANCE MATRIX

E-8. The examples shown in Figures E-5 and E-6 are simpler than those discussed in Chapter 3 and combine the formats. This allows the targeting team to specify HPTs in priority order with as much detail as desired. It also allows the team to immediately specify the **when**, **how**, and **restrictions** information for attack of the HPTs. The HPTL and AGM will likely change as the battle progresses from one phase or critical event to another. Therefore, a separate HPTL and AGM can be prepared for each phase of the battle.

EVENT OR PHASE: Attack through security zone.

HIGH-PAYOFF TARGET LIST	ATTACK GUIDANCE WHEN, HOW, RESTRICTIONS
COPs	Prep, A, N, cannon and/or rocket.
RSTA	Prep, A, N, cannon and/or rocket.
2S3	Prep, I, N, cannon and/or rocket.
M46	Prep, I, N, cannon and/or rocket. Use corps assets beyond PL Diamond.
ADA	SEAD, P, S
CPs	Prep, A, D
Ammunition	Prep, A, D
Maneuver and reconnaissance patrols	Prep, A, N

LEGEND: I = IMMEDIATE S = SUPPRESS
A = AS ACQUIRED N = NEUTRALIZE
P = PLANNED D = DESTROY

Prep: Include in preparation fires.

Figure E-5. Example of HPTL-AGM (Option 1)

PRIORITY	CATEGORY	HPTs	WHEN	HOW	COMMENTS
1	ADA	SA-8, SA-11, SA-15	A/P	N	
2	FS	Arty CP MRL, C/B weapons	1	N/EW	Coord with ES
3	ENGINEER	Bridging units, pontoons	A	N	
4	C^3	MRR, MRD CP	A	N/EW	Coord with ES
5	MANEUVER	1st Ech/lead div	A	N	
6	RSTA	Fwd intercept DF nodes	I	N	
-	NUKE/CHEM		I	D	Need BDA
-	RECON		A	N	Not HPT
-	CLASS III POL		A	N	Not HPT
-	CLASS V AMMO		A	N	Not HPT
-	CLASS IX MAINT		A	N	Not HPT
-	LIFT		A	N	Not HPT
-	LOC		A	N	Not HPT

LEGEND: I = IMMEDIATE S = SUPPRESS
A = AS ACQUIRED N = NEUTRALIZE
P = PLANNED D = DESTROY

Figure E-6. Example of HPTL-AGM (Option 2)

TARGET SHEETS

E-9. The decision on which HVTs should or could be attacked requires knowledge of their individual vulnerabilities, locations, signatures, and functions. Also considered is the effect that an attack on them will have on the parent enemy unit. This information, when consolidated, is called a target sheet. Locally produced target sheets should contain the major sections discussed in paragraph E-10.

E-10. The construction of target sheets, as shown in Figure E-7, is simple and much of the information is readily available, although from varied sources.

- **Security Classification** of target sheet information should appear at the top and bottom.
- **Target Category** indicates to which of the 13 sets the target belongs.
- **Sheet No/Title** should be assigned to the target so it may be referenced in the future. The sheet number can be used to cross-reference the target sheet with the spreadsheet. The title refers to the type and function.

- **Function** details the specific operations and tasks that the target is expected to do. It includes the primary and secondary functions of the target and indicates any relationship to other target categories or types.
- **Description** details the number and type of vehicles and equipment in a position and the approximate number of people with the target. The description is useful in considering the types of attack systems and munitions to be used.
  - Usual distance form the current forward edge of the battle area (FEBA).
  - Expected posture of the target with respect to camouflage and orientation.
  - Type and amount of terrain occupied.
- **Signature** describes all possible signatures to include visual, electronic, auditory, and infrared. This portion is especially useful to target acquisition and intelligence collection managers.
- **Degradation** describes the effects on the parent or associated intelligence unit when the target can no longer function. This is called the **degradation** portion.
- **Graphic Representation** aids in identifying the target and in analyzing its vulnerabilities. It may be used to help determine the effects desired against the target.

