Chapter 1
Electronic Counter-Countermeasures in Defense Planning

1-1. Introduction

a. Since the beginning of this century, we have been developing electronic devices for military purposes. These purposes include--

- Communicating.
- Detecting.
- Navigating.
- Identifying targets.
- Countering and monitoring hostile use of the electromagnetic spectrum.
- Retaining friendly use of the spectrum.

b. Electronic warfare (EW) uses electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum. It also involves actions taken to retain friendly use of the electromagnetic spectrum. Figure 1-1 shows the three categories of EW:

- Electronic warfare support measures (ESM).
- Electronic countermeasures (ECM).
- Electronic counter-countermeasures (ECCM).

Command, control, and communications (C^3CM) integrates operations security (OPSEC), military deception, jamming, and physical destruction. Using this integration and supported by intelligence, C^3CM denies information to the enemy and influences, degrades or destroys the enemy's C^3 capabilities. At the same time, C^3CM protects friendly C^3. ECCM reduces or eliminates the effects of hostile attempts to degrade or disrupt friendly C^3.

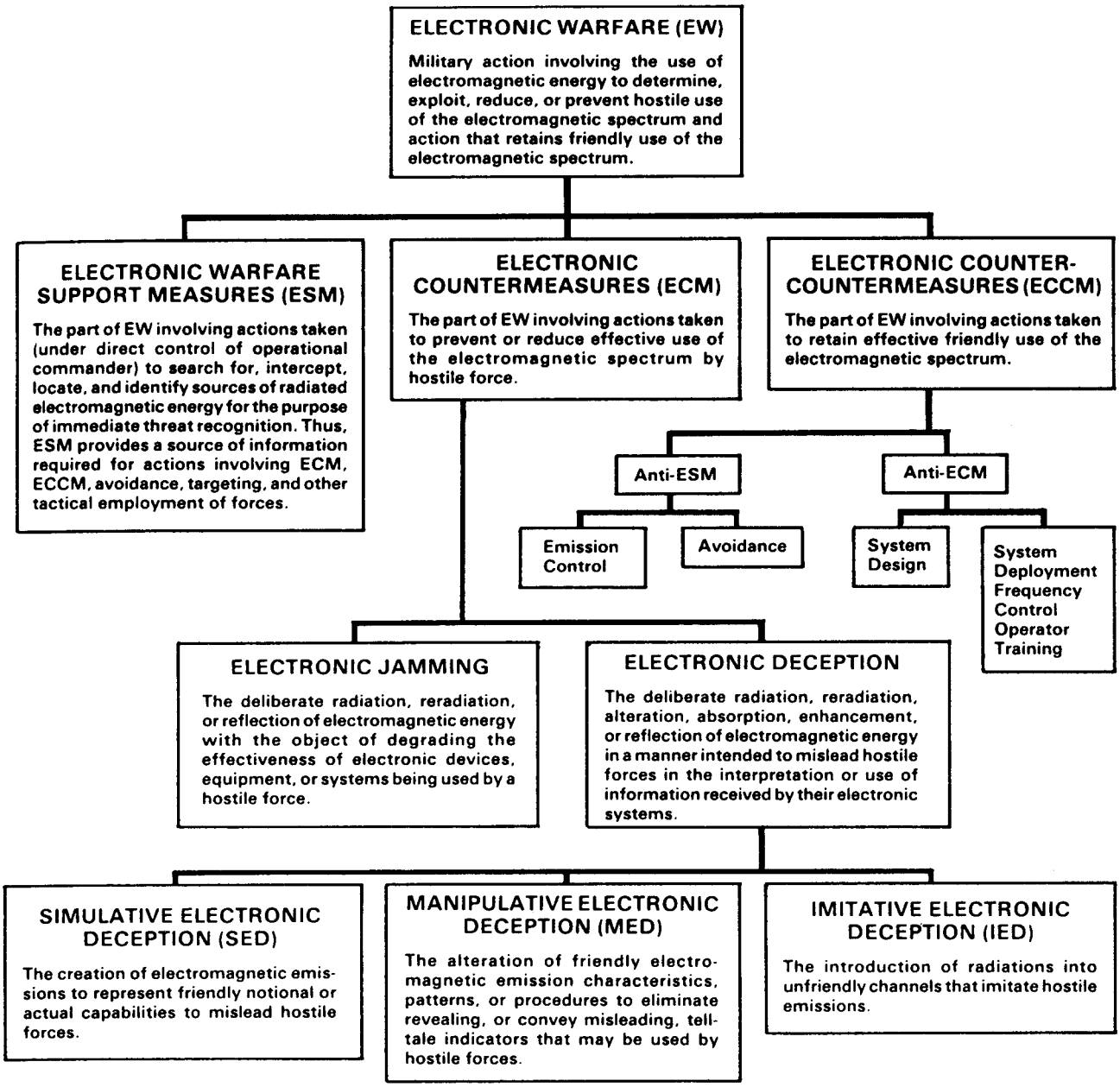

Figure 1-1. Electronic warfare functions.

