Field Manual
No 24-33

*FM 24-33
HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 17 July 1990

Communications Techniques: Electronic Counter-Countermeasures

Contents

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

*This publication supersedes FM 24-33, 22 March 1985.

Preface

Purpose and Scope

This manual concentrates on the defense against enemy efforts to disrupt or destroy our effective use of the electromagnetic spectrum for communications. Following the techniques in this manual will increase our chances for success on the AirLand battlefield.

The communications electronic counter-countermeasures (ECCM) in this manual will assist commanders, staff personnel, and radio operators. This manual will also assist signal officers and electronic warfare (EW) personnel. The techniques in this manual are proven; however, they are not all inclusive. Maintaining effective, friendly communications on the AirLand battlefield will depend on our ability to enhance proven ECCM techniques.

This manual amplifies the EW doctrine in FM 100-5 and FM 24-1. Appendix D gives instructions for implementing ECCM for radio systems.

User Comments

The proponent of this publication is HQ TRADOC. Your comments on this publication are encouraged. Submit changes for improving this publication on DA Form 2028 (Recommended changes to Publications and Blank Forms) and key them to pages and lines of text to which they apply. If DA Form 2028 is not available, a letter is acceptable. Provide reasons for your comments to ensure complete understanding and proper evaluation. Forward your comments to Commander, United States Army Signal Center and Fort Gordon, ATTN: ATZH-DTL, Fort Gordon, Georgia 30905-5075.

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.

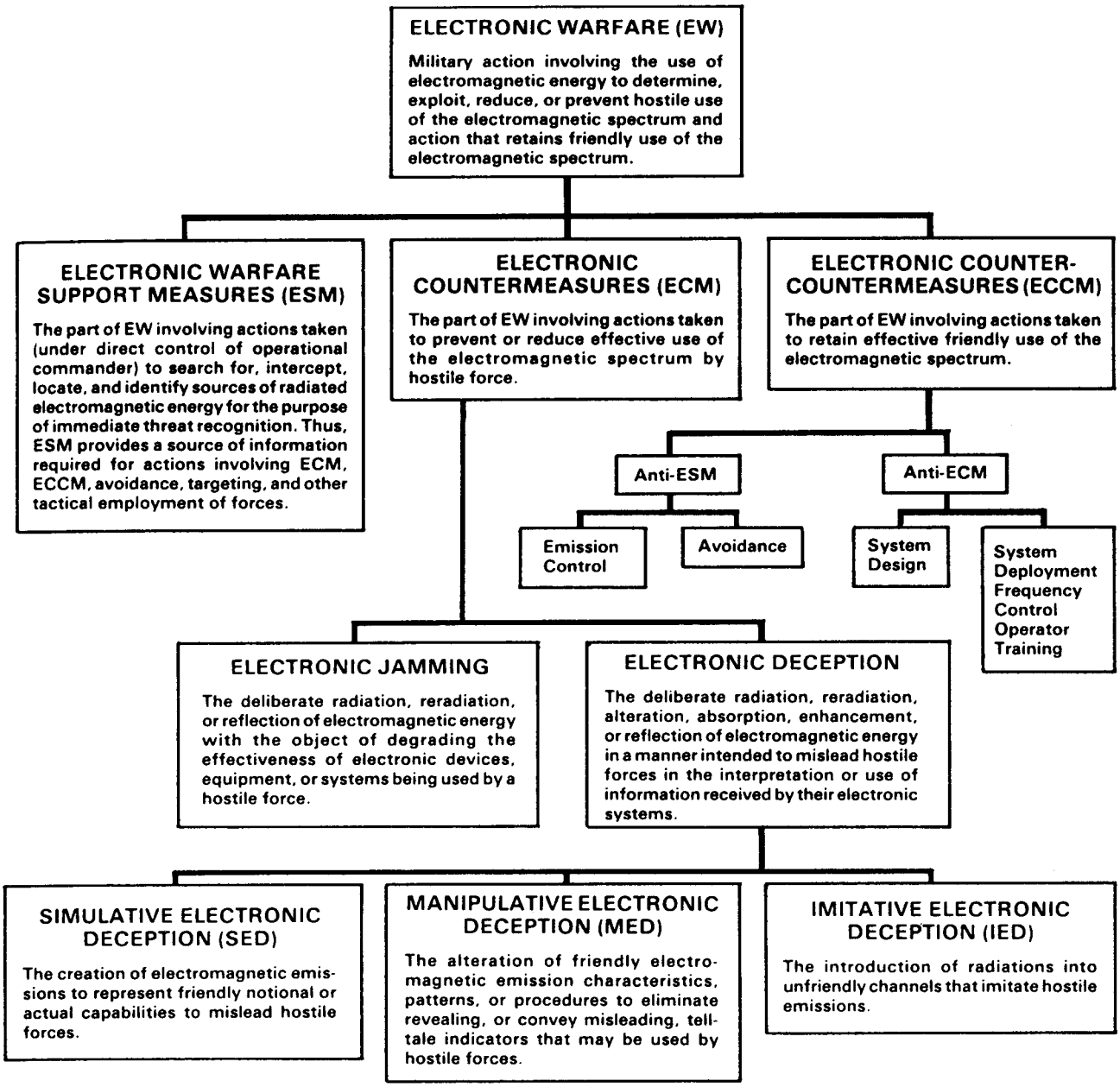


Figure 1-1. Electronic warfare functions.

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.

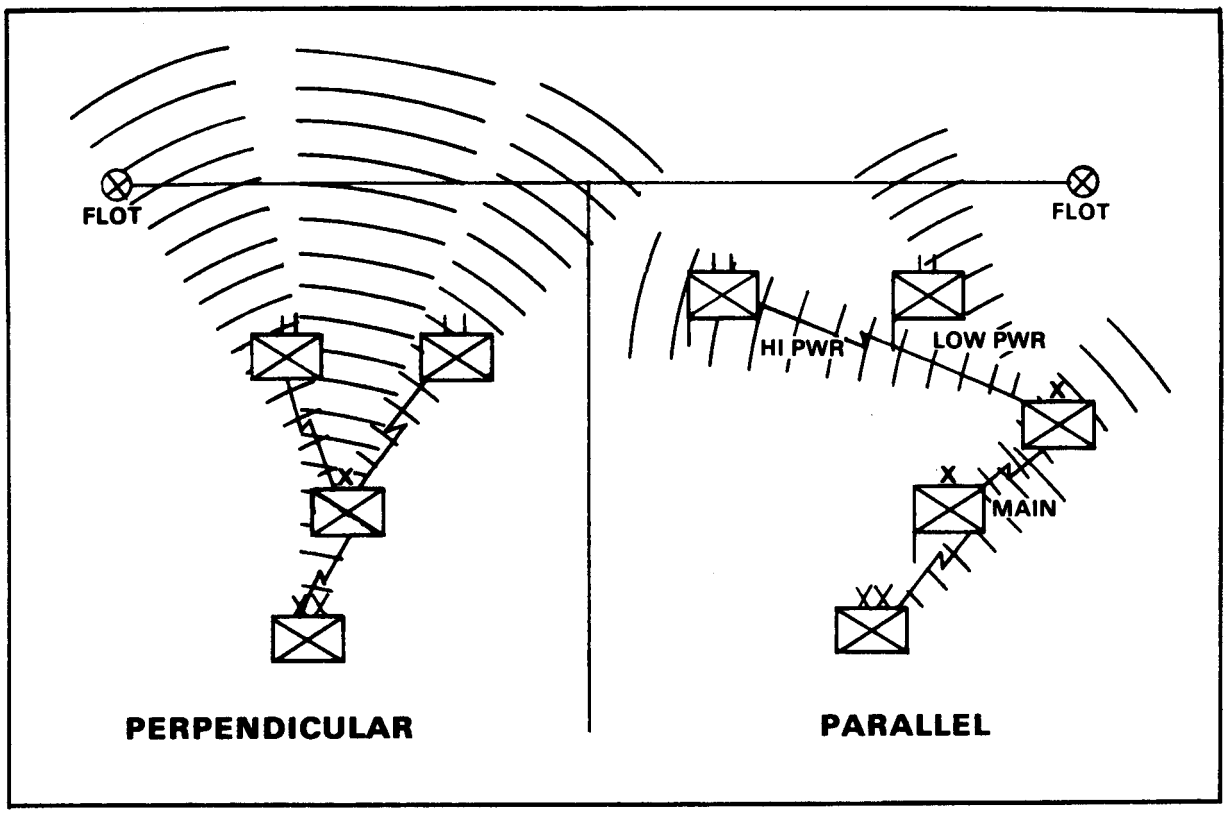


Figure 1-2. Geometry of the battlefield.

(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.

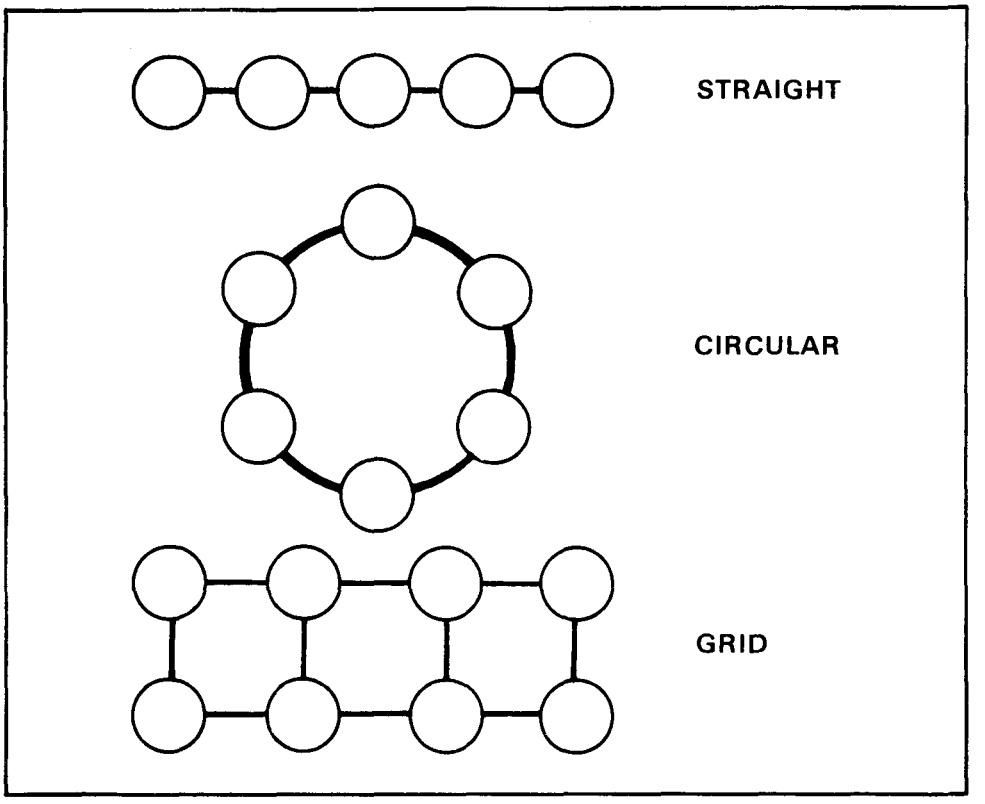


Figure 1-3. Deployment configurations.

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.)

