CHAPTER 11

ELECTRONIC WARFARE

11-1. Introduction

a. Communications have always been the heart of command and control. On today's highly sophisticated battlefield, the Army places even greater dependence on communications and other battlefield electronic systems. Our potential enemies (Threat forces) know this. A large part of Threat resources will be dedicated against our command and control systems. EW will be used by both sides to an extent not known in the past. How vulnerable we are to Threat EW depends very much on the communicator.

b. Tropo Company personnel must be trained to recognize the Threat's EW activities and know what to do about them. This chapter introduces EW and highlights actions taken at the C-E operating level to minimize its effect. Specific tactics that will help plan the defensive against EW are found in FM 32-30 and equipment TMs.

11-2. Components of electronic warfare

a. Three components of EW are described in FM 32-30. They include all types of battlefield electronic systems: communications, surveillance, target acquisition, and others. This manual deals with EW only as it involves communications systems that support TA command and control.

b. Table 11-1 summarizes the three components of EW as they pertain to communications devices. The first two EW components, electronic warfare support measures (ESM) and electronic countermeasures (ECM), are technical. We rely on military intelligence (MI) units and U.S. Army Intelligence and Security Command (USAINSCOM) for advice and implementation of ESM and ECM. The Threat force's equivalent of our ESM and ECM is described as radioelectronic combat (REC). To counter Threat use of REC, we rely on communicators to use electronic counter-countermeasures (ECCM).

11-3. Electronic threat

The Threat forces use REC measures to collect intelligence data against our C-E systems. This is what intercept provides. The Threat then decides what REC would be appropriate from the data gained through intercept. High on the Threat REC target list will be theater level troposcatter communications. The Threat will use selected reconnaissance and REC assets to detect and locate terminals, links, and relays. The Threat will attempt to disrupt those communications which are considered priority targets. Figure 11-1 depicts the Threat's REC cycle. The goal of REC is to disrupt friendly use of the electromagnetic spectrum through destruction, deception, or jamming. The Threat will coordinate all three in an attempt to deprive us of command and control. All Tropo Company personnel must understand the severity of this electronic threat. More specific information on Threat force's electronic intercept and direction-finding capabilities can be found in FM 100-2-1. About 25 seconds after friendly communications begin, the Threat targeting sequence can continue even if friendly communications cease. Accordingly, the danger point is when radio transmissions exceed 20-25 seconds.

a. Interception of signa1s intelligence. It is difficult for Threat forces to fix on a troposcatter terminal. However, the radios used for Tropo Company command and control are highly vulnerable to REC. Through an alert Threat signals intelligence effort, we

TABLE 11-1
COMPONENTS OF ELECTRONIC WARFARE

Component	Objective	Actions
Electronic warfare support measures	Disclose information about enemy communications	Search, intercept, identify, locate
Electronic countermeasures	Deny or reduce use of enemy communications	Jam, deceive
Electronic counter-countermeasures	Ensure continued effective use of friendly communications (protect against enemy detection, location, and identification)	Antijam, circuit discipline, use approved operating techniques, security, harden, move, improve equipment, report, plan, train