ELECTRONIC WARFARE ANNEX

E-11. The EW annex (Figure E-8) is a tool used to determine the attack system (nonlethal) for targets. The EWO will place HPTs designated by the commander onto the annex for engagement. The engagements will be synchronized with the AGM and will be tied to the ISM for queuing for engagement.

(Classification)

TARGET CATEGORY: Engineer.

TARGET SHEET NO/TITLE: GT 75/Ferry crossing site.

FUNCTION: Provide rapid crossing of water obstacles for tanks and other systems lacking amphibious capability.

DESCRIPTION: Target radius-point target.
Posture-exposed on water surface FEBA distance.
Composition: Vehicles, normally two ferries or rafts. (If the river is over 300 meters wide, there may be as many as five.)
Personnel:

SIGNATURE: Visual- (See graphic representation)
Electronic-
Other-

DEGRADATION: Forces lacking amphibious capability must find alternate means to cross.

GRAPHIC REPRESENTATION: (Omitted)

(Classification)

Figure E-7. Sample Target Sheet

SITUATION Detail enemy capabilities, communications, noncommunications, and radio-electronic combat systems. (NOTE: These may be provided in appendixes to the annexes.) Outline the higher headquarters' EW plan with any additional EW assets or resources to support the unit.

2. MISSION Detail type of nonlethal attack and the mission of this engagement.

3. EXECUTION

a. provide a brief statement of the defensive EW and electronic combat operations to be executed including priorities.

b. Identify the placement of friendly EW assets

4. SERVICE SUPPORT Detail specific support necessary for asset to remain operational.

5. COMMAND AND SIGNAL

Tabs: 1 Enemy EOB Overlay
2 Electronic Combat Target List
3 Schedule of Jamming
4 Electronic Warfare Contingency Augmentation
5 Joint Restricted Frequency List

Figure E-8. Sample EW Annex.

Appendix F

Direct Support To The Brigade

Tactical SIGINT and EW units operate normally in GS of the parent regiment, division, or corps. This support relationship is the most effective for providing SIGINT support to the commander's deep battle and information operations campaign. In the division, however, EW assets often operate in DS of the subordinate maneuver brigades. This support relationship increases the combat power of brigades and the effectiveness of EA during entry, cross-FLOT, and close battle offensive operations.

TASK ORGANIZATION

F-1. Task organization is the process of allocating available assets to subordinate commanders and establishing their command and support relationships. Formal task organization begins during COA analysis when the division commander assigns tasks to subordinate commanders and defines command and support relationships. These relationships are stated in the division OPORD and its annexes.

F-2. The MI battalion commander uses the division OPORD to task organize the battalion's EW assets. Annex A (Task Organization), Annex B (Intelligence) and Annex T (Electronic Warfare) provide the commander the information needed to allocate EW assets and support. Normally, the task organization for organic EW assets is not stated in Annex A but expressed as requirements in Annex B and Annex T of the division OPORD. It is the MI battalion commander who lays out the EW task organization and relationships within the MI battalion OPORD.

F-3. Although FM 101-5 does offer other support relationships, the most common relationship for MI units places EW and intelligence assets in a DS role to the maneuver brigade. To provide DS EW support, the MI battalion commander has two basic options for command relationships: GS-reinforcing and DS.

GENERAL SUPPORT-REINFORCING

F-4. The GS MI company commander retains command of the EW assets. Since effective EA requires proximity to the enemy, this command relationship requires the GS MI company commander to maneuver, control, and supply the EW assets over an extended AO. It does, however, support rapid redirection of support between GS and DS with minimum disruption to command and technical control. This relationship is appropriate for short duration offensive missions, during defensive operations, or when the size of the AO is small enough to enable effective C^2.

DIRECT SUPPORT

F-5. The battalion commander attaches the EW assets from the GS MI company to the DS MI company. This relationship improves the synchronization of EA with the brigade FS plan. It also adds additional logistic burden on the DS MI company and increases the company's "footprint" (physical and communications) within the brigade's AO. This relationship is recommended for entry and cross-FLOT operations, movement to contact situations, and extended offensive operations where EA is a significant combat multiplier in the close battle.