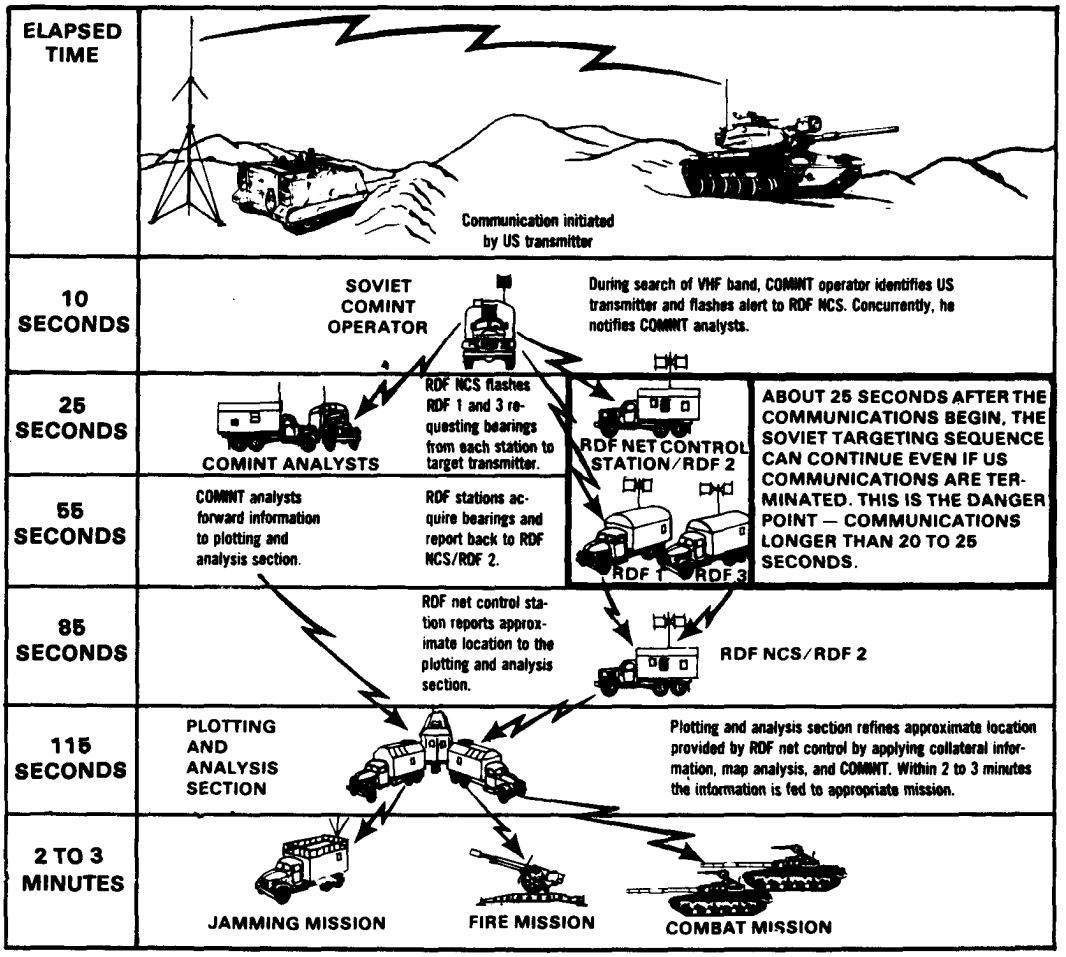


Figure 1-4. Intercept and direction finding.

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.

Chapter 3
Remedial Electronic Counter-Countermeasures Techniques

3-1. Introduction

Remedial ECCM techniques (Table 3-1) reduce the effectiveness of enemy efforts to jam our radio nets. They apply only to enemy jamming efforts or any unidentified or unintentional interference that disrupts our ability to communicate. There are no remedial ECCM techniques that apply to other actions the enemy might use to disrupt or destroy our communications. We must prevent enemy jamming and interference--after the enemy has gathered information about us, we cannot get it back.

Table 3-1. Summary of remedial ECCM techniques.

I. Recognize jamming/interference.
- Determine whether the interference is internal or external to the radio.
- Determine whether the interference is jamming or unintentional.
- Report jamming/interference incidents.

II. Overcome jamming/interference.
- Continue to operate.
- Improve the signal-to-jamming ratio.
- Adjust the receiver.
- Increase the transmitter power output.
- Adjust or change the antenna.
- Establish a retransmission station.
- Relocate the antenna.
- Use an alternate route for communications.
- Change frequencies.
- Acquire another satellite.

3-2. Types of Jamming Signals

Jamming is an effective way for the enemy to disrupt our command, control, and communications on the battlefield. All the enemy needs to jam us is a transmitter tuned to our frequency with enough power to override friendly signals at our receivers. Jammers operate against receivers--not transmitters. There are two modes of jamming: spot and barrage. Spot jamming is concentrated power directed toward one channel or frequency. Barrage jamming is power spread over several frequencies or channels at the same time. Jamming can be difficult, if not impossible to detect. For this reason, we must always be aware of the possibility of jamming and be able to recognize it. The two types of jamming most commonly encountered are obvious and subtle jamming.

a. Obvious jamming. This is normally very simple to detect. The more commonly used jamming signals of this type are described below. Do not try to memorize them; just be aware that these and others exist. When experiencing a jamming incident, it is more important to recognize and overcome the incident than to identify it formally.

(1) Random noise. This is synthetic radio noise. It is random in amplitude and frequency. It is similar to normal background noise and can be used to degrade all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate ECCM actions.

(2) Stepped tones. These are tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are normally used against single-channel AM or FM voice circuits.

(3) Spark. The spark signal is easily produced and is one of the most effective for jamming. Bursts are of short duration and high intensity. They are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications.

(4) Gulls. The gull signal is generated by a quick rise and slow fall of a variable radio frequency and is similar to the cry of a sea gull. It produces a nuisance effect and is very effective against voice radio communications.

(5) Random pulse. In this type of interference, pulses of varying amplitude, duration, and rate are generated and transmitted. They are used to disrupt teletypewriter, radar, and all types of data transmission systems.

(6) Wobbler. The wobbler signal is a single frequency which is modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.

(7) Recorded sounds. Any audible sound, especially of a variable nature, can be used to distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.

(8) Preamble jamming. This type of jamming occurs when a tone resembling the synchronization preamble of the speech security equipment is broadcast over the operating frequency of secure radio sets. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio nets using speech security devices.

b. Subtle jamming. Subtle jamming is not obvious; no sound is heard from our receivers. They cannot receive an incoming friendly signal, even though everything appears normal to the radio operator. Subtle jamming takes advantage of design features of the AN/PRC-77 and AN/VRC-12 series radios. In order to activate the receiver of an AN/PRC-77 in the SQUELCH mode or an AN/VRC-12 series radio in the NEW SQUELCH ON mode, a 150-hertz tone must be transmitted to them along with the carrier signal. In addition to this squelch feature, the AN/PRC-77 and AN/VRC-12 series radio receivers lock onto the strongest carrier signal received and eliminate the reception. of all other signals. For example, if we have an AN/PRC-77 in the SQUELCH mode and an AN/VRC-12 series radio in the NEW SQUELCH ON mode and they receive a jamming signal without the 150-hertz tone, the receivers of these radios will not be activated by any signal as long as the jamming signal is stronger than any other signal being received. In effect, the threat jammers block out these radios' ability to receive a friendly transmission without the operator being aware it is happening. This is called squelch capture and is a subtle jamming technique. The radio operator can readily detect jamming in all other function control modes and the other modes must be checked. Often, we assume that our radios are malfunctioning instead of recognizing subtle jamming for what it is.

3-3. Recognizing Jamming

a. Radio operators must be able to recognize jamming. Again, this is not always an easy task. Threat jammers may employ obvious or subtle jamming techniques. Also, interference may be caused by sources having nothing to do with enemy jamming. Interference may be caused by the following:

- Unintentionally by other radios (friendly and enemy).
- Other electronic or electric/electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.

(1) Internal or external interference. The two sources of interference are internal and external. If the interference or suspected jamming can be eliminated or substantially reduced by grounding the radio equipment or disconnecting the receiver antenna, the source of the disturbance is most likely external to the radio. If the interference or suspected jamming remains after grounding or disconnecting the antenna, the disturbance is most likely

internal and is caused by a malfunction of the radio. Maintenance personnel should be contacted to repair it. External interference must be checked further for enemy jamming or unintentional interference.

(2) Jamming or unintentional interference. Unintentional interference may be caused by other radios, some other type of electronic or electric/electromechanical equipment, or atmospheric conditions. The battlefield is so crowded with radios and other electronic equipment that some unintentional interference is virtually unavoidable. Also, the static electricity produced by atmospheric conditions can negatively affect radio communications. Unintentional interference normally travels only a short distance, and a search of the immediate area may reveal the source of this type of interference. Moving the receiving antenna for short distances may cause noticeable variations in the strength of the interfering signal. These variations normally indicate unintentional interference. Conversely, little or no variation normally indicates enemy jamming. Regardless of the source, actions must be taken to reduce the effect of interference on our communications.

b. In all cases, suspected enemy jamming and any unidentified or unintentional interference that disrupts our ability to communicate must be reported. This applies even if the radio operator is able to overcome the effects of the jamming or interference. The format for reporting this information is the MIJI report. Instructions for submitting a MIJI report are in Chapter 4 and are usually listed in the SOI. As it applies to remedial ECCM techniques, the information provided to higher headquarters in the MIJI report can be used to destroy the enemy jamming efforts or take other action to our benefit.

c. The enemy can use two types of jamming signals: powerful unmodulated or noise-modulated signals. Unmodulated jamming signals are characterized by a lack of noise. Noise-modulated jamming signals are characterized by obvious interference noises. The following procedures will help radio operators determine whether their radios are being threatened by enemy jamming.

(1) AN/PRC-77.

(a) Turn the function control from the SQUELCH OFF to the ON position.

(b) Lack of noise may indicate that the radio is being jammed by an unmodulated jamming signal. The operator should temporarily disconnect the antenna. If normal static noise returns when the antenna is disconnected, there is a high probability that the radio is being jammed by an unmodulated signal.

(c) A greater than normal level of noise or an obviously modulated signal may indicate that the radio is being jammed by a noise-modulated jamming signal. The operator should temporarily disconnect the antenna. If normal static noise returns when the antenna is disconnected, the radio most likely is being jammed by a noise-modulated signal.

(d) If the above tests indicate there is a high probability the radio is being jammed, the operator should follow the local SOP to reestablish communications and initiate a MIJI report informing higher headquarters of the incident.

(2) AN/VRC-12 series radio.

(a) Turn the squelch control from the NEW SQUELCH ON to the NEW SQUELCH OFF mode.

(b) Lack of noise and an unlighted call light may indicate that the radio is being jammed by an unmodulated jamming signal. The operator should temporarily disconnect the antenna. If normal static noise returns and the call light goes off when the antenna is disconnected, the radio is most likely being jammed by an unmodulated signal.

(c) A greater than normal level of noise or an obviously modulated signal may indicate that the radio is being jammed by a noise-modulated jamming signal. The operator should temporarily disconnect the antenna. If normal static noise returns, and the call light goes off when the antenna is disconnected, there is a high probability that the radio is being jammed by a noise-modulated signal.