c. Increased mobility and technical advances force commanders and staff to view the modern battlefield faster and clearer than before. Our units depend on effective communications to ensure the flow of critical command, control, intelligence, fire support, and service support orders and information. Therefore, commanders, staff, and radio operators must know and practice sound communications ECCM techniques.

1-2. Radio Electronic Combat

a. Most potential enemies of the US are trained in Soviet military doctrine; therefore, the following paragraphs address Soviet doctrinal approaches. To practice sound ECCM techniques, we must understand the threat to our continued use of the electromagnetic spectrum. Radio electronic combat (REC) is one such threat. REC is the total integration of EW and physical destruction resources to deny us the use of our electronic control systems. It also protects friendly electronic control systems from disruption by the enemy. Our potential enemies consider REC integral to all combat actions. They have made major investments in developing techniques and equipment to deny enemies the effective use of the electromagnetic spectrum for communications.

b. The purpose of REC is to disrupt or destroy our command and control systems at the most advantageous time. A goal of REC is to disrupt or destroy at least 60 percent of our command, control, intelligence, and weapons system communications: 30 percent by jamming and 30 percent by destructive fires. To accomplish this goal, enemy forces expend considerable effort and resources to gather combat information about their enemies. As locations are determined and units are identified, enemy forces establish priorities as follows:

- To fire suppressive fires.
- To jam communications assets.
- To deceptively enter radio nets.
- To interfere with the normal flow of their enemy's communications.

1-3. Commander's Responsibilities

a. Because REC is a real threat on the modern battlefield, commanders at all levels must ensure their units are trained to practice sound ECCM techniques. The information in this manual is a basis for this training. ECCM is a command responsibility. The greater the command emphasis given ECCM, the greater the benefits in terms of casualty reduction and combat survivability in a hostile environment.

b. In addition to ensuring their units are trained to practice sound ECCM techniques, commanders must constantly measure the effectiveness of the ECCM techniques. They must also consider ECCM while planning tactical operations. Commanders may accomplish these objectives by--

(1) Reviewing all after-action reports where jamming or deception was encountered and assessing the effectiveness of the defensive ECCM.

(2) Ensuring all encounters of interference, deception, or jamming are reported and properly analyzed by the signal officer and the G2/S2.

(3) Analyzing the impact of enemy efforts to disrupt or destroy friendly command and control communications systems on friendly operations plans.

(4) Ensuring the unit practices communications security (COMSEC) techniques daily. Units should practice--

- Changing call signs and frequencies often, but only in accordance with the signal operation instructions (SOI).
- Using approved encryption systems, codes, and authentication systems.
- Controlling emissions.

(5) Making equipment ECCM requirements known through quick-reaction capabilities as outlined in AR 105-7.

(6) Ensuring radios with mechanical or electrical faults are repaired quickly. This is one way to reduce radio distinguishing characteristics.

(7) Practicing net discipline.

1-4. Staff Responsibilities

a. The military staff is organized to assist the commander in accomplishing the mission. Specifically, the staff is organized and operates to respond immediately to the commander and subordinate units. The staff should--

(1) Keep the commander informed.

(2) Reduce the time to control, integrate, and coordinate operations.

(3) Reduce the chance for error.

(4) Relieve the commander of supervisory details in routine matters.

b. All staff officers provide information, furnish estimates, provide recommendations, prepare plans and orders, and supervise. Staff members should assist the commander in carrying out communications ECCM responsibilities.

(1) The G3/S3--

- Exercises staff responsibility for ECCM.

- Includes ESM and ECM play in all command post and field training exercises and evaluates ECCM techniques employed.

- Includes ECCM training in the unit training program.

(2) The G2/S2--

- Advises the commander of enemy capabilities that could be used to deny the unit the effective use of the electromagnetic spectrum.

- Keeps the commander apprised of the unit's signal security posture.

(3) The signal officer--

- Prepares and conducts the unit ECCM training program.

- Ensures there are alternate means of communications for those systems most vulnerable to enemy jamming.