F-6. When the MI battalion FRAGO or OPORD arrives, the GS MI company commander coordinates the linkup between the EW assets and the DS MI company. The commander issues a FRAGO to the EW assets that includes departure time, routes, linkup location and time, and pertinent command and signal instructions. Attachment is effective upon linkup between the EW assets and the DS MI company. The DS MI company commander integrates the EW assets into the unit and familiarizes the officer or NCOIC with the brigade's mission and AO. The attachment remains in effect until the MI battalion commander orders a change to the task organization or the EW assets complete the mission as specified by criteria (event, time, or location) in the OPORD.

ORGANIZATION AND OPERATIONS

F-7. EW assets attached to a DS MI company vary in size and capability based on the mission and unit. In heavy divisions, the MI battalion traditionally attaches a C&J platoon to the DS MI company supporting an armored or mechanized brigade. The C&J platoon consists of a headquarters element, a TA team, a voice intercept team, and an EA team. The headquarters element and the analysis team collocate with the DS MI company ACT. This physical collocation ensures that EW is integrated into the brigade's concept of operation and allows the S2 to leverage the combined analytic power of the ACT and the TA team. The DS MI company works with the brigade S3 to ensure intercept and EA positions are coordinated with brigade for terrain management and security purposes. Once coordinated, the intercept and attack teams use the same TTP described in Chapters 5 and 6 to move to and occupy sites.

F-8. The brigade uses the same process described in Chapter 4 to plan and execute EW operations. While the overall process remains the same, some roles and responsibilities are shifted and consolidated at brigade level. Some of these changes are discussed below.

ELECTRONIC WARFARE OFFICER

F-9. At brigade level, the C&J platoon leader assumes the special staff officer role and responsibilities of the EWO.

TARGET DEVELOPMENT

F-10. The TA team provides the ACT a scaled-down version of the ACE SIGINT team at division. The size of the team and the nature of brigade level operations limit the degree of EW target development that the team

performs. At this level, the team's primary tasks are to assist the ACT in maintaining the enemy situation picture and MM of subordinate EW assets. Both tasks rely on the team's low-level analysis of C&J platoon's intercepts, broadcast reports received from the common ground station, and technical support from the ACE. The SIGINT analyst in the team performs target value analysis and target nomination based on the understanding of the current situation derived from these information sources. More detailed analysis of potential enemy electronic targets must come from the ACE. Since the team lacks an organic processor, it must receive ACE EOB, SIGINT templates, and EW targeting data from the ACE.

COMBAT ASSESSMENT

F-11. When required, operators of the intercept and EA systems perform the initial assessment of the effects of their EA missions. The operators pass the assessment and technical data to the TA team. The TA team consolidates the assessments and forwards them the C&J platoon leader. The C&J platoon leader, as the EWO, evaluates the operator assessments and provides an evaluation of the effectiveness of EA missions to the S2 and the FSCOORD. The S2 incorporates the evaluation into the BDA of the target while the FSCOORD rolls the information into the overall combat assessment. Based on the C&J platoon leader's evaluation and the S2's BDA, the FSCOORD makes a reattack recommendation to the commander.

Appendix G

Military Operations on Urbanized Terrain

This appendix discusses the difficulties and restrictions on ES and EA in MOUT environments. These problems are hard to overcome.

G-1. Buildings diffract radio signals, making DFs highly inaccurate, unless systems have LOS. This in turn makes the use of EA difficult without accurate antenna orientation towards the target. The diffraction also hampers the ES if signals are at the threshold levels for intercept but are not intercepted due to the diffraction.

G-2. Use of terrain to lay landlines not readily detectable by friendly forces, (for example, the use of sewer systems) prevents the use of ES or EA on those communications. Urban environments favor the use of couriers to maintain C^2 channels. A modern adversary in an urban environment can make use of secure Internet service to pass information (for example, passing calls for fire via the Internet).

G-3. SIGINT teams use EOB to identify threat communications systems and their critical nodes. Development of the EOB begins with MOUT IPB in which analysts template the EM spectrum and describe how the threat uses it. National level SIGINT teams and assets provide additional information which analysts use to refine the EOB and to support future developments in the EOB. Other elements, such as PSYOP teams, may contribute to the development of the EOB by providing information on communications architecture and critical nodes of public information systems.

