Chapter 2
Preventive Electronic Counter-Countermeasures Techniques

2-1. Introduction

a. We must use preventive ECCM techniques to safeguard our communications from enemy disruption and destruction. ECCM techniques include all measures taken to avoid enemy detection and to deny enemy intelligence analysts useful information. There are two categories of preventive ECCM techniques:

- ECCM designed circuits (equipment features).
- Radio system installation and operating procedures.

Radio operators have little control over the effectiveness of ECCM designed circuits; therefore, the primary focus of this manual is radio system installation and operating procedures.

b. Reducing the vulnerability of our communications to enemy efforts to disrupt or destroy them is largely a matter of avoiding detection by the enemy. If the enemy cannot detect our communications, he will have difficulty disrupting or destroying them. Effective jamming depends on knowing the frequencies and approximate locations of units to be jammed. We must do all we can to prevent disclosing this information. Using the techniques in this chapter will help accomplish this. Table 2-1 lists preventive ECCM techniques.

2-2. Minimal Transmissions

a. The most effective preventive ECCM technique is to minimize radio transmissions and transmission times. Even though normal day-to-day operations require radio communications, these communications should be kept to the minimum needed to accomplish the mission. Using the following preventive ECCM techniques will minimize transmissions and transmission times.

(1) Ensure all transmissions are necessary. Analysis of US tactical communications indicates that most communications used in training exercises are explanatory and not directive. Radio communications must never be used as a substitute for complete planning. Tactical radio communications should be used to convey orders and critical information rapidly. Execution of the battle must be inherent in training, planning, ingenuity, teamwork, and established and practiced SOPs. The high volume of radio communications that usually precedes a tactical operation makes the friendly force vulnerable to enemy interception, direction finding, jamming, and deception.

> NOTE: Even when communications are secure, the volume of radio transmissions can betray an operation and the enemy can still disrupt or destroy our ability to communicate.

Table 2-1. List of preventive ECCM techniques.

I. Minimize Transmissions.
- Ensure all transmissions are necessary.
- Preplan messages before transmitting them.
- Transmit quickly and precisely.
- Use equipment capable of data burst transmission.
- Use an alternate means of communications when possible.

II. Protect transmissions from enemy interception.
- Use low power.
- Select the proper antenna.
  - Use the antenna with the shortest feasible range.
  - Use directional antennas.
- Select a site that masks transmitted signals from enemy interception.
- Use mobile antennas.
- Use decoy antennas.
- Use steerable null antenna processors.

III. Practice proper radiotelephone operators procedures.
- Reduce operator distinguishing characteristics.
- Operate on a random schedule.
- Authenticate when using nonsecure communications means.
- Encrypt all EEFI category data.
- Use COMSEC equipment when available.
- Use PROWORDs.

(2) Preplan messages before transmitting them. The radio operator should know what he is going to say before beginning a transmission. When the situation and time permit, the message should be written out before beginning the transmission. This will minimize the number of pauses in the transmission and decrease transmission time. It will also help ensure the conciseness of the message. The Joint Interoperability of Tactical Command and Control Systems (JINTACCS) voice templates are some of the best tools a RATELO can use to minimize transmission time.

(3) Transmit quickly and precisely. When a transmission is necessary, the radio operator should--

- Speak in a clear, well-modulated voice.
- Use proper radiotelephone procedures.

This is especially critical when the quality of communications is poor. This minimizes the chances that a radio transmission will have to be repeated. Unnecessary repetition increases transmission time and the enemy's opportunity to intercept our transmissions and thus gain valuable information.

(4) Use equipment capable of data burst transmission. This is one of the most significant advantages of tactical satellite communications systems. When messages are encoded on a digital entry device for transmission over satellite systems, the transmission time is greatly reduced.