- Ensures available COMSEC equipment is distributed to those systems most vulnerable to enemy information gathering activities.

- Ensures measures are taken to protect critical friendly frequencies from intentional and unintentional interference.

- Evaluates interference and prepares follow-up meaconing, intrusion, jamming, and interference (MIJI) reports.

- Enforces proper use of radiotelephone, ECCM, and transmission security procedures on communications channels.

- Performs frequency management duties and issues SOI booklets on a timely basis.

- Prepares and maintains a restricted frequency list of taboo, protected, and guarded frequencies.

- Prepares the ECCM and restricted frequency list appendices to the signal annex with appropriate cross-references to the other annexes (EW, OPSEC, deception) and to the SOI for related information.

1-5. Planning Categories

The enemy threat to our communications must be assessed during the planning process. We must plan to counter the enemy's attempts to take advantage of the vulnerabilities of our communications systems. As a minimum, four categories of ECCM planning must be considered: deployment, employment, replacement, and concealment.

a. Deployment.

(1) Geometry.

(a) We must analyze the terrain and determine methods to make the geometry of the battlefield work in our favor. Adhering rigidly to standard command post deployment makes it easier for the enemy to use the direction finder (DF) and aim his jamming equipment at us. Our command post vulnerability to enemy DF efforts can be greatly reduced by incorporating tactical satellite systems. We also tend to deploy our units and communications systems perpendicular to the forward line of own troops (FLOT). This greatly enhances the enemy's ability to intercept our communications because we aim our transmissions in the enemy's direction. As much as possible, we must install our terrestrial line-of-sight communications parallel to the FLOT. This will keep the primary strength of our transmissions in friendly terrain. (See Figure 1-2.) Tactical satellite communications systems are relieved of this constraint because of their inherent resistance to enemy DF efforts. Terrain features should be used when possible to mask friendly communications from enemy positions. This may mean moving senior headquarters farther forward and using more jump or tactical command posts so that commanders can continue to direct their units effectively.

(b) Locations of command posts must be carefully planned. Command post locations generally determine antenna locations. The proper installation and the siting of antennas around command posts are critical. Antennas and emitters should be dispersed and remoted so that all a unit's transmissions are not coming from one central location.

(2) System design.

(a) In designing the communications system, we must establish alternate routes of communications. This involves establishing enough communications paths so that the loss of one or more routes will not seriously degrade the overall system. The commander establishes the priorities of critical communications links. The higher priority links should be afforded the greatest number of alternate routes.