G-4. The EWO uses EOB information developed by the SIGINT team to develop HPTs for specific COAs, and during the targeting process to determine targets for EA. The EWO also determines the support necessary to engage targets with assets from higher. During MOUT, IPB analysts can expect to find three critical communications systems common to most MOUT environments.

- Radio and Television. Radio and television stations provide the threat with mass communication, over a large portion of the battlefield. This communication will also give the threat a propaganda tool.
  - Advantage: Easily monitored with ES, one-way communication, and digitally not encrypted.
  - Elimination: The strong signal generated by radio and television stations are easily located with ES, After location, three ways remain to deal with radio and television stations: lethal fires, nonlethal fires (EA), or capture with friendly forces.

- Telephone and Cellular Phone. Telephone systems provide a landline capability that is impossible for division tactical SIGINT assets to

monitor or engage with EW. National assets are available, but the EWO or collection manager must request these assets in advance to monitor and engage this system. Cellular phones, while not depending upon landlines, depend upon relay station and satellite communications, some of these communications; can be monitored by divisional assets while others require national assets support.

- Advantage: Infrastructure is not designed to function after being engaged with lethal fires. Cellular phones are dependent upon critical uplinks and are limited by terrain and weather conditions.
- Elimination: EOB provides the critical nodes of telephone system for targeting. These nodes can be engaged with lethal fire or nonlethal national assets. The capture of this system provides a large database and critical information for targeting (for example, location and function of threat units using the telephone system).

- Internet. The Internet provides the threat a system for secure communications. This landline communication system is difficult to monitor or engage. Coordination with the IO cell will provide support and experience on how to best engage this target.
  - Advantage: Infrastructure provides unlimited access for friendly forces into threat communications; it has no redundancies to prevent the shutting down of this communication system after being engaged with lethal fire.
  - Elimination: The IO cell provides the critical nodes of this communication system. National assets either with EA (DE) or with information warfare assets can engage these nodes. IO support for engagement of the Internet is critical due to the expertise and scope of the IO personnel.

G-5. Aggressive and focused use of EA is critical in a MOUT environment. The threat C^2 nets are critical targets. These nets provide the threat the ability to shape the battlespace to their advantage. In this constrained environment, where the environment favors the defender, the added advantage of a strong C^2 net causes numerous difficulties culminating in unacceptably high losses.

G-6. Hospitals, ambulances, fire fighters, and other agencies rely on the use of telephones and Internet services to provide humanitarian assistance to numerous noncombatants: to disrupt these and cause a high loss of life to noncombatants must be weighed against the mission priority. These resources must be left intact, if possible, to provide services to maintain the populace. Friendly forces must curtail their EA of communication resources due to the ROE and humanitarian constraints. Civilian Affairs must be consulted before any barrage EA engagements begin, if at all possible, and must examine the legal and ethical ramifications of disrupting the noncombatant use of EM.

Appendix H

Brigade Combat Team

The emerging Brigade Combat Team (Initial, Interim, and Objective) will use the same process as divisions, brigades, and squadrons to plan, execute, and assess SIGINT operations. The structure of the Brigade Combat Team, however, requires changes to where and who executes the process. This appendix describes the basic features of EA planning within the Brigade Combat Team.

ORGANIZATION

H-1. The Brigade Combat Team possesses limited resources with which to plan and direct EA. Within the MI company, the SIGINT officer in charge (from the intelligence, surveillance, and reconnaissance [ISR] integration platoon) is responsible for SIGINT RM and performs the role of the EWO. The MI company can perform only initial low-level SIGINT processing, and relies upon the Army Force or other external organization for SIGINT analysis and technical support.

H-2. The Brigade Combat Team's SIGINT assets that execute EA are found in the surveillance troop of the reconnaissance, surveillance, and target acquisition (RSTA) squadron. The SIGINT personnel (in the troop's sensor control team of the ISR section in the surveillance troop) provide technical control of the four Prophet Ground systems. The ISR integration section is imbedded within the squadron CP during deployment. The four Prophet Ground systems are divided evenly among the four sections of the multi-sensor platoon.