(5) Use an alternate means of communications when possible. Alternate means of communications, such as cable, wire, or organic soldiers performing as messengers, can be used to convey necessary directives and information. Radio is a convenient means of communications; however, convenience does not justify making a radio transmission. Other means of communications must be used when practical.

b. We must not operate our radios unnecessarily. Minimizing transmissions will safeguard our radios for critical transmissions. The enemy cannot effectively disrupt or destroy our communications without first gathering information from our radio transmissions. This does not advocate total, continuing radio silence; it advocates minimum transmissions and transmission times. We must never forget that operating our radios unnecessarily increases the enemy's opportunities to gather information.

2-3. Transmission Protection

All radio communications systems consist of antennas, receivers, and transmitters. A transmitted signal can be received by any radio station with which it is compatible. However, the receiving and transmitting radio stations must be set to the same frequency, and the receiving antenna must receive a strong enough signal to activate the receiver. If these criteria are met, any

receiver--friendly or enemy--can intercept a transmitted signal. Therefore, protecting our transmissions must be our goal. We can reduce the possibility of our transmissions being intercepted by properly selecting and properly installing our radio systems. This applies to secure and nonsecure communications. Practicing the following preventive ECCM techniques will reduce the strength of the signals being transmitted toward the enemy.

a. Use low power. Power controls and antennas are closely related. The strength of the signal transmitted by an antenna depends on the strength of the signal delivered to it by the transmitter. The stronger the signal, the farther it travels. A radio communications system must be planned and installed to allow those stations that have a need to communicate with each other to do so. In carefully planned and installed communications systems, we can usually operate on low power. Using low power decreases the range and makes it more difficult for the enemy to detect and intercept our transmissions. It also reserves our high power for burning through enemy jamming.

b. Select the proper antenna. The range of a transmission depends on having a usable frequency and on two equipment-related factors:

- The power output of the transmitter.
- The antenna selected for use with a given radio.

The characteristics and orientation of an antenna affect the strength of the signal transmitted in all directions. An antenna should be selected and installed to ensure that a radio station can communicate with those radio stations with which it needs to communicate. It should also be selected to minimize the strength of the signal transmitted in the direction of the enemy. This can be accomplished by observing the following rules in the selection and the installation of our antennas.

(1) Select the antenna with the shortest feasible range capability. Almost every US Army radio will operate with two or more different kinds of antennas. For example, either the short whip, the long whip, or the OE-254 antenna may be used with the Radio Set AN/PRC-77. The short whip antenna has the shortest range. The OE-254 has the longest range. The antenna used with a given radio should be the one with the shortest range that still permits good communications with all radio stations with which that radio station must communicate. This decreases the chances of enemy interception and reserves longer range antennas for use in overcoming enemy jamming.

(2) Use directional antennas. The three types of antennas are--

- Omnidirectional.
- Bidirectional.
- Unidirectional.

Omnidirectional antennas transmit radio waves in all directions; however, they are more vulnerable to enemy information gathering, jamming, and deception than bidirectional and unidirectional antennas. Bidirectional antennas transmit radio waves in two directions. This enables us to communicate with two or more radio stations in opposite directions. They are good for lateral communications along the FLOT and should, when possible, be positioned so that transmission paths are parallel with enemy lines. Positioning the antenna in this way reduces the possibility of the enemy intercepting our communications. The unidirectional antenna can transmit and receive best in only one direction. When it is positioned properly, this antenna is the least vulnerable to enemy information gathering, jamming, and deception. FM 24-18 explains installation of directional antennas. Tactical satellite communications terminals should be installed to allow the terminal to communicate through the satellite with other terminals in its net.

c. Select a site that masks transmitted signals from enemy interception.

(1) When possible, the antenna should be positioned so that a terrain feature or man-made obstacle is between the antenna and the enemy. The antenna should be positioned as low as possible on the side of terrain features or man-made obstacles away from the enemy. This decreases the range of the transmitted signal and scatters the signal in the direction of the enemy. It makes our transmissions less vulnerable to enemy direction finding and detection. Also, by masking our transmissions from enemy interception, we safeguard our antennas against enemy information gathering, jamming, and deception efforts.

