FM 100-32 (Test)

RESCINDED Per DA Circular # 310-10, 15 Mar 78

FM 100-32 (TEST)

FIELD MANUAL

TACTICAL ELECTRONIC WARFARE

HEADQUARTERS, DEPARTMENT OF THE ARMY
JUNE 1975

This test publication is provided to disseminate the latest thought on electronic warfare. Unclassified and hypothetical data have been provided to insure the manual's usability for basic instruction in units and service schools where utilization of classified reference material is not feasible. Users are requested to submit recommended changes or comments using DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commandant, US Army Command and General Staff College, Fort Levenworth, Kansas 66027.

FIELD MANUAL
No. 100-32

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., *30 June 1975*

TACTICAL ELECTRONIC WARFARE

CHAPTER 1

GENERAL

1–1. Purpose

This manual provides guidance to commanders and staff officers in the tactical aspects of electronic warfare employment in combat operations. It has been purposely written without technical language to make it a more useful tool for tactical forces. An understanding of the concepts and discussions herein will assist in adaptation to the more technical language of FM 32–20, *Electronic Warfare*.

1–2. Scope

a. The doctrine in this test manual encompasses those principles and policies that have been derived from the study of experience, realistic simulations, and military judgment. Application of this doctrine requires judgment to adapt to the peculiarities of the situation, since textbook conditions will rarely exist. Recommendations and supporting rationale for changes to this doctrine should be sent to the Commandant, US Army Command and General Staff College, Fort Leavenworth, Kansas 66027.

b. This manual incudes the following information:

(1) Intelligence provided by and required for electronic warfare operations.

(2) Techniques for degrading enemy electronic systems.

(3) Methods to reduce the impact of enemy electronic warfare operations on friendly electronic systems.

(4) Electronic warfare considerations for deception planning.

(5) Generalized data concerning friendly and enemy electronic warfare capabilities.

(6) Command and staff responsibilities for control, planning, coordination, and execution of electronic warfare operations.

1–3. Basic Considerations

Electronic warfare (EW) is not a new capability for tactical commanders. Electronic warfare began affecting combat capability in World War I, but it has rarely been prominently employed in combat or in exercises by US Army elements due to an absence of awareness of the real significance of EW, in either its offensive or defensive role. EW resource nonavailability, security classifications, fear of disrupting friendly communication-electronic (C-E) systems impeded the growth of EW awareness.

a. Security. The classification of EW information and material has contributed to the mystique of EW. EW is viewed as a complicated and mysterious resource that should be kept behind the "green door" in the hands of technicians rather than being considered an element of combat power to be included in operational planning. Commanders can no longer accept this attitude. Security requirements can be met without unduly restrictive limitations on EW employment. Acceptance of this fact will facilitate realistic EW training at all levels of command.

b. Resources. Electronic warfare is a combat support system and must be considered along with artillery and aviation. However, there has been a major difference in the circumstances surrounding the employment of these systems. During other than active confrontation situations, the EW assets have not been a part of the division troop list. Consequently, they were not automatically considered in the conduct of the division's everyday activities as were the other combat support systems. The US Army Security Agency (USASA) is responsible for providing direct support units (DSU) with an EW capability to support Army combat organizations. In the past, sufficient resources have not been available to provide each separate brigade/regiment, division, and corps with such units. Current Department of Army actions will relieve this situation and provide the required DSU's, thereby giving the commander this asset on a continuing basis. Additionally, requirements for self-protection EW equipment are recognized. This equipment is exemplified by airborne radar and infrared (IR) warning receivers; airborne radar, IR and VT fuze-jammers to protect the aircraft itself; man portable and vehicular radar and IR illumination detectors; jamming and deception equipment to protect tanks and other combat vehicles from enemy antitank guided missiles; and expendable cannon or air-launched devices designed to disrupt communication-electronic systems and equipment. Though many of these items will function with a minimum of manual manipulation, optimum results will be obtained only through complete integration of system capability to assure balance and response to meet the anticipated enemy threat. Commanders and staff officers at all levels of command must be cognizant of this requirement and take action to meet their responsibility.