H-3. The Brigade Combat Team depends upon the Army Force or higher echelon organizations for SIGINT analysis and technical support. The Brigade Combat Team uses the TROJAN SPIRIT II to access these external SIGINT organizations and their databases. Some specific products developed outside the Brigade Combat Team's MI company include the EOB and electronic preparation of the battlefield. These products support target development, technical support, and tasking within the Brigade Combat Team.

OPERATIONS

H-4. After a COA is determined, the Brigade Combat Team's S3 convenes a targeting team to develop the HPTL, targeting portion of the DST, AGM, and BOS synchronization matrix. As a member of the targeting team, the SIGINT personnel develop the—

- EA portion of the AGM and BOS synchronization matrix.
- EW annex with SIRs supporting the EW Annex.

H-5. The EW Annex goes through the ISR planner for approval and integration into the overall ISR plan. The ISR requirements team further develops the SIRs and provides the RSTA squadron with technical support for planned SIGINT missions. The SIGINT personnel coordinate with the Army Force for SIGINT analysis products and technical support to support target development and EA operations. When necessary, the SIGINT personnel request that higher echelon organizations execute EA missions for targets that the Prophet Ground systems cannot attack.

H-6. The Squadron S3 tasks the surveillance troop based on the Brigade Combat Team's OPORDs, FRAGOs, SIRs, and EW Annex. The surveillance troop commander, with the support of the sensor control team, determines if the EW assets can accomplish the mission and, if so, tasks the multi-sensor platoon with the mission.

H-7. The sensor control team in the surveillance troop provides MM and AM. Acting as the equivalent of the TA team found in divisional C&J platoons, the sensor control team passes technical data provided by the MI company or from its own database to the multi-sensor sections being tasked to conduct the EA and supporting SIGINT missions. The sensor control team fuses JERs and MAERs from the multi-sensor sections into a single report and sends it to the MI company's ISR analysis platoon for BDA.

Glossary

AC	Active Component
2D	two dimensional (data)
3D	three dimensional (data)
A^2C^2	Army Airspace Command and Control
AA	avenue of approach
ACE	analysis and control element
ACT	analysis and control team
ADA	Air Defense Artillery
AFATDS	Advanced Field Artillery Tactical Data System
AGM	attack guidance matrix
ALO	air liaison officer
AM	asset management
AO	area of operation
AOC	Air Operations Center
ARNG	Army National Guard
Arty	artillery
ASAS	All-Source Analysis System
ASL	above sea level
ATO	air tasking order
Avn	aviation
BCD	Battlefield Coordination Detachment
BDA	battle damage assessment
BER	bit error rate
bn	battalion
BOC	Battalion Operations Center
BOS	battlefield operating system
C^2	command and control
C^3	command, control, communication
C&J	collection and jamming
C^4I	command, control, communications, computers, and intelligence
CA	combat assessment
cdr	commander

CEE	captured enemy equipment
CM	collection management
CNA	computer network attack
COA	course of action
COMINT	communications intelligence
COMSEC	communications security
COP	command observation post
CP	command post
CS	combat support
CSS	combat service support
CW	continuous wave
DE	directed energy
DEW	directed energy warfare
DF	direction finding
DOCC	Deep Operations Coordination Cell
DP	decision point
DS	direct support
DST	decision support template
E3	electromagnetic environmental effects
EA	electronic attack
EAC	echelons above corps
ELINT	electronics intelligence
ELSEC	electronics security
EM	electromagnetic
EMC	electromagnetic compatibility
EMCON	electromagnetic control
EME	electromagnetic environment
EMI	electromagnetic interference
EMP	electromagnetic pulse
EOB	electronic order of battle
EP	electronic protection
EPG	Electronic Proving Ground
EPL	excess-path-loss
ES	electronic warfare support
EW	electronic warfare
EWAF	Electromagnetic Wave Attenuation in a Forest