(d) If the above tests indicate that there is a high probability that the radio is being jammed, the operator should follow the local SOP to reestablish communications and initiate a MIJI report informing higher headquarters of the incident.

(3) Other unique organizational radios. Signal officers should coordinate with organic military intelligence units for assistance in developing appropriate tests for special capacity radios or radios that are unique to that specific organization. Examples of these are nonstandard issue, off-the-shelf commercial, intermediate high frequency radios (IHFR), or SINCGARS radios. Signal officers should ensure that their unit radio operators are trained to use these radios.

3-4. Overcoming Jamming

The enemy constantly strives to perfect and use new and more confusing forms of jamming. Our radio operators must be increasingly alert to the possibility of jamming. Training and experience are the most important tools operators have to determine when a particular signal is a jamming signal. Exposure to the effects of jamming in training or actual situations is invaluable. The ability to recognize jamming is important, because jamming is a problem that requires action. Once it is determined that jamming is being used against our radios, the following actions must be taken. If any of the actions taken alleviate the jamming problem, we simply continue normal operations and make a MIJI report to higher headquarters.

a. Continue to operate. Stop for a moment and consider what the enemy is doing during his typical jamming operation. Usually, enemy jamming involves

a period of jamming followed by a brief listening period. He is attempting to determine how effective his jamming has been. What we are doing during this short period of time when he is listening will tell him how effective his jamming has been. If the operation is continuing in a normal manner, as it was before the jamming began, the enemy will assume that his jamming has not been particularly effective. On the other hand, if he finds us excitedly discussing our problem on the air or if we have shut down our operation entirely, the enemy may very well assume that his jamming has been effective. Because the enemy jammer is monitoring our operation this way, we have a simple yet very important rule that applies when we are experiencing jamming. Unless otherwise ordered, never shut down operations or in any other way disclose to the enemy that you are being adversely affected. This means normal operations should continue even when degraded by jamming.

b. Improve the signal-to-jamming ratio. The signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. Signal refers to the signal we are trying to receive. Jamming refers to the hostile or unidentified interference being received. It is always best to have a signal-to-jamming ratio in which the desired signal is stronger than the jamming signal. In this situation, the desired signal cannot be significantly degraded by the jamming signal. The following will improve the signal-to-jamming ratio to our benefit.

(1) Adjust the receiver. When jamming is experienced, we should always check to ensure the receiver is tuned as precisely as possible to the desired incoming signal. A slight readjustment of the receiver may provide an improved signal-to-jamming ratio. Specific methods that apply to a particular radio set are explained in the appropriate operator's manual. Depending on the radio being used, some of these methods are--

- Adjust the beat frequency oscillator (BFO).
- Adjust the bandwidth.
- Adjust the gain or volume control.
- Fine tune the frequency.

(2) Increase the transmitter power output. The most obvious way to improve the signal-to-jamming ratio is to increase the power output of the transmitter emitting the desired signal. In order to increase the power output at the time of jamming, the transmitter must be set on something less than full power when jamming begins. We must remember that using low power as a preventive ECCM technique depends on the enemy not being able to detect our radio transmissions. Once the enemy begins jamming our radios, the threat of being detected becomes academic. We should use the reserve power on our terrestrial line-of-sight radios to override the enemy's jamming signal. Tactical satellite communications terminals will not increase their transmit power.

(3) Adjust or change the antenna. Antenna adjustments can appreciably improve the signal-to-jamming ratio. When jamming is experienced, the radio operator should ensure the antenna is optimally adjusted to receive the desired incoming signal. Specific methods that apply to a particular radio set are in the appropriate operator's manual. Depending on the antenna being used, some of these methods are--

- Reorient the antenna.
- Change the antenna polarization. (Must be done by all stations.)
- Install an antenna with a longer range.

(4) Establish a retransmission station. A retransmission station can increase the range and power of a signal between two or more radio stations. Depending on the available resources and the situation, this may be a viable method to improve the signal-to-jamming ratio.

(5) Relocate the antenna. Frequently, the signal-to-jamming ratio may be improved by relocating the antenna and associated radio set affected by the jamming or unidentified interference. This may mean moving a few meters or several hundred meters. It is best to relocate the antenna and associated radio set so that there is a terrain feature between them and any suspected enemy jamming location.

c. Use an alternate route for communications. In some instances, enemy jamming will prevent us from communicating with a radio station with which we must communicate. If radio communications have been degraded between two radio stations that must communicate, there may be another radio station or route of communications that can communicate with both of the radio stations. That radio station or route should be used as a relay between the two other radio stations.

d. Change frequencies. If a communications net cannot overcome enemy jamming using the above measures, the commander (or designated representative) may direct the net to be switched to an alternate or spare frequency. If practical, dummy stations can continue to operate on the frequency being jammed to mask the change to an alternate frequency. This action must be preplanned and well coordinated. During enemy jamming, it is very difficult to coordinate a change of frequency. All radio operators should know when and under what circumstances they are to switch to an alternate or spare frequency. If this is not done smoothly, the enemy may discover what is happening and try to degrade our communications on the new frequency.

e. Acquire another satellite. In many cases, a satellite communications terminal can see more than one satellite in a given theater. If one satellite is being jammed, then the operator should request permission to access another satellite until the jamming ceases or until the enemy jammer is neutralized.

Chapter 4

Meaconing, Intrusion, Jamming, and Interference Reporting

4-1. Introduction

a. Meaconing, intrusion, and jamming are deliberate actions intended to deny an enemy the effective use of the electromagnetic spectrum. Interference is the unintentional disruption of the effective use of the electromagnetic spectrum by friendly, enemy, or atmospheric sources. Collectively, meaconing, intrusion, jamming, and interference incidents are referred to as MIJI incidents.

b. MIJI reports document all disruptions of--

- Radios.
- Radars.
- Navigational aids (NAVAIDS).
- Satellites.
- Electro-optics.

Disruptions caused by equipment malfunctions or destruction are exceptions. The MIJI report serves two purposes. First, it provides information to the tactical commander allowing timely decisions to be made to overcome the MIJI problem. Second, it provides a historical record of MIJI incidents from which appropriate ECCM techniques and measures can be developed. This helps us to counter future attempts by the enemy to deny us the effective use of the electromagnetic spectrum.

c. This chapter gives instructions for completing MIJI reports for communications and noncommunications emitters. To fulfill the two purposes stated above, there are two kinds of MIJI reports. The MIJIFEEDER voice template message is a brief report of a MIJI incident. It serves as a decision-making tool for the command. The MIJIFEEDER record message is a complete report of a MIJI incident. This provides a historical record from which appropriate ECCM techniques and measures can be developed. DA Pam 25-7 gives instructions for completing the MIJI reports.

4-2. Terms

a. Meaconing. Meaconing is a system of receiving radio beacon signals from NAVAIDs and rebroadcasting them on the same frequency to confuse navigation. The enemy conducts meaconing operations against us to prevent our aircraft and ships from arriving at their intended targets or destinations. Successful enemy meaconing causes--

- Aircraft to be lured into hot landing zones or enemy airspace.
- Ships to be diverted from their intended routes.
- Bombers to expend ordnance on false targets.
- Ground stations to receive inaccurate bearings or position locations.

b. Intrusion. Intrusion is intentionally inserting electromagnetic energy into transmission paths in any manner. The object is to deceive equipment operators or cause confusion. The enemy conducts intrusion operations against us by inserting false information into our receiver paths. This false information may consist of voice instructions, ghost targets, coordinates for fire missions, or even rebroadcasting of prerecorded data transmissions.

c. Jamming. Jamming is deliberately radiating, reradiating, or reflecting electromagnetic energy to impair the use of electronic devices, equipment, or systems. The enemy conducts jamming operations against us to prevent us from effectively employing our radios, radars, NAVAIDs, satellites, and electro-optics.

d. Interference. Interference is any electrical disturbance that causes undesirable responses in electronic equipment. As a MIJI term, interference refers to the unintentional disruption of the use of radios, radars, NAVAIDs, satellites , and electro-optics. This interference may be of friendly, enemy, or atmospheric origin. For example, a civilian radio broadcast may interfere with military communications.

4-3. MIJIFEEDER Voice Template

a. Purpose and use. The MIJIFEEDER voice template has only the information needed to adequately inform the tactical commander of the incident in a timely manner. It is used to make evaluation of enemy actions or intentions easier and to provide data to implement appropriate counter-countermeasures.

b. Reporting procedure.

(1) The MIJIFEEDER voice template is forwarded through the chain of command to the unit operations center by the equipment operator experiencing the MIJI incident. The report should be forwarded using the most expeditious secure communications means available.

(2) Upon receiving the MIJIFEEDER voice template, the signal officer--

(a) Coordinates the unit response to the MIJI incident with the unit operations officer, intelligence officer, fire support officer, and unit commander(s), as applicable and appropriate.

(b) Consolidates the voice templates referring to the same MIJI incident.

(c) Forwards one MIJIFEEDER voice template report for each MIJI incident through operations channels to the corps operations center or as appropriate. This report should be accompanied by any requests for support the command needs to overcome the MIJI problem.

(d) Initiates staff action to complete the MIJIFEEDER record message as quickly as possible. (Coordination will not delay reporting the incident within 24 hours.)

(3) Upon receiving the MIJIFEEDER voice template, in the process of forwarding it through operations channels, the signal officer at each operations center takes the following actions:

(a) Provides support as requested by the unit submitting the voice template report, if possible and deemed appropriate by the command.

(b) Informs the operations officer and intelligence officer of the details of the MIJI incident.

c. Report format and contents. The MIJIFEEDER voice template has been developed for use under the JINTACCS program. It is designed to ensure interoperability on the battlefield during combined, joint, and intra-Army operations. The standardized, simple format permits the expeditious notification of appropriate action elements in time-critical situations. Only the completed and underlined areas (as appropriate) of the format are transmitted. As shown in Figure 4-1, MIJIFEEDER voice templates are self-explanatory and contain ten items of information. When the message is transmitted over nonsecure means, each line number is stated and the completed information must be encrypted. When a secure means is used, the title of each line is transmitted along with the completed information. The operator of the affected system fills out the MIJIFEEDER voice template as shown below.

- Line 1 - Enter the unit designation.
- Line 2 - Enter the type of interference encountered:
  - Meaconing
  - Jamming
  - Intrusion
  - Interference
  - Chaff

- Line 3 - Enter the unit location in either of two ways: Longitude and latitude in minutes and seconds, or in complete grid coordinates down to 10 or 100 meter increments.

- Line 4 - Enter 2 digits each for day, hour, minute, and 1 letter for the time zone for the start of the MIJI incident.

Line 5 - Enter 2 digits each for day, hour, minute, and 1 letter for the time zone for the end of the MIJI incident.

- Line 6 - Enter the nomenclature for the equipment affected.

- Line 7 - Enter the channel, frequency, or frequency range affected and the unit of measure. *Examples:* 3456.2 kHz, 42.35 MHz, or 2.5 to 2.7 GHz.

- Line 8 - Enter, in your own words, a brief description or other information regarding the MIJI incident.

- Line 9 - When required, enter the hour, minute, and time zone.

- Line 10 - Enter the message authentication in accordance with the joint task force (JTF) requirements.

Figure 4-2 is an example of a completed voice template. The circled numbers to the right of each line in Figure 4-2 correspond to extracts of the MIJIFEEDER record message format in Annex 81, DA Pam 25-7.