c. Current Requirement. Modern military forces have become increasingly dependent on electronic devices for command and control. The increasing demand for rapid and accurate communications has resulted in significant advances in both the quantities and technological sophistication of the systems employed. These factors, when viewed in the context of events of the last decade, have demonstrated that to be successful in combat a commander must not only control the land, sea, and air but also the communications-electronics environment. Such control envisages proper application of electronic environment to maintain friendly command and control systems while disrupting similar enemy systems. Electronic warfare must be an inseparable part of all operations orders and plans. Measures designed to disrupt enemy electronic systems or deceive enemy intelligence capabilities must be totally integrated into the commander's maneuver and fire plans. Information derived from employment of electronic warfare capabilities can, at times, be more valuable than a maneuver battalion or artillery battery. Conversely, a lack of proper communication security or operating procedures can be disastrous to friendly forces.

d. Capability. The Army has an EW capability and a system for its employment. Awareness and knowledge in this subject must be emphasized to insure adequate application. The commander has specific authorities for employment of available EW assets; he also has certain responsibilities to those personnel and units that conduct EW operations for him. These responsibilities must be understood, and a study of the chapters of the FM will provide a basis for that understanding. *Demand EW support, study its capabilities, and apply it at every opportunity—it is a "must."*

CHAPTER 2

LISTENING

2–1. General

Modern warfare requires extensive use of electronic equipment to maintain control over combat forces and surveillance over the battlefield. Since electronic equipment radiates both intentional and unintentional energy that can be detected by other than the intended recipients, it is a valuable source of information. Listening to the enemy's electronic emissions may provide the tactical commander with an indication of the magnitude of the enemy force, his intentions, technical information for disrupting his electronic devices, and other information useful in developing order of battle. Information derived from listening to the enemy's electronic devices is an indispensable input to the commander's estimate and, when integrated with other intelligence, normally provides assistance in answering the questions: who, what, when, where and how. All commanders can benefit from listening; however, the criteria prescribed by paragraph 5*b*(1) through (4), AR 105–87, must be met for authorizing listening operations.

2–2. What to Listen For

Rarely, if ever, will a commander have enough equipment resources and linguists to listen to all enemy electronic systems. Thus, priorities must be established for listening to the radios and radars that provide the most lucrative sources of information. Normally these will include those enemy electronic signals associated with command and control, fire control, air-ground coordination, and intelligence systems. Listening to other electronic systems should be assigned a lower priority unless the information being obtained dictates otherwise. The assignment of a lower priority to other electronic systems does not mean that those systems will not be monitored, but rather that they will be listened to when there is no activity on the systems assigned a higher priority.

2–3. Factors That Affect Listening

The enemy's communication and surveillance devices are quite similar to ours and require basically the same considerations for employment. Depending on the particular system, factors such as terrain, weather, distance, and security will determine the probability of detecting and listening to delectronic emissions.

a. To listen to some tactical electronic systems, the listening receiver must have line-of-sight with the target transmitter antenna. Locating the listening receivers on terrain or in airborne platforms to attain line-of-sight with the enemy transmitting antenna becomes a requirement. In addition, the location of listening receivers must also be within the effective range of the enemy transmitters. Just as US C-E equipment can only transmit for a specific distance, enemy electronic emitters are likewise limited. Therefore, depending on the type emitters being exploited, the listening receivers must be positioned as far forward as necessary to acquire the desired enemy signal.

b. There may be times when terrain and distance restrict efforts to listen to the enemy radios and radars from a ground site. Aircraft provide the means to extend the radio horizon. However, hostile air defense systems and severe weather can restrict airborne electronic warfare operations. Heavy overcast or precipitation may require instrument flying for listening platforms and reliance on radar control for position verification. These limitations to airborne systems, therefore, require complementary ground-based capabilities.

c. Just as emission control, good radio procedure, use of authorized codes and ciphers, and security equipment will deny friendly information to the enemy, enemy use of the same procedures and devices will assist in denying information to friendly intelligence efforts.