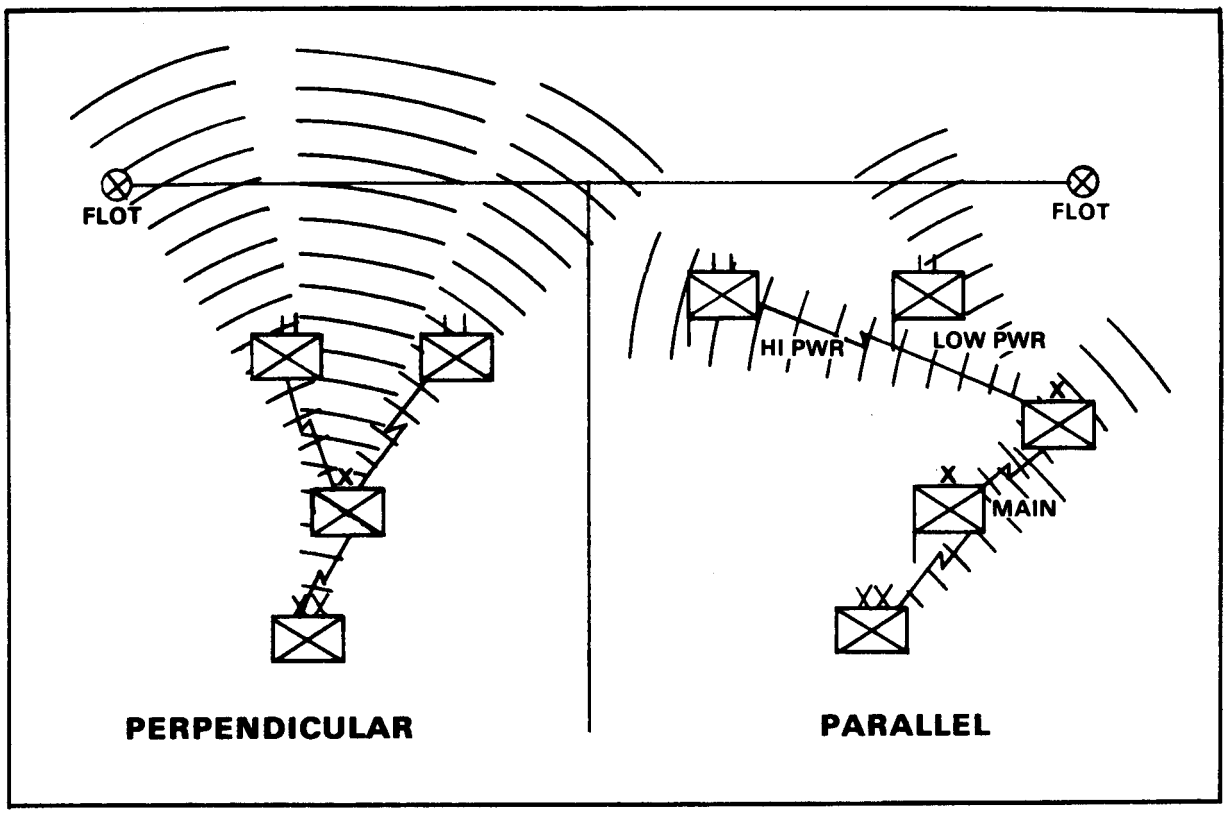

Figure 1-2. Geometry of the battlefield.

(b) Three routing concepts or some permutation of them can be used in communications: straight line, circular, and grid. (See Figure 1-3.) The straight-line system gives no alternate routes of communications. The circular system gives one alternate route of communications. The grid system gives as many alternate routes of communications as can be planned practically. Any combination of the three routing concepts may be used to establish the communications system that best supports the mission.

(c) Normally, the grid routing system allows the greatest number of alternate routes of communications. These alternate routes can enable our units to continue to communicate in spite of the enemy's efforts to deny us the use of our communications systems. They can also be used to transmit false messages and orders on the route that is experiencing interference while they transmit actual messages and orders through another route or means. A positive benefit of continuing to operate in a degraded system is that it will cause the enemy to waste assets that might otherwise be used to impair our communications elsewhere.

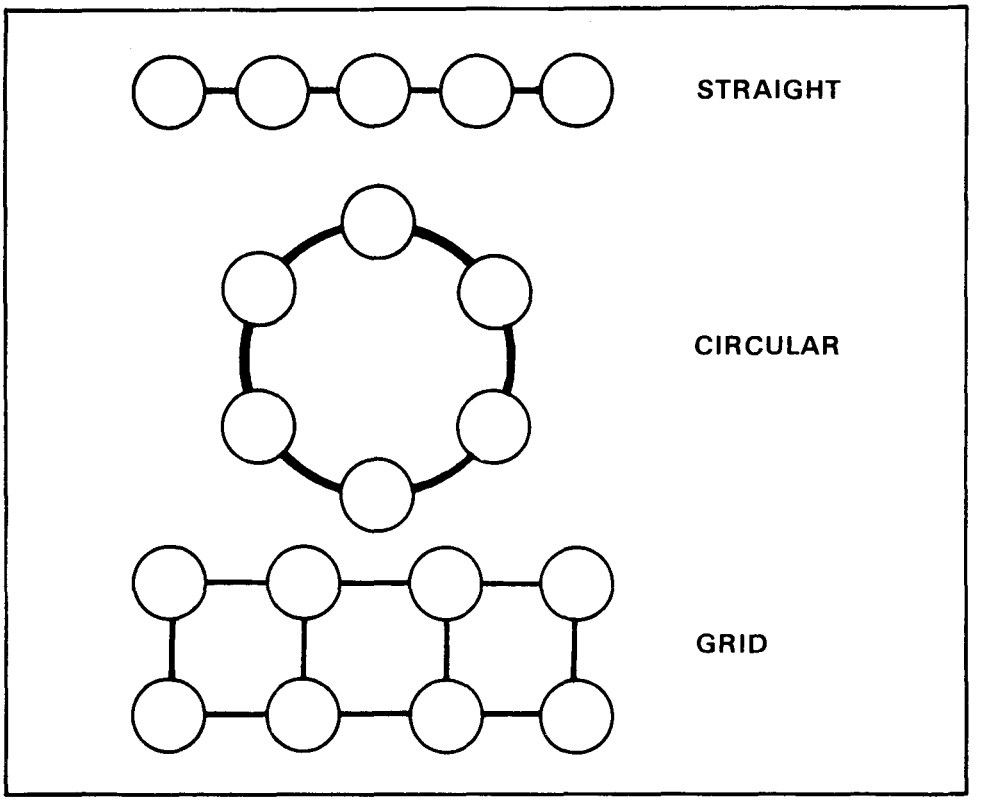

Figure 1-3. Deployment configurations.

b. Employment.