MIJIFEEDER VOICE TEMPLATE Pg 1 of 1

THIS IS _____ MIJIFEEDER _____ OVER
addressee originator

addressee answers then originator responds: THIS IS _____
addressee originator

FLASH IMMEDIATE PRIORITY ROUTINE (Underline and transmit the precedence of this message.)

TOP SECRET SECRET CONFIDENTIAL UNCLASSIFIED (Underline and transmit the security classification of this message.)

MIJIFEEDER

LINE 1 (or) UNIT _____ (Unit Identification)

LINE 2 (or) TYPE _____ (Type of Interference)

LINE 3 (or) LOCATION _____ (Location - LAT/LONG or UTM)

LINE 4 (or) ONTIME _____ (Start Day-Time-Zone)

LINE 5 (or) OFFTIME _____ (End Day-Time-Zone)

LINE 6 (or) EFFECTS _____ (Operations/Equipment Affected)

LINE 7 (or) FREQUENCY _____ (Frequency/Frequency Range)

LINE 8 (or) NARRATIVE _____

_____

_____

LINE 9 (or) TIME _____ (Message Hour-Minute-Zone when required)

LINE 10 (or) AUTHENTICATION IS _____ (Message Authentication IAW JTF Procedures)

OVER

Figure 4-1. MIJIFEEDER voice template.

MIJIFEEDER VOICE TEMPLATE Pg 1 of 1

3H28 THIS IS 7M21 MIJIFEEDER OVER
addressee originator

addressee answers then originator responds: THIS IS 7M21 (addressee / originator)

FLASH IMMEDIATE PRIORITY ROUTINE (Underline and transmit the precedence of this message.)

TOP SECRET SECRET CONFIDENTIAL UNCLASSIFIED (Underline and transmit the security classification of this message.)

MIJIFEEDER

LINE 1 (or) UNIT 56TH INF. DIV. (Unit Identification) 5

LINE 2 (or) TYPE INTRUSION (Type of Interference) 8

LINE 3 (or) LOCATION 32TMV123123 (Location - LAT/LONG or UTM) 6

LINE 4 (or) ONTIME 252330Z (Start Day-Time-Zone) 9

LINE 5 (or) OFFTIME 260230Z (End Day-Time-Zone) 10

LINE 6 (or) EFFECTS SEARCH RADAR (Operations/Equipment Affected) 13

LINE 7 (or) FREQUENCY 42.35 MHZ (Frequency/Frequency Range) 19

LINE 8 (or) NARRATIVE RADAR PICTURE TO NORTHEAST ERRATIC. 37

LINE 9 (or) TIME 0235Z (Message Hour-Minute-Zone when required)

LINE 10 (or) AUTHENTICATION IS JU (Message Authentication IAW JTF Procedures)

OVER

Figure 4-2. Completed MIJIFEEDER voice template.

4-4. MIJIFEEDER Record Message Report

a. Purpose and use. The MIJIFEEDER record message is a complete report of a MIJI incident. It provides a basis for developing appropriate counteraction measures to be implemented at proper command levels. AR 105-3 and DA Pam 25-7 establish the information to be included in this report. The Joint Electronic Warfare Center (JEWC) is the action agency for this report. All MIJIFEEDER record message reports initially evaluated as nonexercise should be forwarded as soon as possible to the JEWC. The JEWC uses these reports to develop trends and to evaluate foreign ECM operations. They are also used by the JEWC to recommend operational methods and equipment changes that will reduce MIJI vulnerability of our:

- Radios.
- Radars.
- NAVAIDs.
- Satellites.
- Electro-optics.

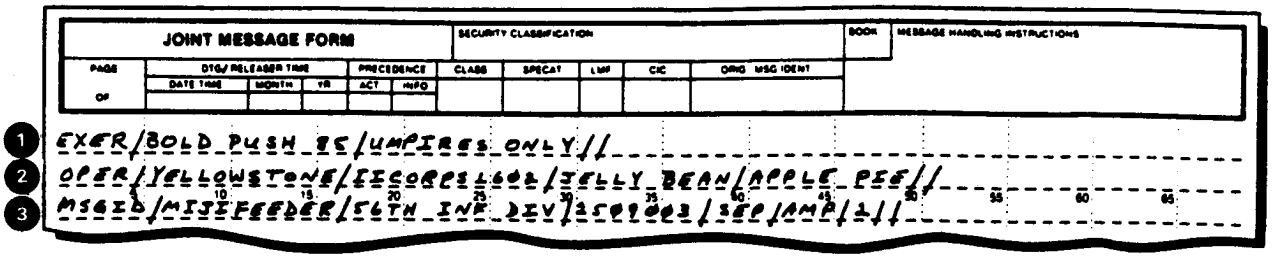
b. Reporting procedures.

(1) The MIJIFEEDER record message is forwarded by the signal officer of the affected unit to the JEWC SAN ANTONIO TX//OPM//through operations channels to the corps operations center. All MIJIFEEDER reports are forwarded via secure means within 24 hours of the MIJI incident.

(2) Items such as photographs, diagrams, and tape recordings, that cannot be included in the message are forwarded by other means (for example, US mail) to the JEWC/OPM, San Antonio, TX 78243-5000, as soon as possible.

(3) Each operations center receiving this report should check the contents for information that may be of use to the entire command.

c. Report format and contents. Excerpts from a joint message form and DA Pam 25-7 at Figure 4-3 illustrate the proper MIJIFEEDER record message format. The circled numbers on the joint message form correspond with the explanation in Annex 81, DA Pam 25-7. Entry lists 11, 97, and 98, referenced in the explanation column, are Appendices A, B, and C of this manual.

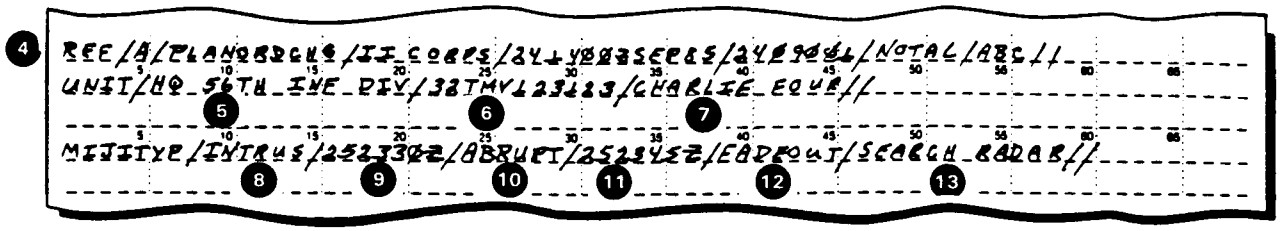


EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
				NOTE: The initial sets (EXER, OPER, MSGID, REF) are described briefly below. See Annex 1 for complete details.
				NOTE: Do not use both EXER and OPER in the same message. If there is no exercise or operation do not use either
1	EXER	c		
	exer name	m	1-56ANBS	Enter the exercise name.
	add id	o	1-16AB	Enter the additional exercise identifier.
2	OPER	c		
	oper name	m	1-32ANBS	Enter the operation name.
	plan orig & number	o	3-23ANS	Enter the headquarters originating the plan and the plan number.
	option name	o	1-23ANBS	Use these two fields to enter code names for options within the operations plan.
	2d option	o	1-23ANBS	
3	MSGID	m		
	title	m	10A	Enter MIJIFEEDER
	originator	m	1-20ANBS	Enter unit name of message originator.
	serial nr	o	1-7ANBS	Enter message serial number.
	month	o	3A	Enter first 3 letters of the month.
	qualifier	o	3A	Enter qualifier code.
	qlf serial	o	1-3N	Enter qualifier serial number.

Figure 4-3. Sample MIJIFEEDER record message format.

EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
4	REF	o r		Use this set to reference other messages.
	serial letter	m	1A	Enter letter A for the first message you reference, B for the second etc.
	msg title or ref type	m	1-20ANBS	Enter the JINTACCS message short title OR one of the following codes for other types of references: CON DOC LTR RMG TEL VMG. (Add a free text set to explain.)
	originator	m	1-20ANBS	Enter unit name of reference originator.
	dtg	m	6-12AN	Enter date-time group of reference.
	serial nr	o	1-7ANBS	Enter serial number of the reference.
	special not	o	5A	Enter PASEP or NOTAL.
	nasis code	o r	3A	FOR NATO USE ONLY. Enter the NASIS code for message subject matter.
	AMPN NARR	c c		You must use a free text set to explain the reference if it is not a JINTACCS message.
				NOTE: Remember you can add free text sets throughout the message. See chapter 2, section VI for free text instructions
	UNIT	m		Use this set to report the MIJI victim.
5	unit name	m		Enter the unit name in one of the following ways:
			6-21ANS	Enter the following:
			1-4AN	• Enter unit number or UNK.
			1S	• Then enter a hyphen (-).
			2-8A	• Then enter orgnization type. ENTRY LIST 97
			1S	• Then enter a hyphen (-).
			1-7A	• Then enter echelon. ENTRY LIST 98
				OR
			1-24ANBS	Enter the unit designation.
6	location	m		Enter the friendly unit location at the time of the event in one of the following ways:

Figure 4-3. Sample MIJIFEEDER record message format (continued).

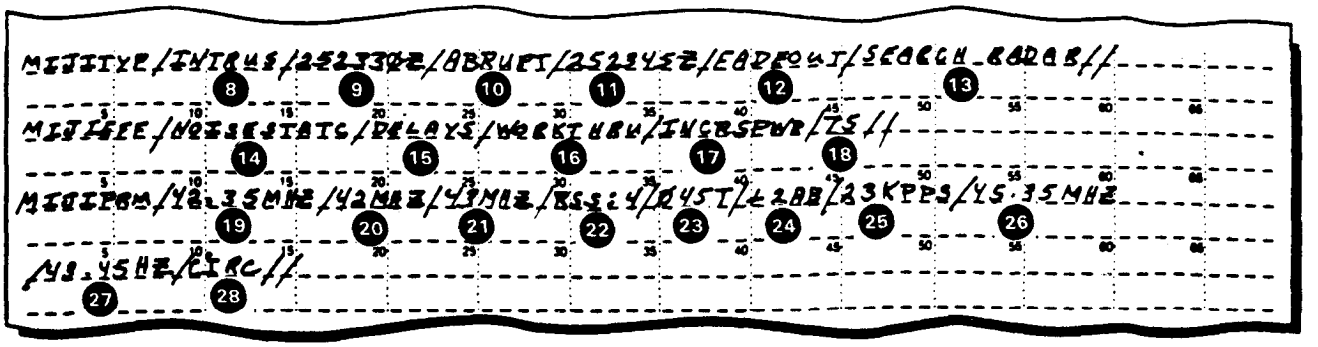


EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
			11-15AN 11-13AN	Lat/Long (min. or sec.) ENTRY LIST 11 UTM (10 m or 100 m) ENTRY LIST 11
7	call sign	o	1-17ANBS	Enter the victim's call sign.
				NOTE: Sets MIJITYPE, MIJIEFF, MIJIPRM, MIJISAT and NARR are a repeatable segment. Repeat them as a group to report multiple MIJI types. You must repeat the sets in their original order. You must include the mandatory sets in each repetition.
	MIJITYP	m		Use this set to report MIJI type, place and time of event, and operator position/ equipment affected.
8	ecm type	m	3-8A	Enter the code for MIJI type: TYPE / CODE / TYPE / CODE Interference / INTERFER / Meaconing / MEACON Intrusion / INTRUS / Chaff / CHAFF Jamming / JAMMING / Other / OTR Explain OTR in a free-text set.
9	time on	m	7AN	Enter 2 digits each for day, hour, minute, 1 letter for time zone for the start of the MIJI event.
10	miji began	m	5-6A	Enter the code describing how the MIJI incident began: TYPE / CODE Abrupt / ABRUPT Fade-In / FADEIN Other / OTHER Explain OTHER in a free text set.
11	time off	m	7AN	Enter the time as in the time on field for the end of the MIJI event.