2–4. Listening Capabilities

There is an abundance of organic electronic equipment within the division that is capable of listening to the enemy electronic systems. A US Army Security Agency (ASA) division support company will normally be attached to the divi-

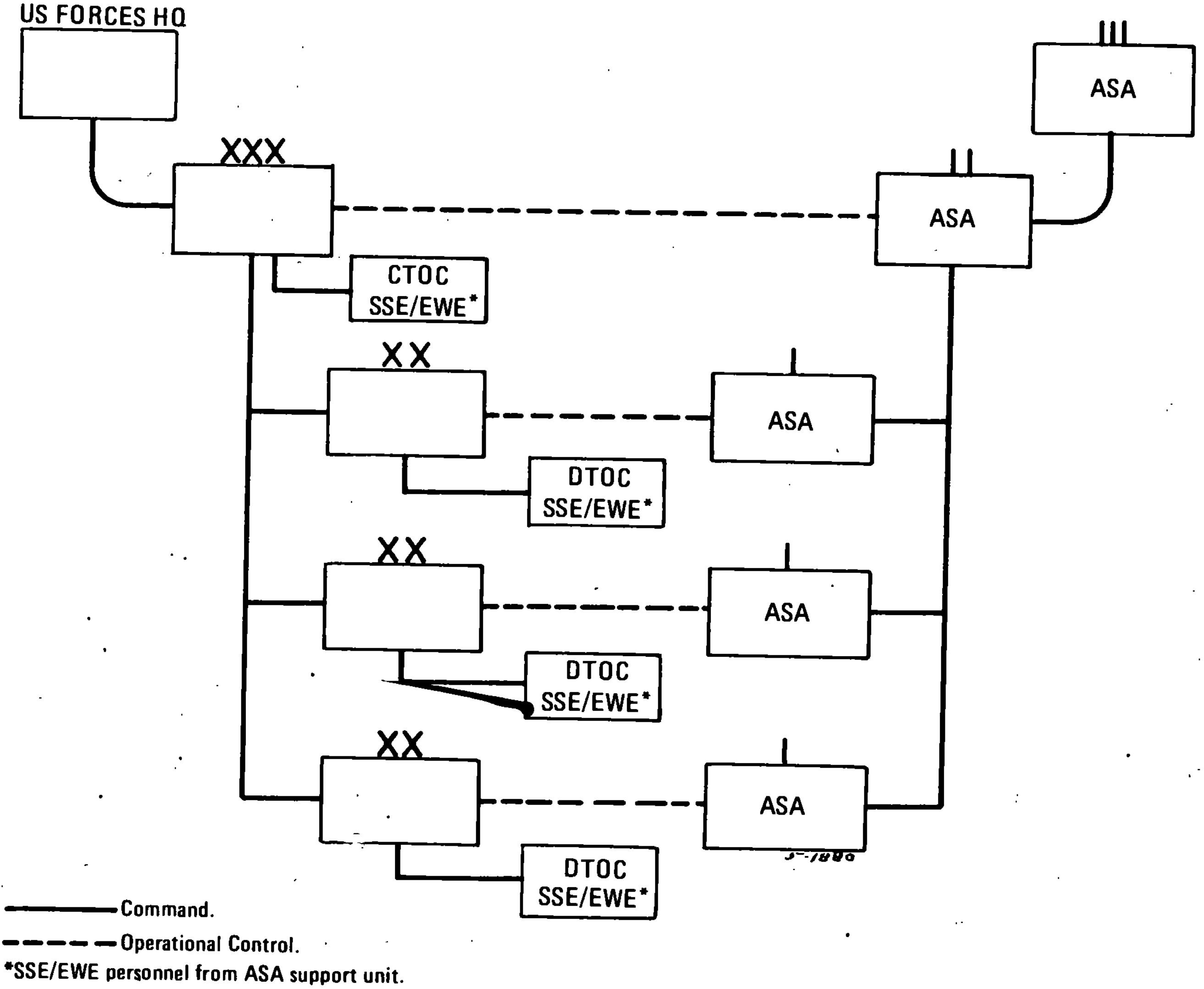

Figure 2-1. Type ASA organization in support of tactical forces.