EWO	electronic warfare officer
EWTL	electronic warfare target list
FAIO	field artillery intelligence officer
FDA	functional damage assessment
FDC	fire direction center
FEBA	forward edge of battle area
FLOT	forward line of own troops
FM	frequency modulation
FO	forward observer
FOV	field of view
FRAGO	fragmentary order
FS	fire support
FSCOORD	fire support coordinator
GDA	general deployment area
GIS	Geographic Information System
GS	general support
GSOC	General Support Operations Center
GUI	graphical user interface
HERO	hazards of electromagnetic radiation to personnel, ordnance
HPT	high-payoff target
HPTL	high-payoff target list
hr	hour
HVT	high-value target
Hz	hertz
IED	imitative electronic deception
IEW	intelligence and electronic warfare
IO	information operations
IPB	intelligence preparation of the battlefield
IR	information requirements
ISM	intelligence synchronization matrix
ISR	intelligence, surveillance, and reconnaissance
JER	jamming effectiveness report
JFAAC	Joint Forces Air Component Commander
JFLAC	Joint Force Land
JRFL	Joint Restricted Frequency List
JSC	Joint Spectrum Center

JSR	jamming-to-signal ratio
km	kilometer
LD	line of departure
LLVI	low-level voice intercept
LOB	line of bearing
LOC	line of communication
LOS	line of sight
LPA	log periodic antenna
LPI	low probability of intercept
LRSD	long-range surveillance detachment
LTIOV	latest time information is of value
m	meter
MAER	multiple assets effectiveness report
MASINT	measurement and signature intelligence
MASTR	multiple assets status report
MATM	multiple assets tasking message
MDMP	military decisionmaking policy
MEA	munitions effects assessment
MED	manipulative electronic deception
METT-TC	mission, enemy, terrain and weather, troops, and time available-civilians
MHz	megahertz
MIJI	meaconing, intrusion, jamming, and interference
min	minute
MLRS	multiple launch rocket system
MM	mission management
MOUT	military operations on urbanized terrain
NAI	named area of interest
NAVAID	navigational aid
NCOIC	noncommissioned officer in charge
OB	order of battle
OPLAN	operations plan
OPORD	operations order
Ops	operations
OPSEC	operations security
PDA	physical damage assessment

PIR	priority intelligence requirements
plt	platoon
POC	platoon operations center
p-static	precipitation static
PSYOP	psychological operations
RDBMS	Relational Database Management System
REMBASS	Remotely Monitored Battlefield Sensor System
RF	radio frequency
RFL	restricted frequency list
RM	requirements management
ROE	rules of engagement
ROZ	restricted operation zone
RSL	receive signal level
RSTA	reconnaissance, surveillance, and target acquisiton
SEAD	suppression of enemy air defenses
SED	simulative electronic deception
S/I	signal-to-interference ratio
SIGINT	signals intelligence
SIGINT/EW	signals intelligence/electronic warfare
SIGSUM	signal summary
SINCGARS	Single-Channel Ground and Airborne Radio System
SIR	specific information requirements
SITREP	situation report
SOF	Special Operations Forces
SOP	standing operating procedure
TA	transcription and analysis
TACFIRE	tactical fire
TACREP	tactical report
TAI	target area of interest
TIREM	terrain integrated rough earth model
TRADOC	US Army Training and Doctrine Command
TSA	target system assessment
TSS	target selection standard
TTP	tactics, techniques, and procedures
USAF	US Air Force
USAR	US Army Reserve

USMC	US Marine Corps
USN	US Navy
VECAT	Virtual Electromagnetic C^4I Analysis Tool
VHF	very high frequency
WARM	wartime reserve mode

Bibliography

FM 6-20-10. TTP For Targeting Process. 8 May 1996.

FM 34-1. Intelligence and Electronic Warfare Operations. 27 September 1994.

FM 34-2. Collection Management and Synchronization Planning. 8 March 1994.

FM 34-130. Intelligence Preparation of the Battlefield. 8 July 1994.

FM 100-5. Operations. 14 June 1993.

FM 101-5. Staff Organization and Operations. 31 May 1997.

Joint Publication 2-01.1. Intelligence Support to Targeting. 23 April 1999.

Index

FM 34-45
9 June 2000

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0006901

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with initial distribution number 115797, requirements for FM 34-45.

PIN: 077921-000