Figure 4-3. Sample MIJIFEEDER record message format (continued).

EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
12	miji ended	m	5-7A	Enter the code describing how the MIJI incident ended: TYPE — CODE Abrupt — ABRUPT Fade-Out — FADEOUT Other — OTHER Explain OTHER in a free text set.
13	pos, equip	m r	1-20ANBS	**Enter the name(s) of the operator position(s) and/or nomenclature of equipment affected.**
	MIJIEFF	m		Use this set to describe the MIJI effects.
14	interference	m	3-10A	Enter the code for interference type: TYPE — CODE — TYPE — CODE Analog — ANALOG — Continuous wave (CW)/ random — CWRANDOM Analog chatter — ANALCHAT Analog music — ANALMUSIC Intentional noise — INTNOISE Analog voice — ANALVOICE Noise/Static — NOISESTATC Chaff — CHAFF Bagpipes — BAGPIPES Other — OTR Explain CHAFF or OTR in a free-text set.
15	ecm effect	m	3-10A	Enter the code for ECM effect: EFFECT — CODE — EFFECT — CODE Denial — DENIAL Increased handling time — DELAYS Inter-mittent — INTER-MITNT Loss of Secure mode — LOSTSECURE Nuisance — NUISANCE Break Lock — BREAKLOCK Other — OTR Explain OTR in a free-text set.
16	eccm action	m	3-10A	Enter the code for friendly ECCM action: ECCM ACTION — CODE Worked Through — WORKTHRU Cease Emitting — CEASEXMTR Change Band — CHANGEBAND Change Frequency — CHANGEFREQ Change Location — CHANGELOC Increase Power — INCRSPWR Change Mode — CHANGEMODE Change Technical Characteristics — CHANGETECH Change Directivity — CHANGEDIR Chaff — CHAFF Other — OTR Explain OTR in a free-test set.

Figure 4-3. Sample MIJIFEEDER record message format (continued).

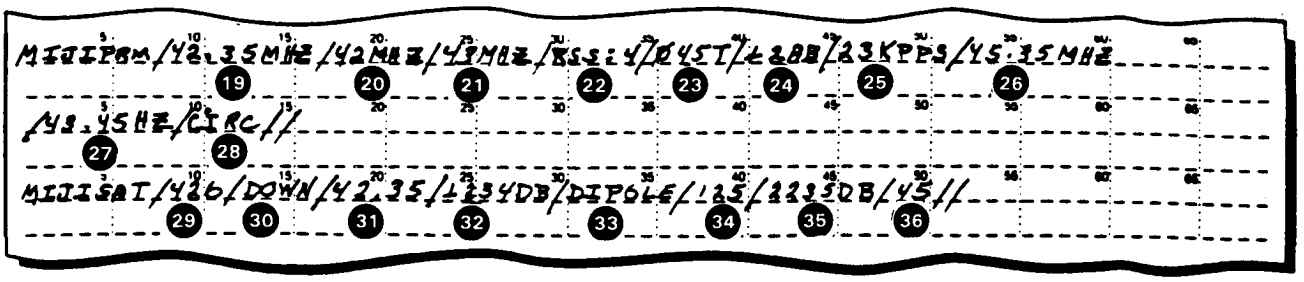


EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
17	enemy reaction	c	3-10A	Enter the code as in the previous field for enemy reaction to ECCM actions.
18	percent effect	o	1-2N	Enter the percent of effectiveness of the MIJI prior to starting countermeasures.
	MIJIPRM	m r		Use this set to report MIJI data.
19	freq	m	3-11ANS	Enter the frequency in use at time of MIJI event as follows:
			1-8NS	• Enter the number (use decimal point if needed).
			2-3A	• Then enter unit of measure: hertz HZ, kilohertz KHZ, megahertz MHZ, or gigahertz GHZ.
				NOTE: Use the next 2 fields to report a bandwidth being interfered with
20	lower freq	c	3-11ANS	Enter the lowest frequency affected by ECM.
21	upper freq	c	3-11ANS	Enter the highest frequency affected by ECM.
22	signal strength	o		Enter one of the following field names and signal strength:
	MSS: or RSS:		1-2N 1N	Measured signal strength in decibels. OR Rated signal strength. Enter a scale value: 1 (lowest), 2,3,4, or 5 (highest).
23	miji bearing or loc	o	4-15AN	Enter the bearing or location of the source of the MIJI from the victim in one of the following ways:

Figure 4-3. Sample MIJIFEEDER record message format (continued).

EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
	bearing	o	4AN	Enter the bearing of the source of the MIJI from the victim as follows:
			3N	• Enter the angle in degrees.
			1A	• Then enter T (for True North) or M (for Magnetic North).
	or			OR
	miji fix - utm 100 meters	o	11AN	Enter the location of the MIJI source in UTM coordinates to 100 meters. ENTRY LIST 11
	or			OR
	miji cut - utm 1000 meters	o	9AN	Enter the location of the MIJI source in UTM coordinates to 1000 meters. ENTRY LIST 11
	or			OR
	miji fix - seconds	o	15AN	Enter the location of the MIJI source in Lat/Long coordinates to the nearest second. ENTRY LIST 11
	or			OR
	miji cut - minutes	o	11AN	Enter the location of the MIJI source in Lat/Long coordinates to the nearest minute. ENTRY LIST 11
24	elint notation	o	4-5AN	**Enter the ELINT notation or sorting code equating to the ECM signal IAW Data Requirement No E-5A, DIAM 65-6-6.**
25	pulse repetition freq	o	3-7AN	**Enter the pulse repetition frequency of ECM as follows:**
			1-4AN	• Enter the number. K or M permitted as last character.
			2-3A	• Enter PPS.
26	ecm	o	3-11ANS	**Enter the ECM center frequency as follows:**
			1-8NS	• Enter the number (use decimal point if needed).
			2-3A	• Then enter unit of measure: hertz HZ, kilohertz KHZ, megahertz MHZ, or gigahertz GHZ.
27	scan rate	o	3-8ANS	**Enter the ECM rate as follows:**
			1-5NS	• Enter the number (Use decimal point if needed).
			2-3A	• Then enter unit of measure: Hertz HZ, or seconds per cycle SPC.
28	scan type	o	2-4A	**Enter the ECM scan type.** ENTRY LIST 92

Figure 4-3. Sample MIJIFEEDER record message format (continued).

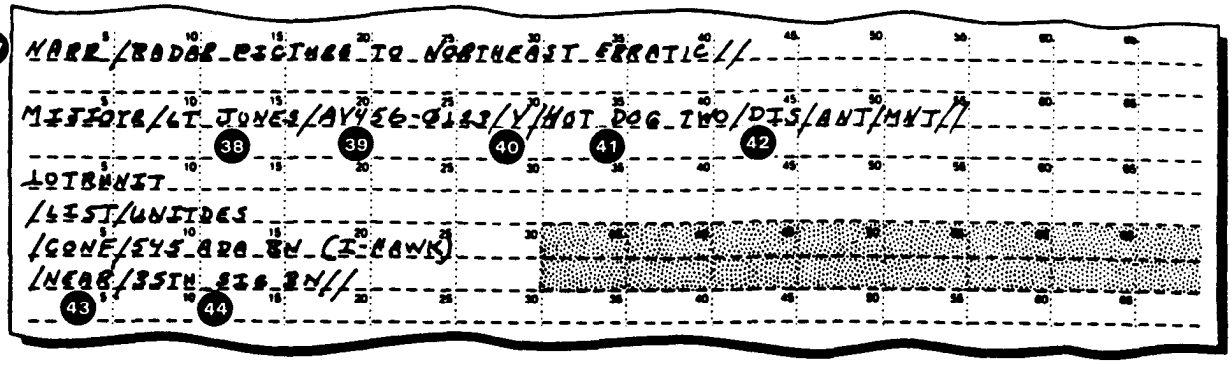


EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
	MIJISAT	c		This set is required if the MIJI incident being reported affects satellite links.
29	space obj id	m	3-6N	Enter the NSSC code for the space object.
30	link	m	2-4A	Enter the signal links affected by the MIJI. Use UP for uplink or DOWN for downlink.
31	freq	m	1-8NS	Enter the receiver's frequency bandwidth in megahertz (use decimal point if needed).
32	receiver sensitivity	m	3-6ANS	Enter receiver sensitivity in decibels, followed by DB. (Use hyphen for negative values.)
33	antenna type	m	5-17ANS	Enter the code for antenna type: TYPE — CODE Dipole — DIPOLE Omnidirectional — OMNIDIRECTIONAL Phased Array — PHASED ARRAY Other — OTHER Explain OTHER in free text set.
34	antenna size	m	1-3N	Enter the size of the antenna in feet.
35	antenna gain	m	3-6ANS	Enter antenna gain in decibels, followed by DB. (Use hyphen for negative values.)
36	antenna elevation	m	2N	Enter the angular elevation of the antenna to the space object.

Figure 4-3. Sample MIJIFEEDER record message format (continued).

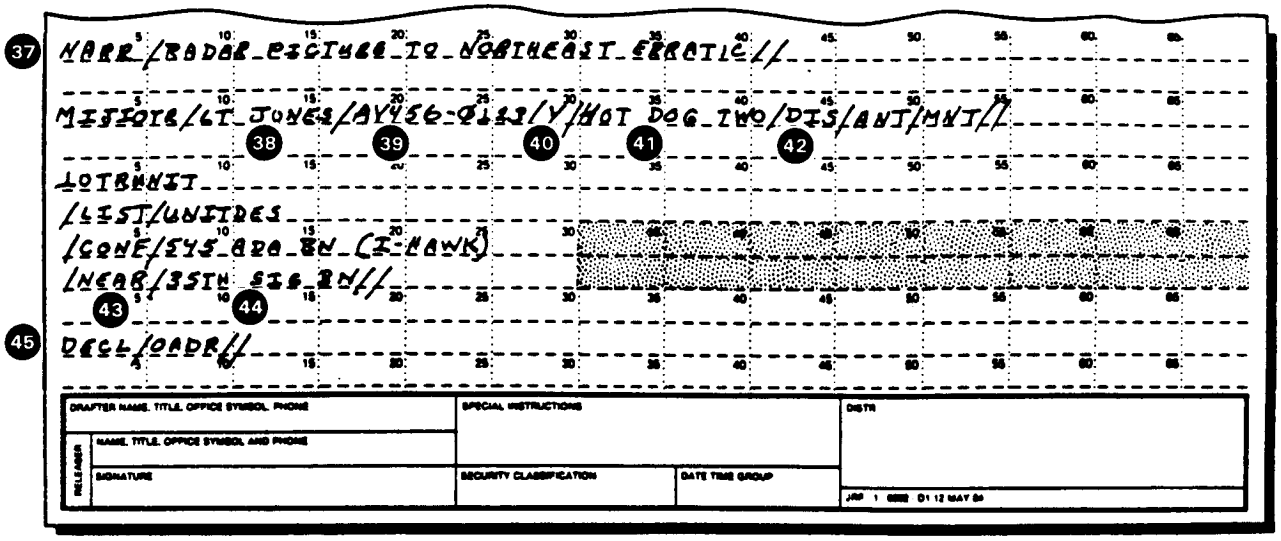
EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
37	NARR	o		Enter free text as necessary concerning sets MIJITYP, MIJIEFF, MIJIPRM, and MIJISAT.
	MIJIOTR	m		Use this set to report other information regarding the MIJI incident.
38	contact name	m	1-20ANBS	Enter the name of the person knowledgeable about the MIJI incident.
39	contact number	m		Enter the MIJI contact number in one of the following ways:
	phone number		3-15ANBS	Enter the telephone number of the person entered in the contact name field.
	or			OR
	freq		1-8NS	Enter the contact frequency in megahertz of the person entered in the contact name field. (Use decimal point if needed.)
	or			OR
	designator		1-8AN	Enter the contact frequency designator of the person entered in the contact name field.
40	technical assistance	m	1A	Enter Y (for yes) if technical assistance is required. Otherwise, enter N (for no).
41	nickname or codeword	m		Enter the nickname or codeword in one of following ways:
	exercise nickname		1-56ANBS	Enter the nickname of an exercise being conducted nearby, in which the reporting unit is not participating.
	or			OR
	operation codeword		1-32ANBS	Enter the name or codeword of an operation being conducted nearby, in which the reporting unit is not participating.