	Friendly Listening Capability		
Enemy Electronic System	*Organic to Div*	*ASA Co Attached to Div*	*ASA Bn or Gp*
Command and Control	X	X	X
Fire Direction	X	X	X
Administration and Logistics	X	X	X
Air-Ground	X	X	X
Area Communications	X		X
Operation and Intelligence	X	X	X
Radars			
– Fire Control	X	X	X
– Acquisition	X	X	X
– CM/CB		X	X
– Surveillance		X	X
Facsimile			X
Radios			
FM	X	X	X
AM			
SSB	X	X	X
RTT	X	X	X
UHF (AM)	X	X	X

Figure 2–2. Friendly listening capability.

sion to provide direct support. This unit has the capability of listening to most types of electronic emissions from enemy electronic systems either from a ground mode or airborne platform. If systems are encountered beyond the capability of the attached ASA division support company, assistance can be obtained from the ASA battalion or group resources supporting the next higher tactical command echelon. Figure 2–1 represents a type ASA organization in support of tactical forces. The ASA organization will be tailored to meet the specific electronic environment posed by an enemy force, thus the organization depicted may vary. Specific functions of the various organizations will not be discussed in this manual; however, each echelon is designed to provide support within the area of interest of the supported command. Detailed information on capabilities of the ASA organizations may be obtained from the supporting ASA units.

a. A summary of listening capabilities organic to the division and ASA resources is shown in figure 2–2.

b. Although organic equipment compatible with some of the enemy electronic systems is authorized within the division, such equipment should be considered as complementary to, but not a subsitute for, ASA support, since its primary purpose is for the communications-electronics support of the division. Listening requires proficiency in the enemy's language, some technical skills, and coordination of the listening effort to preclude undesired duplication. When the necessary skills and language capability are available in the tactical unit and the decision is made to listen using organic resources, provisions must be made to expeditiously provide the information obtained to intelligence personnel to allow its integration with other information. Commanders must recognize that inexperienced personnel conducting listening operations are susceptible to enemy deception operations; thus, integration of information obtained with all other available data is extremely important. Except in unusual situations the attached or nearest ASA unit should be consulted prior to engaging in listening operations. The SIGINT support element/electronic warfare element (SEE/EWE) will assist the command in developing and using its organic listening capability to include provision of technical guidance and report formats.

Depend on supporting ASA units to fulfill most listening requirements. That's what they are there to do.

2-5. Requirements for Intelligence

As stated earlier, a commander will not have the resources to listen to all the communication and surveillance devices of the opposing enemy force. Therefore, priorities must be established consistent with the total listening capability available. Normally this is accomplished after the identification of the essential elements of information (EEI) and other intelligence requirements (OIR) of the command and a decision by the commander on the concept of operation for the mission. Once the information requirements of the command are determined, priorities for listening can be established.

CHAPTER 3

LOCATING

3–1. General

The location of enemy electronic emitters can be of significant value to the commander. The capability to locate electronic emitters exists in both friendly and enemy forces. The friendly capability to electronically locate enemy emitters is provided by the US Army Security Agency. The location of electronic emitters coordinated with fire is part of enemy doctrine, and commanders must be alert to this threat. The enemy-locating equipment is deployed to regimental level and targeted against friendly emitters within 35 kilometers of the FEBA. Since current doctrine in some countries is to direct artillery fire on the basis of electronic location information alone, commanders may expect to receive artillery fire based on location of their emitters within 10 to 15 kilometers of the FEBA.

3–2. Evaluation of Location Information

Locating information can provide locations, movement, dispositions, and targeting data. This information normally augments other intelligence held by the command; however, it is sometimes the most timely and accurate information available. The integration of listening and locating capabilities, structured to support command EEI and considered along with the traditional intelligence assets of photography, infrared sensors, SLAR, PW interrogration, and agent reports, can provide the commander with accurate tactical intelligence.

3–3. Location Information Characteristics

a. Emitter location can be accomplished from the ground or air. Ideally, the technique involves listening to the enemy emitter from at least three receivers deployed along a line and determing the location through intersection. Information received from locating enemy emitters is processed through the SIGINT support element/electronic warfare element (SSE/EWE).

b. Location capabilities include the acquisition of enemy radar as well as AM and FM emitters used by the enemy. The chart below generally depicts enemy frequencies for both communication and noncommunication equipment. Location of most enemy emitters, used for tactical purposes, from the ground requires that the position of location equipment provide line-of-sight to the enemy emitters. Aerial locating platforms complement the ground capability. These platforms normally operate behind the FEBA, are independent of terrain, extend line-of-sight, and can conduct surveillance over large areas.

c. Commanders should consider aerial location platforms as an extension of other aerial reconnaissance and surveillance assets.