(2) An antenna can be properly positioned even when a station must communicate with a friendly station located between it and the enemy. Using terrain features or man-made obstacles to mask transmissions only reduces the range of the transmitted signal in the direction of the enemy; it does not stop it. The optimum siting for an antenna must be determined on a case-by-case basis.

d. Use mobile antennas. Frequent relocations of our antennas make accurate enemy direction finding more difficult and effective enemy jamming less likely. Antennas in the vehicular or man-pack configurations can be quickly and easily displaced. Even the ground plane antenna can be made mobile by mounting it on a vehicle and securing it by guy wires. This provides a mobile antenna that can be relocated rapidly. If this cannot be done, ensure the antenna is remoted from the communications equipment.

e. Use decoy antennas. When practical, additional antennas can be used as decoys and set up in credible antenna locations. Enemy intelligence analysts place special emphasis on photographs or reconnaissance reports of visible antenna arrays. Decoy antennas may cause the enemy to expend his limited resources against an unworthy target, thus allowing us to maintain worthy communications.

Use steerable null antenna processors. The Steerable Null Antenna Processor (SNAP-1) Group OL-257()/VRC is designed for use with the AN/VRC-12 family of radios and in the nonhopping mode of the Single-Channel Ground and Airborne Radio System (SINCGARS). It provides ECCM protection for the single-channel combat net radios in the VHF range (30-88 MHz). It will operate efficiently when the operator has no prior knowledge of the direction of either the unwanted or desired signal. It has a bypass or override feature that can be used in a jam-free environment or when equipment fails. The SNAP-1 will process the desired signal to its attached receiver even if the sending transmitter is not equipped with the SNAP-1. The SNAP-1 will be doctrinally employed on essential command and control and fire support single-channel radio nets from platoon to division level in forward areas. FM 24-18 contains a more detailed explanation of steerable null antenna processors.

2-4. Radiotelephone Operator Procedures

The RATELO is the key to the success of preventive ECCM techniques. The RATELO ensures that radio transmissions are minimized and protected, thereby preventing the enemy from intercepting and disrupting or destroying our communications. Besides practicing the preventive ECCM techniques, the RATELO must practice procedures that minimize the usable information transmitted. This prevents the enemy from disrupting or destroying our communications based on information detected in the pattern or content of our transmissions. This is accomplished by using the following RATELO procedures:

a. Reduce operator distinguishing characteristics. Many of our RATELOs can be readily identified by certain voice characteristics or overused phrases. The enemy can use these distinguishing characteristics to identify a unit even though frequencies and call signs are changed periodically. Strictly adhering to the proper use of procedure words (PROWORDs) as outlined in FM 24-18 helps us to keep operator distinguishing characteristics to a minimum. However, this is not enough. Accents and overused phrases must also be kept to a minimum. The enemy must not be able to associate a particular RATELO with a particular unit.

b. Operate on a random schedule. As stated before, the enemy can gather information based on the pattern as well as the content of our radio communications. Therefore, we must not develop patterns through hourly radio checks, daily reports at specific times, or any other periodic transmission. Periodic reports should be made by alternate means of communications. We must take all reasonable measures to deny information to enemy intelligence analysts. Operating on a random schedule is one example.

c. Authenticate.

(1) Proper use of authentication prevents the enemy from deceptively entering our nets. It is a procedure that must be used in radio systems that do not use speech secure devices. The enemy has skilled experts whose sole mission is to enter our nets by imitating friendly radio stations. This threat to our radio communications can be minimized by the proper use of authentication.

Procedures for authentication are found in the supplemental instructions to the SOI. Authentication is required in the following situations:

(a) You suspect the enemy is on your net.

(b) You are challenged by someone to authenticate. (Do not break radio listening silence to do this.)

(c) You transmit directions or orders that affect the tactical situation, such as change locations, shift fire, or change frequencies.