Figure 4-3. Sample MIJIFEEDER record message format (continued).



EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
42	trouble shooting action	m r	3A	Enter the troubleshooting action taken at receiver site to isolate the source or cause of the MIJI incident. Select from one of the following: TYPE — CODE Disconnect Antenna — DIS On/Off Check — OFF Different Receiver — RCV Switch Antenna — ANT Check Filters — FIL Maintenance Check — MNT Other — OTR Explain OTR in free text set.
	1OTRUNIT	o		Use this set to identify other units confirming the MIJI incident or nearby units/ vessels which could have caused the incident. Enter the set name, then the column headers on the next line. Start each header in the space shown below: /LIST /UNITDES 1 6
43	LIST	m	4A	LEFT JUSTIFY Enter the code CONF for confirming units or NEAR for nearby units.
44	UNITDES	m	1-24ANBS	LEFT JUSTIFY Enter the unit designator.

Figure 4-3. Sample MIJIFEEDER record message format (continued).



EX	SET NAME FIELD NAME	CAT s f	NR OF CHAR	EXPLANATION
45	DECL	c		If the message is classified, use this set to enter declassification or downgrading instructions.
	inst	m	1-25ANBS	Enter the instructions in one of the following ways: INSTRUCTIONS — ENTER Declassify — date or event Downgrade to CONFIDENTIAL — DG(C), then date or event Downgrade to SECRET — DG(S), then date or event Originating Agency's Determination Required — OADR

Figure 4-3. Sample MIJIFEEDER record message format (continued).

4-5. Meaconing, Intrusion, Jamming, and Interference Security Classification Guide

Security classification of MIJI incidents or MIJI evaluation reports is determined principally by intent and location of the implied or stated source of the problem. Stations in combat areas or having a sensitive military mission ordinarily classify all MIJI reports.

Information Revealing:	Classification
a. The specific identification of an unfriendly platform or location by country or coordinates as the source of meaconing, intrusion, or jamming incident.	S; OADR
b. The term meaconing, intrusion, jamming and interference; the acronym MIJI; and that MIJI analysis is a function of the JEWC.	U
c. That an organization submits MIJI incident reports.	U
d. Broadly stated objectives of the MIJI program, including explanation of each of the terms that comprise the acronym MIJI.	U
e. Suspected meaconing, intrusion, or jamming, but sources cannot be identified.	C; OADR
f. Interference when source is clearly identified as US or friendly nation electromagnetic emitters.	U
g. Interference to US or friendly country electromagnetic equipment caused by ECM exercise in unfriendly nations.	C; OADR
h. Interference from unfriendly radio broadcast stations, meteorological stations, and other such fixed stations.	C; OADR

i. Parametric data of classified US electromagnetic equipment. Refer to classification guide for the equipment affected.	Classify correspondence equal to the security category assigned to the equipment affected.
j. Specific or general susceptibility or vulnerability of US electronic system to foreign exploitation.	S; OADR

Appendix A

Entry List 11
Location

There are several different ways of giving a location in JINTACCS messages. This entry list shows you how to write locations in the following ways:

- UTM coordinates
- Abbreviated UTM coordinates
- Latitude and longitude (Lat/Long)
- Verified latitude and longitude
- Geographic reference (GEOREF)
- Bearing and range (meters)
- Bearing and range (nautical miles)
- Basic Encyclopedia number (BE number)

When you use this entry list make sure to use the section called for by the Chapter 3 message instructions. Also make sure to write your location to the accuracy called for by the message instructions.

UTM

Follow the directions below to enter UTM coordinates.

(1). Enter the grid zone designator in first 3 spaces (2 numbers, 1 letter).

(2). Enter 100,000 meter grid square (2 letters).

(3). The next spaces (up to 5) are for casting.

(4). The next spaces (up to 5) are for northing.

EXAMPLES:															
	NEAREST 1 METER	3	2	S	M	V	1	2	3	4	5	1	2	3	4	5
	NEAREST 10 METERS	3	2	S	M	V	1	2	3	4	1	2	3	4		
	NEAREST 100 METERS	3	2	S	M	V	1	2	3	1	2	3				
	NEAREST 1000 METERS	3	2	S	M	V	1	2	1	2						

NOTE: Make sure to write UTM coordinates to the accuracy required by Chapter 3 directions. If you do not have the location to the required accuracy put zeros in the spaces for the unknown values. For example, if you must write coordinates to the nearest 1 meter, but you only know them to the nearest 100 meters enter:

3 2 S M V 1 2 3 0 0 1 2 3 0 0

ABBREVIATED UTM

Enter abbreviated UTM coordinates by following the same steps as above for UTM coordinates EXCEPT start with step 2. (Do not enter in the grid zone designator.) You can write abbreviated UTM coordinates to the accuracies shown in the examples below.

EXAMPLES:	**NEAREST 10 METERS**	M V 1 2 3 4 1 2 3 4
	NEAREST 100 METERS	M V 1 2 3 1 2 3

LAT/LONG

Follow the directions below to enter Latitude and Longitude coordinates.

(1). Enter latitude in degrees (00-90), minutes (00-59), seconds (00-59). If message instructions call for it, you may enter minutes or seconds to the nearest tenth (.1).

(2). Enter N for North latitude or S for South latitude.

(3). Enter longitude in degrees (000-180), minutes (00-59), seconds (00-59). If a message instructions call for it, you may enter minutes or seconds to the nearest tenth (.1).

(4). Enter E for East latitude or W for West latitude.

EXAMPLES:	**NEAREST TENTH OF A SECOND**	4 5 2 3 1 3 . 4 N 1 2 2 4 6 1 7 . 2 W
	NEAREST SECOND	4 5 2 3 1 3 N 1 2 2 4 6 1 7 W
	NEAREST TENTH OF A MINUTE	4 5 2 3 . 1 N 1 2 2 4 6 . 2 W
	NEAREST MINUTE	4 5 2 3 N 1 2 2 4 6 W
	NEAREST DEGREE	4 5 N 1 2 3 W

NOTE: Make sure to write LAT/LONG coordinates to the accuracy required by Chapter 3 directions. If you do not have the location to the required accuracy put zeros in the spaces for the unknown values. For example, if you must write coordinates to the nearest second, but you only know them to the nearest minute enter:

4 5 2 3 0 0 N 1 2 2 4 6 0 0 W

VERIFIED LAT/LONG

Follow the directions below to enter verified Latitude and Longitude coordinates.

(1). Enter latitude in degrees (00-90), minutes (00-59), and seconds (00-59).

(2). Enter N for North latitude or S for South latitude.

(3). Enter the checksum digit for latitude (righthand digit of the sum of all the digits in latitude).

(4). Enter a hyphen (-).

(5). Enter longitude in degrees (000-180), minutes (00-59), and seconds (00-59).

(6). Enter E for East longitude or W for West longitude.

(7). Enter the checksum digit for longitude (righthand digit of the sum of all the digits in longitude).

EXAMPLES: NEAREST SECOND 4 5 2 3 1 3 N 8 - 1 2 2 4 6 1 7 W 3
NEAREST MINUTE 4 5 2 3 N 4 - 1 2 2 4 6 W 5

NOTE: Make sure to write verified LAT/LONG coordinates to the accuracy required by Chapter 3 directions. If you do not have the location to the required accuracy put zeros in the spaces for the unknown values. For example, if you must write coordinates to the nearest second, but you only know them to the nearest minute enter:
4 5 2 3 0 0 N 4 - 1 2 2 4 6 0 0 W 5

GEOREF

Follow the directions below to enter GEOREF coordinates.

(1). Enter 2 letters for the 15-degree segment of the Earth defined by the GEOREF system.

(2). Enter 2 letters for the l-degree segment of the Earth defined by the GEOREF system.

(3). Enter 2 digits (00-59) to show the casting coordinate to the nearest minute.

(4). Enter 2 digits (00-99) to show the casting coordinate to the nearest hundredth of a minute.

(5). Enter 2 digits (00-59) to show the northing coordinate to the nearest minute.

(6). Enter 2 digits (00-99) to show the northing coordinate to the nearest hundredth of a minute.

EXAMPLES:		
	Nearest hundredth of a minute	D K Q A 2 4 1 5 1 2 2 4
	Nearest minute	D K Q A 2 4 1 2
	Nearest degree	D K Q A

NOTE: Make sure to write GEOREF coordinates to the accuracy required by Chapter 3 directions. If you do not have the location to the required accuracy put zeros in the spaces for the unknown values. For example, if you must write coordinates to the nearest minute, but you only know them to the nearest degree enter:
D K Q A 0 0 0 0

BEARING AND RANGE (METERS)

NOTE: Use this method only in the MCMOPS and MINEOPS messages.

Follow the steps below to give location of one object by giving its direction and distance in meters from another object.

(1). Enter direction (degree magnetic) in the first three spaces (000-359).

(2). Enter a hyphen. Then enter the distance in meters. You can use up to five spaces (1-99999).

(3). Enter a hyphen. Then enter the name of the location you are measuring from (city, town, terrain feature, call sign, reference point from an operations order, etc.). You can use up to 12 spaces.

EXAMPLE: The following example shows an object located 500 meters from Hill 239 in a direction of 50 degrees magnetic:

0 5 0 - 5 0 0 - H I L L 2 3 9

NOTE: You can use bearing and range in meters to outline an area in set "MINEFIELD" of the MINEOPS message or sets "MCMACT, MOA, and SAFELANE" of the MCMOPS message. Use the repeatable field "location" as shown below:

(1). In the first field give the location of the first reference point. (Use LAT/LONG, UTM, or location name.)

(2). In the next fields use bearing and range in meters to give the relative location of each point from the point before it.