3–4. Requirements for Intelligence

a. Depending on the echelon, some emitters are listened to and heard more frequently and established. It may not be possible or desirable to obtain the location of every emitter heard.

b. The commander, with the advice of his staff, must determine the priority for emitter location. This priority is stated in the EEI. The command listening and locating operations are thus guided by and responsive to the command EEI. Assistance in the establishment of priorities may be provided by the SSE/EWE.

c. In this regard, the commander should be aware that an emitter that is being monitored can be located as quickly as the operating frequency is known and a triangulation conducted. The priorities established by the commander and his staff are crucial to the proper use of available assets.

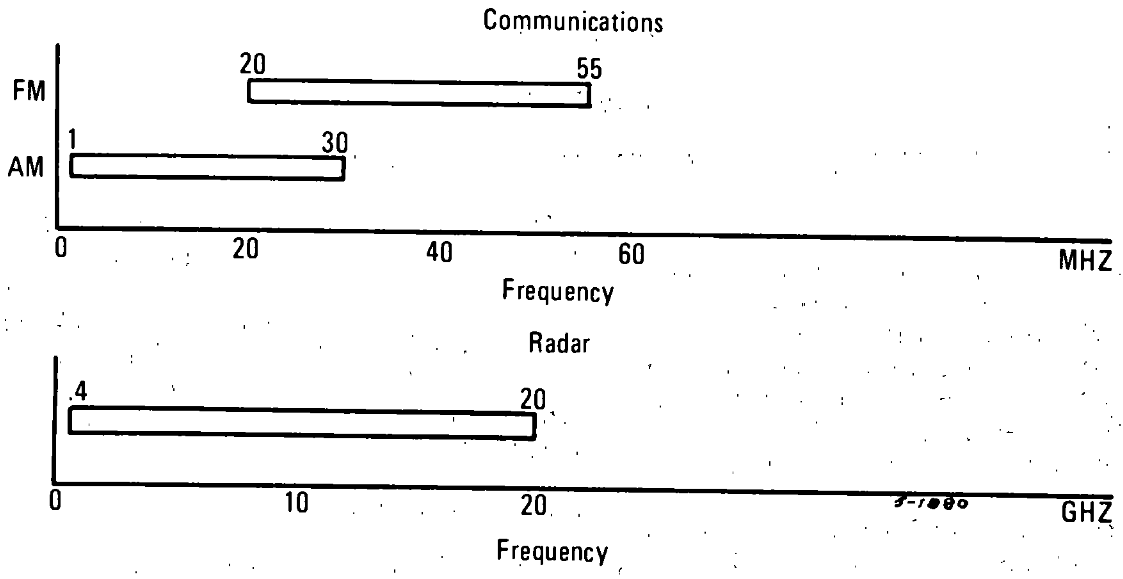

Figure 3–1. Enemy frequency usage.

CHAPTER 4

DISRUPTING

4-1. General

The enemy relies heavily on electronic systems to pass orders and information as well as to collect data. Regardless of the function of the enemy electronic system, the commander must contend with these enemy systems during all phases of the tactical operation. This chapter is an overview of electronic disruption on the battlefield. It is designed to provide basic data from which the commander and staff may begin a more detailed exploration into the possibilities of using the electronic environment to gain tactical advantage.

4-2. Disrupt Options

There are five options to be considered:

a. Destruction. From the standpoint of noncommunication emitters (e.g., radars), destruction is usually the best option available to the commander. Communication emitters (e.g., radios) should be destroyed when disruption of the enemy's command and control is more important than using an emitter as a source of intelligence.

b. Jamming. This option degrades receipt of the desired signal at the receiving station and applies to both communication and noncommunication systems. Some jamming signals are difficult to identify; thus radio or radar operators may believe they are experiencing equipment difficulty rather than jamming activity.

c. Imitative Deception. The input of false information into the enemy communication system using enemy radio procedure may be attempted in an effort to cause the enemy to react in a desired manner.

d. Manipulative Deception. The use of friendly communication and noncommunication systems to provide false information to enemy signal intelligence units is manipulation. Successful employment of this option causes the enemy to input false data into his intelligence analysis process.

e. No Action. This final option may be the proper solution when friendly listening efforts are gaining information of significant value to friendly operations from the enemy electronic system. A decision to disrupt such an enemy system might result in loss of the information. In these cases, the value of the information must be compared with the tactical advantage to be gained through disruption to determine which option is better. This is a commander's decision.