(1) We must plan to avoid establishing a pattern of communications. Enemy intelligence analysts are highly trained to extract information from the pattern as well as the text of our transmissions. If easily identifiable patterns of friendly communications are established, the enemy can gain valuable information.

(2) The number of friendly transmissions tends to increase or decrease according to the type of tactical operation being executed. Plans that prevent enemy intelligence analysts from using these increases and decreases as intelligence should be included in the battlefield deception plan. This can be done by using false peaks or traffic leveling. False peaks are created by preplanning increases in transmission traffic on a random schedule. Tactically, traffic leveling is done by preplanning messages to be sent when there is a decrease in transmission traffic. Thus, traffic leveling is used to keep the transmission traffic fairly constant. False peaks are used to prevent the enemy from connecting an increase of communications with a tactical operation. Messages transmitted for traffic leveling or false peaks must be coordinated to avoid operational security violations, mutual interference, and confusion among our equipment operators.

(3) The SOI resolve many of the problems concerning communications patterns. They allow us to change call signs and frequencies often and at random. This has long been recognized as a key in confusing enemy traffic analysts. The more we change frequencies, call signs, locations, and operators, the more confused enemy traffic analysts become. The enemy uses our SOPs to help perform his mission. We must ensure these procedures have enough flexibility to avoid establishing communications patterns.

c. Replacement.

(1) Replacement is establishing alternate routes and means of doing what the commander requires. FM voice communications are the most critical communications used by the commander during enemy engagements. As much as possible, critical systems should be reserved for critical operations. The enemy should not have access to information about our critical systems until the information is essentially useless.

(2) Alternate means of communications should be used before enemy engagements. This ensures the enemy cannot establish a data base to destroy our primary means of communications. Primary systems must always be replaced with alternate means of communications if the primary means become significantly degraded. These replacements must be preplanned and carefully coordinated; otherwise, the alternate means of communications could be compromised and become as worthless as the primary means. Users of communications equipment must know how and when to use the primary and alternate means of communications. This ensures the most efficient use of our communications systems.

d. Concealment. As much as possible, operation plans should include provisions to conceal communications personnel, equipment, and transmissions. It is difficult to effectively conceal most communications systems. Antennas must have access to free space. However, communications equipment can be concealed by installing antennas as low as possible on the back side of terrain features and behind man-made obstacles. This helps conceal the equipment while still permitting communications.

1-6. Electronic Counter-Countermeasures and Signal Security

a. ECCM and signal security are closely related. They are defensive arts based on the same principle. If the enemy does not have access to our essential elements of friendly information (EEFI), he is much less effective. The goal of signal security is to ensure the enemy cannot exploit the friendly use of the electromagnetic spectrum for communications. Signal security techniques are designed mainly to give commanders confidence in the security of their transmissions. The goal of practicing sound ECCM techniques is to ensure the continued effective use of the electromagnetic spectrum. Signal security and ECCM should be planned based on the enemy's ability to gather intelligence and degrade our communications systems.

b. We must ensure effective employment of all communications equipment by tactical commanders in spite of the enemy's concerted efforts to degrade our communications to his tactical advantage. Modifying and developing equipment to make our communications less susceptible to enemy exploitation is an expensive process. Equipment that will solve some of our ECCM problems is being developed and fielded. However, the burden of security and the burden of continued operation of all communications equipment are on the commander, staff planners, and radio operators.

c. Operators of communications equipment must know the impact of jamming and deception on our communications. Incorrect operating procedures can jeopardize the unit's mission and ultimately increase unit casualties. Operators must instinctively use preventive and remedial ECCM techniques. Maintenance personnel must know that improper modifications to equipment may cause the equipment to develop peculiar characteristics that can readily be identified by the enemy. Commanders and staff must develop plans to ensure the continued use of our communications equipment and systems. They must also be able to evaluate MIJI and after-action reports so that appropriate remedial actions can be initiated. It all starts with good training. FM 25-100 discusses proper training techniques.

d. ECCM should be preventive. In planning communications, we should consider the enemy capabilities to deny us the effective use of our communications equipment. ECCM should be planned and applied to force the enemy to commit more jamming, information gathering, and deception resources to a target than it is worth or than he has readily available. ECCM techniques must also force the enemy to doubt the effectiveness of his jamming and deception efforts.