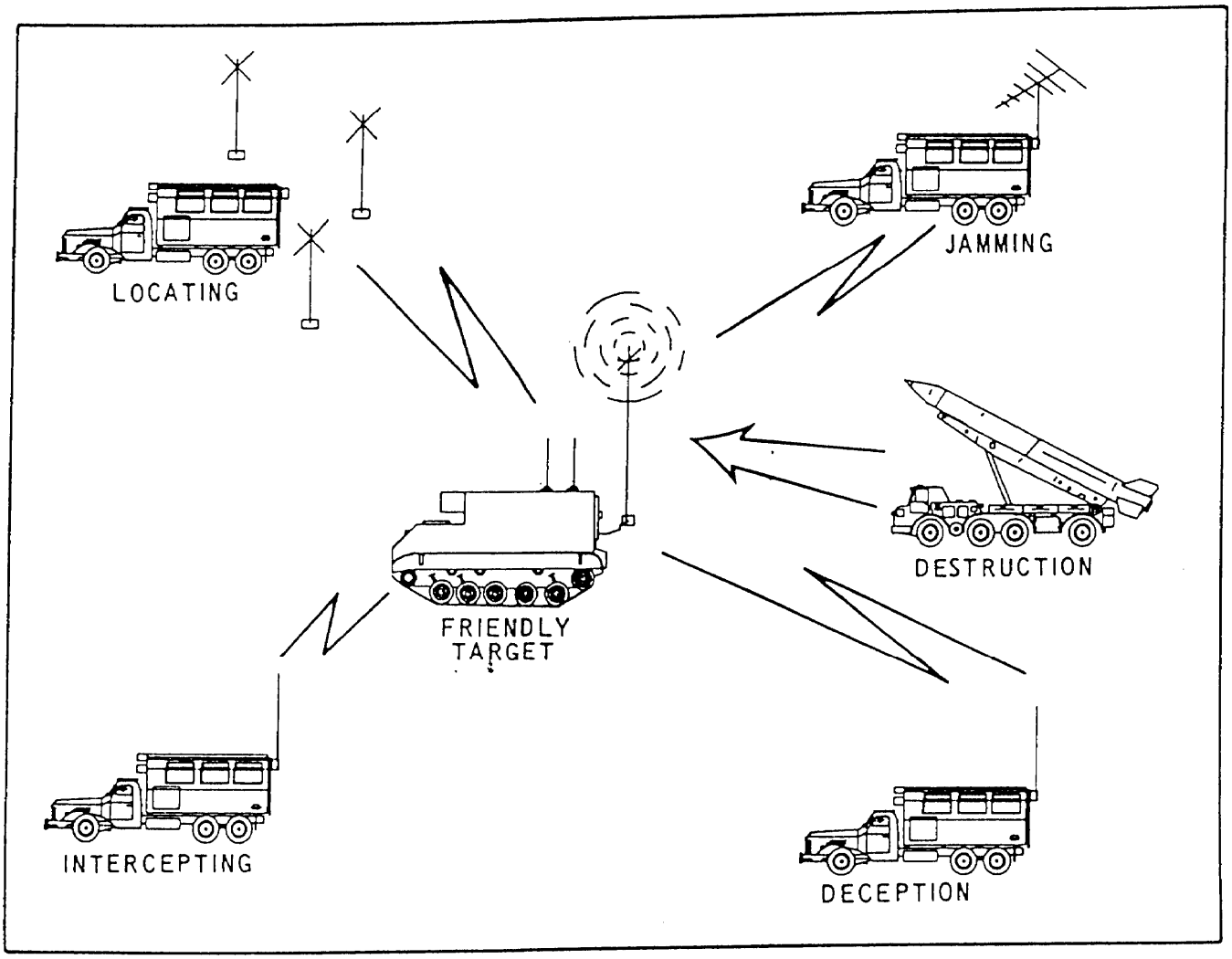

Figure 11–1. Threat radioelectronic combat (REC) cycle.

risk disclosing our troposcatter operations. The Threat monitors intercepted signals and performs traffic analysis to provide a variety of information which can be exploited, such as–

(1) Supported CP identification.

(2) Location of troposcatter terminals.

(3) Tracking of unit movements.

(4) Relative importance of troposcatter to command and control.

(5) Weaknesses in our command and control systems (poor operating procedures, poor COMSEC, lack of redundant or alternate systems, and overloaded networks).

b. Location of emitters. A primary REC threat is the Threat force's ability to locate key communications through radio direction finding (RDF). The Threat's goal is to limit, delay, or nullify our command, control, and intelligence systems during the critical combat periods. RDF is especially effective against CPs which rely heavily on radios with omnidirectional antennas. Through the RDF technique, the troposcatter terminals themselves may be placed in jeopardy. After loeating a friendly communications emitter, the Threat determines if it is a primary target. Once an emitter becomes a primary target, disruption may take the form of destruction, jamming, or deception.

(1) *Jamming.* Threat jammers attempt to disrupt our conduct of the battle by interjecting delay and confusion into the command and control communications system. These jammers operate against receivers–not transmitters. They attempt to transmit with enough power to override friendly signals before they can be received. This jamming may be subtle and difficult to detect, or it may be overt. It can be accomplished from both ground and aerial platforms. However jamming is accomplished, it is often most effective when operators become impatient and relax signal security (SIGSEC) and operations security (OPSEC) procedures, thus providing additional opportunities for deception or destruction operations. Radio operators must be familiar with this form of REC. The more common jamming signals are described in FM 32-30.

(2) *Deception.* REC attempts to deceive friendly emitters through intercepting, locating, and inserting false or misleading information. Threat REC may imitate friendly forces to gain access to our communications nets or provide incorrect or misleading information over Threat communications links. They may also establish "dummy" nets to feed false information to our forces or to simulate nonexistent forces.

11-4. Defensive electronic warfare

Communications can still operate within the REC environment just described. To do this, it is necessary to maximize the efficiency of available equipment and use sound, common-sense countermeasures. Communications discipline, security, and resourcefulness underlie countermeasures to shield emissions. COMSEC techniques give the commander confidence in the security of communications materiel and communications. ECCM techniques provide some degree of confidence in the continued use of communications in a hostile EW environment. The two are closely related–many COMSEC techniques also serve an ECCM role. Thus, the more effective the Tropo Company is in COMSEC, the more effective it is in ECCM.

a. Communications security techniques.