4-3. Application

In general, disruption options can be applied to any enemy system that receives an electronic signal. Some of the more vulnerable systems are:

a. Forward Air Controller Communications. Disruption of these communications seriously inhibits enemy tactical air reliability. When target information cannot be supplied, these aircraft generally must expend ordnance against targets that can be acquired visually. Imitation, as well as jamming, should be considered for use in this situation.

b. Enemy Navigational Aids and Radar Bombing Systems. Destruction of these systems is the obvious choice. However, if location data is inadequate or other factors preclude destruction of these systems, the use of jamming and employment of false navigational aids should be considered.

c. Surveillance or Weapon Drones. Jamming and deception can be employed against their control systems as well as the drone sensor system.

d. Enemy Communication Nets. Disruption of enemy communications may be achieved through destruction, jamming, or imitation.

e. Missile Systems. Enemy tactical missile systems are subject to effective disruption to the extent that they depend on communications and electromagnetic data links for performance of their functions.

f. Electronic Surveillance Systems. Ground-based devices consist primarily of radars, infrared detectors, and light-amplification and thermal-imaging devices. These devices may be jammed or deceived by friendly equipment having appropriate radiating characteristics.

4-4. Planning

Each of the commander's options discussed in paragraph 4-2 assumes that the enemy receiver or emitter can impact on friendly combat operations. The working definitions and the partial list of applications above will assist the commander in determining how best to degrade the enemy electronic capability. The three electronic options available (jam, imitate, manipulate) are discussed in more depth below to insure understanding.

a. Electronic Jamming. Technical planning for jamming operations includes consideration of numerous factors. Some important areas are:

(1) *Required data.* Data on the identification, technical characteristics, locations, and use of emitters and their associated receiver systems are continually updated and assembled into a priority listing in accordance with the current tactical situation by the SSE/EWE.

(2) *Variables.* The major variables to be considered include availability of jamming equipment, environmental factors, radiating power requirements, tactical environment, and possible enemy reaction.

(3) *Controls.* Frequencies to be jammed must be compared with the current restricted frequency list held by the SSE/EWE. This list contains specific frequencies that, if jammed, would interfere with friendly operations and/or affect the safety aspects of friendly nuclear or conventional weapons that employ electronic command or guidance systems. Should a restricted frequency be considered for jamming operations, permission must be obtained from the command that restricted the frequency before the jamming operations may commence. The command conducting jamming operations must have an effective ON/OFF control procedure that allows immediate starting and stopping of jamming activities. The command's ability to exercise this type of control must be assured prior to starting any disruption operations.

b. Imitation. Imitative operations are most likely to succeed when enemy signal security measures are poor and operators are undisciplined. Imitation is generally more successful at lower levels of command, due primarily to increasingly sophisticated communication systems and security procedures at the higher echelons. Captured enemy equipment should be used when available. Friendly linguists must be convincing, sound authentic, and be competent in the use of enemy terminology. The level of tactical activity impacts heavily on the success of imitation operations. Obviously, enemy operators are less likely to question a transmission in the "heat of battle" than in preparation for the attack. Commanders are authorized to conduct imitative operations provided the Army component commander has given prior approval. See FM 32-20 for detailed authorizations.

c. Manipulation. This technique can take two forms: alteration of emissions from existing units to limit the amount of information presented, and/or simulation of emissions from notional units to deceive the enemy. A successful manipulation operation requires that friendly electronic data be intercepted by enemy signal intelligence units and that the enemy believe the intercepted transmission. This type of operation is designed to influence the enemy estimate of the situation and must be consistent with terrain, disposition of troops, and the tactical situation. The information presented must be plausible to the enemy. The information must be calculated to cause the enemy to react in a definite manner; however, the outcome of the tactical operation must not depend entirely on the enemy reacting as anticipated. The commander may conduct manipulative operations any time on circuits that are wholly within his control. This action should be fully integrated with the commander's overall deception plan.