1-7. Emission Control

The key to successful defense against the enemy's attempts to destroy or disrupt our communications is the control of our electromagnetic emissions. Transmitters should be turned on only when needed to accomplish the mission. The enemy intelligence analyst will look for patterns he can turn into usable information. If our transmitters are inactive, the enemy has nothing to work with as intelligence. Emission control can be total. For example, radio silence or radio listening silence may be directed by the commander whenever desired. Emission control should be habitual. Transmissions should be kept to a minimum (20 seconds absolute maximum, 15 seconds maximum preferred) and should contain only information critical to the mission. Good emission control makes using our communications equipment appear to be without pattern and is therefore consistent with good ECCM practices. This technique alone will not eliminate the enemy's ability to direction find a friendly transmitter but, when combined with other ECCM techniques, it will make locating a transmitter more difficult. (See Figure 1-4.)

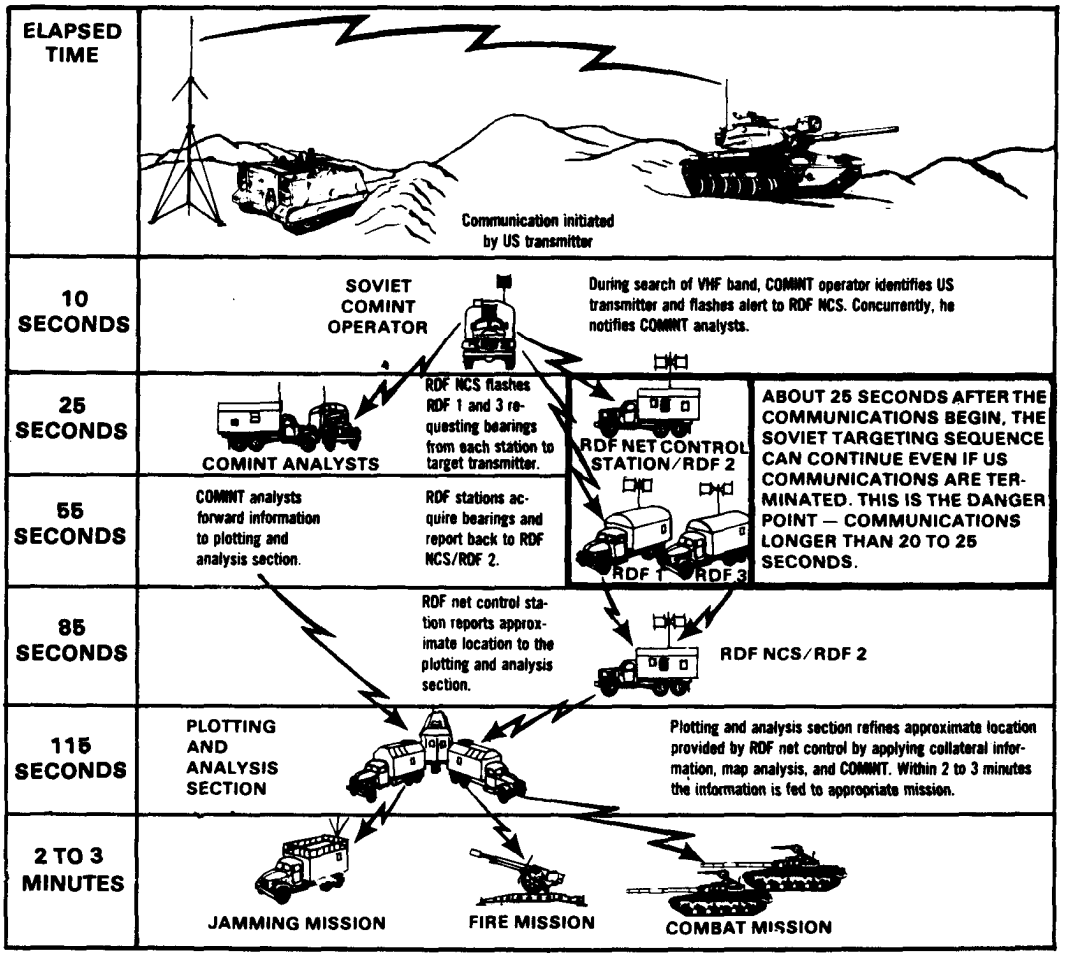

Figure 1-4. Intercept and direction finding.