EXAMPLE: The example below shows an area where:

- Point A is at 22° 15' north latitude and 30° 9' east longitude.
- Point B is 5000 meters from the Point A in a direction of 45° magnetic.
- Point C is 3000 meters from Point B in a direction of 325° magnetic

/ 2 2 1 5 N 0 3 0 0 9 E / 0 4 5 - 5 0 0 0 - A / 3 2 5 - 3 0 0 0 - B / /

(POINT A) (POINT B) (POINT C)

BEARING AND RANGE (NAUTICAL MILES)

Follow the steps below to give the location of one object by giving its direction and distance in nautical miles from another object.

(1). Enter 3 digits (000-359) to give the direction (degrees true for maritime, degrees magnetic for all other) from one object to the other object.

(2). Enter a hyphen, Then enter up to 12 characters to give the location from which you are measuring (city, town, terrain feature, call sign, reference point from an operations order, etc.).

(3). Enter a hyphen. Then enter up to 3 digits (0-999) to give a distance (nautical miles) from one object to the other object.

EXAMPLE

The following example shows an object 25 nautical miles from Hill 123 on a bearing of 75 degrees magnetic.

0 7 5 - H I L L 1 2 3 - 2 5

BASIC ENCYCLOPEDIA NUMBERS

There are several ways to write basic encyclopedia (BE) numbers. The tables on the next two pages show you how to write each one. (Each of the columns labeled A-H is for a different type BE number. Make sure to use the right table and column for the message you are writing).

Some BE numbers are assigned by DIA. They are in the columns marked by an *. If you have a DIA assigned BE number you don't need to follow the instructions to enter it. Just enter it as is. The instructions are just to help you read DIA assigned numbers in messages you receive.

To enter BE numbers you originate in the field follow the instructions in the proper column and table shown below.

- Use Table I (any column) for:

IIR and RECCEXREP

- Use Table II (any column) for:

AFU.MFN	FM.CFF	FP.FPO	NUCWARN
AFU.MFR	FM.FMC	FP.FPT	TACELINT
ATI.ATR	FM.MTO	FP.NUCSCD	TARBUL
ATI.TIR	FM.NCF	INTREP	TGTINFOREP
ATO.CONF	FM.SUB	MISREP	

- Use Table II, Column F for:

AIRSUPREQ	ALLOREQ	REQCONF	SARSIT
ALORD	JSARREQ	REQSTATTASK	SORTIEALOT

TABLE I

USE FOR IIR AND RECCEXREP ONLY

(FOR ALL OTHER MESSAGES SEE TABLE II)

A*	B	C	D	E	
X	X	X	X	X	(1) Enter the DIA assigned world area number (0000-9999).
X X X	 X 	 	 X X X 	 X 	(2) Enter one of the following program indicator codes to show type of installation or target: PROGRAM/TYPE — CODE Electronics — E Ficticious — F Suspect — X Directed search area — V Broad search area or transitory target — W Line of communication — U No particular type — 0(NOTE: DIA printouts use a hyphen (-) instead of 0)
		X	X		(3) Enter the two letter producer unit identification code from DIAM 57-5.
	X		X	 X	(4) If you entered X, V, or U in step (2) above, enter the two letter producer unit identification code from DIAM 57-5 and a 3 digit originator assigned number within the world area. OR If you entered W in step (3) above, enter the DIA assigned 200 world area grid (WAG), the 50WAG, and the 3WAG.
X					(5) Enter the 5 character DIA assigned installation identification serial number (00000-99999 or A0000-Z0000).
	X				(6) Enter the 4 digit originator assigned installation identification serial number (0000-9999).
					(7) Enter the 3 digit sequence number (001-999).

* Instructions in Column A are for reading DIA assigned BE numbers.

TABLE II

USE FOR ALL MESSAGES EXCEPT IIR AND RECCEXREP

F*	G*	H	
			(1) Enter one of the following codes to show the type of BE NUMBER: TYPE — CODE BE number — B BE number with suffix — S Field initiated BE number — F
X	X	X	
X	X	X	(2) Enter the DIA assigned world area number (0000-9999).
			(3) Enter one of the following program indicator codes to show type of installation or target: PROGRAM/TYPE — CODE Electronics — E Ficticious — F Suspect — X Directed search area — V Broad search area or transitory target — W Line of communication — U No particular type — 0(NOTE: DIA printouts use a hyphen (-) instead of 0)
X	X		
X	X		
X	X		
		X	(4) Enter the two letter producer unit identification code from DIAM 57-5.
			(5) If you entered X, V, U or W in step (3) above, enter the two letter producer unit identification code from DIAM 57-5 and a 3 digit originator assigned number within the world area. OR If you entered W in step (3) above, enter the DIA assigned 200 world area grid (WAG), the 50WAG, and the 3WAG.
X	X		(6) Enter the 5 character DIA assigned installation identification serial number (00000-99999 or A0000-Z9999).
		X	(7) Enter the 4 digit originator assigned installation identification serial number (0000-9999).
X			(8) Enter the DIA assigned BE category suffix number (00-99). NOTE: 00 means no suffix value.

* Instructions in Columns F and G are for reading DIA assigned BE numbers.

Appendix B

Entry List 97
Organization Type

ORGANIZATION TYPE	CODE
Unknown	UNK
Administrative	ADMIN
Airborne Commando	ABNCMDO
Airborne Infantry	ABNINF
Air Cavalry	AIRCAV
Air Defense Artillery	AAA
Airmobile Infantry	AMBLINF
Air-to-Air Missile	AAM
Air-to-Surface Missile	ASM
Amphibious Assault	AMPHASLT
Amphibious Engineers	AMPHENG
Amphibious Tank	AMPHTK
Antiair Warfare	AAW
Antiarmor Missile	AARMMSL
Antisubmarine Warfare	ASW
Armor	ARMOR
Armored Cavalry	ARMDCAV
Army Aviation	ARMYAVN
Artillery Unit	ARTY
Assault Engineers	ASLTENG
Assault Landing	ASLTLAND
Biological Ordnance Capable Unit	BIO
Bomber	BMBR
Cavalry	CAV
Chemical	CHEM
Combat Engineers	CMBTENG
Combat Service Support	CMBTSPT
Combat Type Unknown	CMBT
Combined Arms	CMBARM
Commando	CMDO
Composite Warfare Commander	CWC
Dismounted Cavalry	DMTDCAV

ORGANIZATION TYPE	CODE
Electronic Countermeasures	ECM
Electronic Support Measures	ESM
Engineer	ENG
EW Coordinator	EWC
Field Artillery	FLDARTY
Fighter	FTR
Fighter Bomber	FTRBMBR
Frog SSM Unit	FROG
Gun-Howitzer	HOWTZR
Helicopter	HELO
Infantry	INF
Infantry on Foot	INFONFT
Intelligence	INTEL
Maintenance	MAINT
Marine Amphibious Brigade	MAB
Marine Amphibious Force	MAF
Marine Amphibious Unit	MAU
Mechanized Infantry	MECHINF
Medical	MED
Military Police	MP
Military School or Academy	SCH
Mining	MINE
Mortar	MORT
Motorized Rifle Troops	MRFLTRP
Mountain Infantry	MTINF
Navy Infantry/Marines	
Nuclear Ordnance Capable Unit	NUC
Ordnance	ORD
Paramilitary	PARAMIL
Picket	PKT
Pontoon	PONT

ORGANIZATION TYPE	CODE
Railroad Troops	RRTRPS
Ranger	RNGR
Reconnaissance	RECON
Reconnaissance, Armor	RCNARM
Sapper (Mine)	SAP
Scud SSM Unit	SCUD
Signal/Electronics	SIGELECT
Special Forces	SPFORCE
Supply	SUPLY
Surface-to-Air Missile	SAM
Surface-to-Surface Missile	SSM
Surveillance	SUR
Tactical Air Control	TACAIRC
Tactical Missiles	TACMSLS
Tank	TK
Light Tank	LTK
Medium Tank	MTK
Heavy Tank	HTK
Tank Destroyer	TKDSTR
Tank Recovery	TKRCVY
Training	TNG
Transport	TRNSP
Transportation	TRANSP
Weather	WX

Appendix C

Entry List 98
Echelon Level

ECHELON LEVEL	CODES
Unknown	UNK
Army Army	AIRARMY
Air Command	AIRCMD
Air Control Party	AIRCONP
Air Corps	AIRCRPS
Air Detachment	AIRDET
Air Division	AIRDIV
Air Element	AIRELMT
Air Flight	AIRFLT
Air Group	AIRGP
Air Regiment	AIRRGT
Air Squadron	AIRSQ
Air Wing	AIRWG
Army Group	ARMYGP
Battalion	BN
Battery	BTY
Border District Headquarters	BRDHQ
Brigade	BDE
Combat Command	CMBTCMD
Command	CMD
Company	CO
Corps	CORPS
Detachment	DET
Division	DIV
Divisional Artillery Group	DAG
Field Army	ARMY
Fleet	F
Front	FRNT
Group	GP
Group of Forces	GPFRCS
Group of Fronts	GPFRNT

ECHELON LEVEL	CODES
Komendatura	KMDTR
Major Fleet	FLT
National Defense Headquarters	NDHQ
Naval Detachments	NAVDET
Naval Division	NAVDIV
Naval Force	NAVFOR
Naval Group	NAVGP
Naval Section	NAVSEC
*Naval Task Element	TE
*Naval Task Force	TF
*Naval Task Group	TG
Naval Squadron	NAVSQ
*Naval Task Unit	TU
Numbered Fleet	NFLT
Otryad	OTRYD
Patrol	PTRL
Platoon	PLT
Regiment	RGT
Regimental Artillery Group	RAG
Section	SEC
Squad	SQD
Squadron	SQ
Task Element	TSKELMT
Task Force	TSKFOR
Task Group	TSKGP
Task Unit	TSKUNIT
Theater Army	THTA
Troop	TROOP
Zastrova	ZASTRV

*ONLY USE THESE ENTRIES IN SETS "NUID" AND "7SHPALRT"

Appendix D

Implementing Electronic Counter-Countermeasures for Radio Systems

D-1. Background

a. It is assumed that your system has the proper received signal level and that you and the other station are using low power; your sites are masked from the enemy when possible by using terrain obstacles.

b. Systems that are parallel to the front lines are less open to ECM than systems that are perpendicular. Division systems are more prone to ECM than corps systems because of the proximity to front lines.

c. Multichannel systems should be separated from HF radios because of the high power and resulting spontaneous and harmonic radiation. FM radios should not be collocated with multichannel sets for the same reasons. Collocated multichannel antennas should be either back to back or on-line to reduce mutual interference. Antennas should never be in line with one another.

d. The need for dispersion and the need for high mobility always clash. To mask a unit's location, all radios including multichannel should be separated from the command post by at least 2 kilometers (1.2 miles). Cables should not be used to interconnect radios and the command post because cable recovery is too time consuming. A radio link should be used when available.

e. In most cases, the enemy prefers to monitor our systems even though they are denied clear reception of our signals because of encryption. An electronic signature of our unit's location is of better intelligence than jamming. Multichannel systems indicate headquarters' locations. Their presence indicates a stable nonmobile situation. We give the enemy valuable signal intelligence when stations go off the air and then reappear elsewhere. We are telling the enemy our situation is changing.

f. Determining if ECM is being used against your system is not easy since most interference is from our own emitters.

g. Proper and diligent frequency management is imperative. When interference occurs, submit the MIJI report. Do not change the frequency up or down to get away from interference. This creates additional problems for other users. Use tactical satellite instead of terrestrial line of sight when possible.