(d) You talk about enemy contact, give an early warning report, or issue a follow-up report. (This rule applies even if you used a brevity list or operations code.)

(e) You tell a station to go to radio or listening silence or ask it to break that silence. (Use transmission authentication for this.)

(f) You transmit to a station that is under radio listening silence. (Use transmission authentication for this.)

(g) You cancel a message by radio or visual means, and the other station cannot recognize you.

(h) You resume transmitting after a long period of time, or it is the first transmission.

(i) You are authorized to transmit a classified message in the clear. (Use transmission authentication for this.)

(j) You are forced, because of no response by a called station, to send a message in the blind. (Use transmission authentication for this.)

(2) All instances in which the enemy attempts to deceptively enter our nets to insert false information must be reported. The procedures for reporting these incidents are in Chapter 4. The procedures are also in the supplemental instructions to the SOI.

d. Encrypt all essential elements of friendly information. EEFI are those items of information which we must not allow the enemy to obtain. A broad, general list of these items of information is contained in the supplemental instructions to the SOI. These items of EEFI are applicable to most Army units engaged in training exercises or tactical operations. The list is to support the Army self-monitoring program and is not all inclusive. Individual units should develop a more specific EEFI list to be included in unit operation orders, operation plans, and field SOPs. These items of information must be encrypted manually or electronically before transmission. Electronic encryption is accomplished by using COMSEC devices such as the KY-57/58, KG-84, or KG-93/94. Manual encryption is accomplished by using

approved operations codes. Manual and electronic encryption need not be used together. Either method used alone will protect EEFI from enemy exploitation.

2-5. Equipment and Communications Enhancements

In addition to the equipment enhancements and proper RATELO procedures, other techniques can be used to reduce the vulnerability of friendly communications to hostile exploitations. Some of these ECCM procedures are the introduction of frequency hopping modules in radios, null steering and adaptive antennas, spread spectrum waveforms, automatic adjustable power output, and fiber optics technology.

a. Frequency hopping is particularly useful in lessening the effects of enemy communications jamming and in denying the enemy friendly position location data. This is done by changing the instantaneous frequency of a narrowband transmission in a psuedo-random manner. The new family of SINCGARS will employ frequency hopping.

b. Null steering and adaptive antenna techniques are designed to achieve more survivable communications systems. Null steering masks the radiation pattern to nullify the effects of jamming and provides an improved signal-to-jamming ratio. These techniques are typically coupled with spread spectrum waveforms combining frequency hopping with psuedo-noise coding.

c. Spread spectrum techniques are intended to suppress interference by other users (hostile or friendly), to provide multiple access (user sharing), and to eliminate multipath interference (self-jamming caused by a delayed signal). The transmitted intelligence is deliberately spread across a very wide frequency band in the operating spectrum so that it becomes hard to detect from normal noise levels. The Enhanced Position Location Reporting System (EPLRS) and the Joint Tactical Information Distribution System (JTIDS) use this technique.

d. Adjustable power automatically limits the radiated power to a level sufficient for effective communications, thereby reducing the electronic signature of the subscriber. The radios currently planned for use in the Mobile Subscriber Equipment (MSE), such as the radio access units (RAUs) and the mobile subscriber radiotelephone terminals (MSRTs), use this feature.

e. Frequency hopping multiplexer (FHMUX) and high-power broadband vehicular whip antennas (HPBVWA) are currently being developed. The FHMUX is an antenna multiplexer used with SINCGARS in both stationary and mobile operations. This multiplexer will allow up to five SINCGARS to transmit and receive through one VHF-FM broadband antenna (OE-254 or HPBVWA) while operating in frequency hopping mode, nonhopping mode, or a combination of both. It will also be capable of operating with the current VRC-12 family of radios. Visual and electronic profiles of command posts will be reduced by using one antenna instead of up to five. Also, emplacement and displacement times will be greatly reduced.