(1) COMSEC is a component of SIGSEC. It protects communications through the use of security measures and techniques such as those shown in Table 11-2.

(a) Physical security safeguards COMSEC materiel and information from access or observation by unauthorized personnel through physical means.

(b) Crypto security protects radio communications through the use of technically sound cryptosystems.

(c) Transmission security is designed to protect transmissions from hostile intercept and exploitation.

(d) Emission security involves studies, investigations, and tests to control compromising and inadvertent emissions from equipment.

(2) Most TCS(A) circuits are protected by COMSEC equipment. However, orderwire and internal Company command and control nets may not be secure. Technical discussions between operators can contain information of vital importance to the Threat forces. The very nature of any communications mission gives them access to critical information on commanders, organizations, and locations of headquarters. This information, although gained casually "on the job," is sensitive and must be protected.

(3) COMSEC must be a function of everyone who uses C-E equipment. It begins with command emphasis. FM 34-62 covers overall SIGSEC and contains detailed information on COMSEC measures and techniques.

b. Electronic counter-countermeasures techniques.

(1) ECCM are taken to protect against Threat attempts to detect, deceive, or destroy friendly communications. The first line of defense against REC is a well-trained and alert operator because, as mentioned earlier, many COMSEC techniques are equally ECCM techniques. To combat Threat REC efforts, operators must use ECCM techniques identified in OPSEC surveys and unit SOPs, or as outlined in table 11-2.

(2) Unit SOPs must include actions to be taken against jamming and deception. Specific techniques are described in troposcatter technical manuals. Prearranged plans and frequent exercises are mandatory. Operators must follow SOPs to maintain or restore communications.

(3) Other ECCM actions that will lessen our vulnerability to a Threat REC effort are–

(a) Preparing backup systems–orderwire, messenger, and HF radio.

(b) Preparing to operate with the minimum amount of communications.

(c) Moving CPs frequently.

(d) Using state of the art equipment and ap-

TABLE 11–2
COMSEC MEASURES AND TECHNIQUES

Physical Security	Crypto Security	Transmission Security	Emission Security
Facility approvals	Machine crypto	Emission control	Site surveys
Facility inspections	Nonmachine crypto	Change of frequencies and call signs	Engineering
Materiel control systems	Electronic crypto	Authentication codes and brevity lists	Inspections Studies
Transportation security		Protective deception Site masking	Tests
Storage security		Power variation Directional antennas	

plying authorized modifications to equipment.

(e) Reporting all known or suspected REC activities.

(f) Planning and training to counter an REC threat.

(g) Dispersing communications equipment over a wide geographical area.

(4) FM 32-30 contains appendixes that cover ECCM checks, ECCM planning, and ECCM training. It also covers EW reporting using the meaconing, intrusion, jamming, and interference (MIJI) report. AR 105-3 requires that all incidents of an electromagnetic nature that affect C-E operations be reported. Unit SOPs and other instructions must include the MIJI program. See glossary for a definition of meaconing.

c. Emission control.

(1) Emission control (EMCON) is both a COMSEC and an ECCM technique, and probably the best method to counter the Threat REC effort. Radio transmissions should be kept to the minimum required to accomplish the mission(s). Transmissions should not exceed 20-25 minutes. The Threat gains less information from a short transmission and has limited capability of locating the transmitter by RDF.

(2) EMCON can also be total or selective. Sometimes, strict radio silence is necessary. The Company commander may also designate certain nets as "free nets" and others as "on order nets." Controls, such as frequent changes in call signs and frequencies and relocation of emitters will tend to confuse Threat forces. Personnel must be taught to "think EMCON."

11-5. Electromagnetic compatibility

a. In an EW environment, we know that Threat forces will intentionally try to interfere with our communications. Self-inflicted unintentional interference is also possible. It may be caused by our own transmitted signals, faulty electronic components, poorly insulated high power lines, noise-producing equipment, and so forth. This type of interference is treated under the term "electromagnetic compatibility" (EMC). EMC is that desirable condition when all of our electronic and electrical equipment, such as radios, radars, generators, and vehicle ignition systems, operate without interfering with each other.

b. Troposcatter site planners and operators must be aware of EMC and its advantages. We do not want to assist the Threat's REC efforts. When planning the layout of the Company CP or a terminal site, EMC must be considered. Operators experiencing interference must make every effort to determine if it is intentional or unintentional. The following are some typical common-sense procedures to promote EMC:

(1) Know the technical operating characteristics of the equipment.

(2) Properly ground, operate, and maintain the equipment.

(3) Site antennas away from noise sources.

(4) Move noise-producing equipment out of transmission paths.

(5) Provide for adequate receiver-transmitter frequency separation.