D-2. Procedures

a. The following may indicate that your systems are being interfered with either intentionally or unintentionally:

- Subscribers report that trunks are noisy, or that the speech of the other party is fuzzy or unintelligible.
- Subscribers and switchboard operators report no contact with a particular unit(s).
- You are unable to make contact with the distant end on the orderwire.

b. The following steps reduce or eliminate the effects of ECM or mutual interference:

- Checking equipment for proper alignment and frequency.
- Increasing power if possible.
- Checking antenna for correct azimuth and polarization.
- Varying antenna height or relocating antenna.
- Requesting a new frequency if the above fails to work.
- Initiating a MIJI report.

Glossary

Abbreviations and Acronyms

AM	amplitude modulated
AR	Army regulation
ARTEP	Army Training and Evaluation Program
attn	attention
AUTOVON	automatic voice network
BE	basic encyclopedia
BFO	beat frequency oscillator
bn	battalion
c	CONFIDENTIAL
CEOI	communications-electronics operation instructions (see SOI)
CEWI	combat electronic warfare and intelligence
COMINT	communications intelligence
COMSEC	communications security
CPT	captain
CW	continuous wave
C^3	command, control, and communications
C^3CM	command, control, and communications countermeasures
DA	Department of the Army
DF	direction finder
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures

E-O	electro-optics
EEFI	essential elements of friendly information
EPLRS	Enhanced Position Location Reporting System
ESM	electronic warfare support measures
EW	electronic warfare
FHMUX	frequency hopping multiplexer
FLOT	forward line of own troops
FM	frequency modulated/field manual (when used with a number)
G2	Assistant Chief of Staff, G2 (Intelligence)
G3	Assistant Chief of Staff, G3 (Operations and Plans)
GEOREF	geographic reference
GHz	gigahertz
HF	high frequency
hi	high
HPBVWA	high-power broadband vehicular whip antenna
HQ	headquarters
IAW	in accordance with
IED	imitative electronic deception
inf	infantry
IHFR	intermediate high frequency radio
JEWC	Joint Electronic Warfare Center
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JTF	joint task force
JTIDS	Joint Tactical Information Distribution System

JUH-MTF	Joint User Handbook for Message Text Format
kHz	kilohertz
km	kilometer
MED	manipulative electronic deception
MHz	megahertz
MIJI	meaconing, intrusion, jamming, and interference
MSE	Mobile Subscriber Equipment
MSRT	mobile subscriber radiotelephone terminal
NAVAID	navigational aid
NCS	net control station
OADR	Originating Agency Determination Required
OPCODE	operations code
OPSEC	operations security
pam	pamphlet
PROWORD	procedure word
pwr	power
RATELO	radiotelephone operator
RAu	radio access unit
RDF	radio direction finding
REC	radio electronic combat
RWR	radar warning receiver
s	SECRET
S2	Intelligence Officer (US Army)
S3	Operations & Training Officer (US Army)
SED	simulative electronic deception

SIGINT	signals intelligence
SINCGARS	Single-Channel Ground and Airborne Radio System
SNAP-1	steerable null antenna processor
SOI	signal operation instructions
SOP	standing operating procedure
TRADOC	United States Army Training and Doctrine Command
TX	Texas
U	unclassified
US	United States
VHF	very high frequency
Z	Zulu

Terms

AUTHENTICATION. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.

BREVITY CODE. A code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content.

COMMUNICATIONS-ELECTRONICS OPERATION INSTRUCTIONS (CEOI). (See signal operation instructions.)

COMMUNICATIONS INTELLIGENCE (COMINT). Intelligence and technical information derived from foreign communications by other than the intended recipients.

COMMUNICATIONS SECURITY (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

DECEPTION. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence in order to induce him to react in a manner prejudicial to his interests.

ELECTROMAGNETIC SPECTRUM. The frequencies present in a given electromagnetic radiation. A particular spectrum could include a single frequency or a wide range of frequencies.

ELECTRONIC COUNTER-COUNTERMEASURES (ECCM). That major subdivision of electronic warfare involving actions taken to retain friendly effective use of the electromagnetic spectrum.

ELECTRONIC COUNTERMEASURES (ECM). That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum.

ELECTRONIC WARFARE (EW). Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. Electronic warfare is divided into three categories - ESM, ECM, ECCM.

ELECTRONIC WARFARE SUPPORT MEASURES (ESM). That division of electronic warfare involving actions taken under the direct control of an operational commander to search for, intercept, locate, and identify sources of radiated electromagnetic energy for the purpose of immediate threat recognition.

EMISSION CONTROL. The management of the use of the electromagnetic spectrum by our forces.

ENCRYPT. To convert plain text into unintelligible form by means of a cryptosystem. This cryptosystem can be manual or electronic.

ESSENTIAL ELEMENTS OF FRIENDLY INFORMATION (EEFI). Items or activities associated with friendly planning which, if exposed to hostile intelligence activities, would serve as intelligence indicators and thus tend to compromise friendly intentions.

GUARDED FREQUENCIES. Frequencies restricted from friendly use or jamming operations, Guarded frequencies are the enemy's communications and electronics systems from which signals intelligence (SIGINT) and ESM information of tactical and technical importance is derived.

INTERCEPTION. As used in this manual, the act of listening to and/or recording signals intended for another party for the purpose of obtaining intelligence,

INTERFERENCE. Any electrical disturbance which causes undesirable responses in electronic equipment.

INTRUSION. The intentional insertion of electromagnetic energy into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

JAMMING. The deliberate radiation, reradiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy.

JOINT INTEROPERABILITY OF TACTICAL COMMAND AND CONTROL SYSTEMS (JINTACCS). A program which provides for information exchange on the battlefield among the military services, the Defense Intelligence Agency, and the National Security Agency. It uses standardized message formats, rules, and vocabulary. (Reference DA Pam 25-7.)

MEACONING. The transmission or retransmission of actual or simulated navigation signals to confuse navigation. Meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

NET CONTROL STATION (NCS). A station designated to control traffic and enforce circuit discipline within a given net.

OPERATIONS CODE (OPCODE). A code used to encrypt tactical information.

OPERATIONS SECURITY (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

OPERATIONS SECURITY INDICATORS. Actions or information, classified or unclassified, obtainable by an adversary that would result in adversary appreciations, plans, and actions harmful to achieving friendly intentions and preserving friendly military capabilities.

PREVENTIVE ECCM TECHNIQUES. Those measures taken to reduce the vulnerability of the friendly use of the electromagnetic spectrum to the efforts by the enemy to disrupt or destroy that use.

PROCEDURE WORD (PROWORD). A word or phrase limited to radio telephone procedure used to facilitate communications by conveying information in a condensed standard form. (Reference ACP 125.)

PROTECTED FREQUENCIES. Frequencies used by tactical friendly forces for a particular operational requirement that are restricted from friendly jamming operations.

RADIO LISTENING SILENCE. A period during which all or certain radio equipment is kept in a receive only mode on a given net except for the net control station.

RADIO SILENCE. A period during which all or certain radio equipment capable of radiation is kept inoperative.

REMEDIAL ECCM TECHNIQUES. Those actions taken to reduce or negate the effectiveness of enemy efforts to jam the friendly use of the electromagnetic spectrum.

SIGNAL OPERATION INSTRUCTIONS (SOI). A series of orders issued for the technical control and coordination of the signal activities of a command. Contains frequencies, call signs, and other information used to establish and maintain radio and other forms of communication.

SIGNAL-TO-JAMMING RATIO. The ratio at a selected point in a signal of the strength of a desired signal to that of a jamming signal.

SINGLE-CHANNEL GROUND AND AIRBORNE RADIO SYSTEM (SINCGARS). A new family of VHF-FM radios designed to provide the primary means of command and control for Infantry, Armor, and Artillery units. The radios can transmit and receive voice and tactical data while operating in a frequency hopping mode.

TABOO FREQUENCIES. Frequencies that are restricted from use or jamming by friendly forces. The following are some examples of these frequencies. Defense Communications System radar frequencies used for friendly early warning air defense; internationally controlled or treaty-governed frequencies, such as broadcast emergency frequencies and commercial air and shipping traffic control frequencies.

VOICE TEMPLATES. Standardized pre-formatted messages used with the JINTACCS message text procedures.

References

Required Publications

Required publications are sources that users must read in order to understand or to comply with this publication.

Allied Communications Publications (ACP)

125( )	Communication Instructions - Radiotelephone Procedures
131( )	Communication Instructions - Operating Signals

Army Regulations (AR)

105-2	(C) Electronic Counter-Countermeasures (ECCM)--Electronic Warfare Susceptibility and Vulnerability (U)
105-3	Reporting Meaconing, Intrusion, Jamming and Interference of Electromagnetic Systems
105-7	Quick Reaction Capability (QRC) for Electronic Warfare
525-20	Command, Control and Communications Countermeasures (C^3CM) Policy
525-22	(S) Electronic Warfare (EW) Policy (U)
530-1	Operations Security (OPSEC)
530-2	Communications Security
530-3	(C) Electronic Security (U)

Department of the Army Pamphlets (DA Pam)

25-7	Joint User Handbook for Message Text Formats (JUH-MTF)
380-2	(C) SIGSEC: Defense Against SIGINT (U)

Field Manuals (FM)

24-1	Combat Communications
24-18	Tactical Single-Channel Radio Communications Techniques
24-35	(0) Communications-Electronics Operation Instructions (The CEOI)
25-100	Training the Force
34-1	Intelligence and Electronic Warfare Operations
34-40	(S) Electronic Warfare Operations (U)
34-62	Counter-Signals Intelligence (C-SIGINT) Operations

Forms

DA Form 2028	Recommended Changes to Publications and Blank Forms

Related Publications

Related publications are sources of additional information. They are not required in order to understand this publication.

Allied Communications Publications (AC)

124( )	Communication Instructions - Radiotelegraph Procedures
124	(C) US Supplement to ACP 124( ) (U)
126( )	*(R) Communication Instructions - Teletypewriter (Teleprinter) Procedures (U)

Army Regulations (AR)

380-40	(C) Policy for Safeguarding and Controlling COMSEC Information (U)

Field Manuals (FM)

34-86	Direction Finding Operations
100-2-1	Soviet Army Operations and Tactics
100-5	Operations
101-5	Staff Organization and Operations

Projected Publications

Projected publications are sources of additional information that are scheduled for printing but are not yet available. Upon print, they will be distributed automatically via pinpoint distribution. They may not be obtained from the USA AG Publications Center until indexed in DA Pamphlet 25-30.

Field Manual (FM)

24-35	(0) Signal Operation Instructions "The SOI"

*Allied Restricted

Index

17 JULY 1990

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:

WILLIAM J. MEEHAN, II
Brigadier General, United States Army
The Adjutant General

DISTRIBUTION:

Active Army, ARNG, and USAR: To be distributed in accordance with DA Form 12-11-E, requirements for FM 24-33, Communications Techniques: Electronic Counter-Countermeasures (Qty rqr block no. 1075).

* U.S. GOVERNMENT PRINTING 0FFICE:1994-300-769/22213