4-5. Planning Data

The success or failure of disruption operations rests on the immediate availability of pertinent electronic data on enemy units. Detailed technical data is generally available within the analytical sections of the division intelligence or ASA units; however, basic planning data should be available either in the all-source intelligence center of the G2 or the SSE/EWE in the TOC. This data should be posted on a map or overlay and accompanied with a data chart such as figure 4-1. This data is sufficient for the commander to begin consideration of the available disruption options.

As of (today)

Cross reference number	Unit/designator	Disruption possibilities	Friendly capability
1	91st Tk Regt Operations net control	Jam, imitate—comm procedures good; most vul when unit moving.	ASA DSU can jam—imitation possible during enemy off opns.
2	QVR-11 Radar (Norm assoc with 159 mm gun)	Jam—radar usually turned on 3 minutes before arty fire for warmup.	Destroy, jam—friendly jamming would most probably result in delay of or prevention of arty fire for assoc gun.
3	211st SIGINT Co	Manipulate—unit moves frequently thereby losing continuity on friendly units.	Organic equipment and personnel to establish false presence of friendly bn.
4	2d CAA Log Net	Jam—must be abn opn due to distance and line-of-sight frequencies used.	Asst from higher headquarters required.

Note. Fictitious data utilized on this sheet.

Figure 4-1. Example of enemy electronic vulnerability sheet.

CHAPTER 5

COMMAND AND STAFF RELATIONSHIPS AND COORDINATION

5-1. General

Responsibility for employing EW is a function of command. EW functions are assigned to the staff to enable the commander to discharge his responsibilities for planning and conducting EW operations. Formal EW mission planning normally does not originate below division level (except in the case of separate brigades); implementation of EW plans can extend to the lowest echelon having requisite resources. Whether or not a TOC is established by the commander, the functions of planning and executing EW operations are exercised as delineated in subsequent paragraphs.

5-2. Coordination

a. The use of EW requires close coordination between operations, intelligence, and C-E staff elements. Generally, a decision must be made concerning the relative value of the intelligence being derived from an enemy emitter versus the tactical value that could accrue from denying him use of the emitter through electronic or other action. This conflict of interest directly involves the G2 and G3, since a close relationship exists between EW and acquisition of intelligence from enemy electronic emissions. Thorough and continuous coordination between the G3 and the communications-electronics (C-E) officer is necessary to insure that EW, which is employed against an enemy threat, will not unacceptably degrade friendly C-E systems. Figure 5-1 depicts the flow of requirements and information within the staff elements having primary EW functions.

b. In the case of adjacent commands that are subordinate to the same immediate headquarters, little difficulty should be encountered in the routine handling of EW matters. There is an increased requirement for liaison and coordination where adjacent units are not subordinate to the same headquarters. Coordination in this situation equates to that which is encountered when a division of one corps desires to place fires in the area of an adjacent division that is under the command of a different corps. The presence of EW-oriented elements in each TOC lends assurance that whenever offensive electronic coordination problems develop, they can be resolved by specialists with mutual knowledge and understanding of the problem area.

5-3. The G3

a. General. The G3 has staff responsibility for the planning, coordination, and supervision of EW activities, except for intelligence aspects, and is the focal point for the conduct of these activities. The G3 provides direction to the EW effort and furnishes priorities and recommendations for EW organization, training, and operations. His principal assistant within the G3 section is the assistant G3 (EW), an electronic warfare staff officer (EWO), who is E-prefix qualified.

b. Responsibilities.

(1) *Organization.* The G3 is responsible for the identification, capabilities assessment, procurement, and allocation of organic and attached personnel and equipment required to perform assigned or planned EW missions in training or combat. To exercise this overall staff responsibility, he coordinates with direct and general support units having EW capabilities.

(2) *Training.* The G3 coordinates EW training to insure the attainment and maintenance of—

(*a*) A staff capability for planning and integrating EW in support of combat operations.

(*b*) The ability of operators of organic equipment resources to participate effectively in EW operations.

(3) *Operations.* the G3—

(*a*) Coordinates approved electronic warfare operations with higher, lower, and adjacent units to insure mission compatibility.

(*b*) Coordinates airborne electronic warfare operations with the fire support element (FSE), the tactical air support element (TASE), the airspace management element (AME), the G2, and C-E officer.

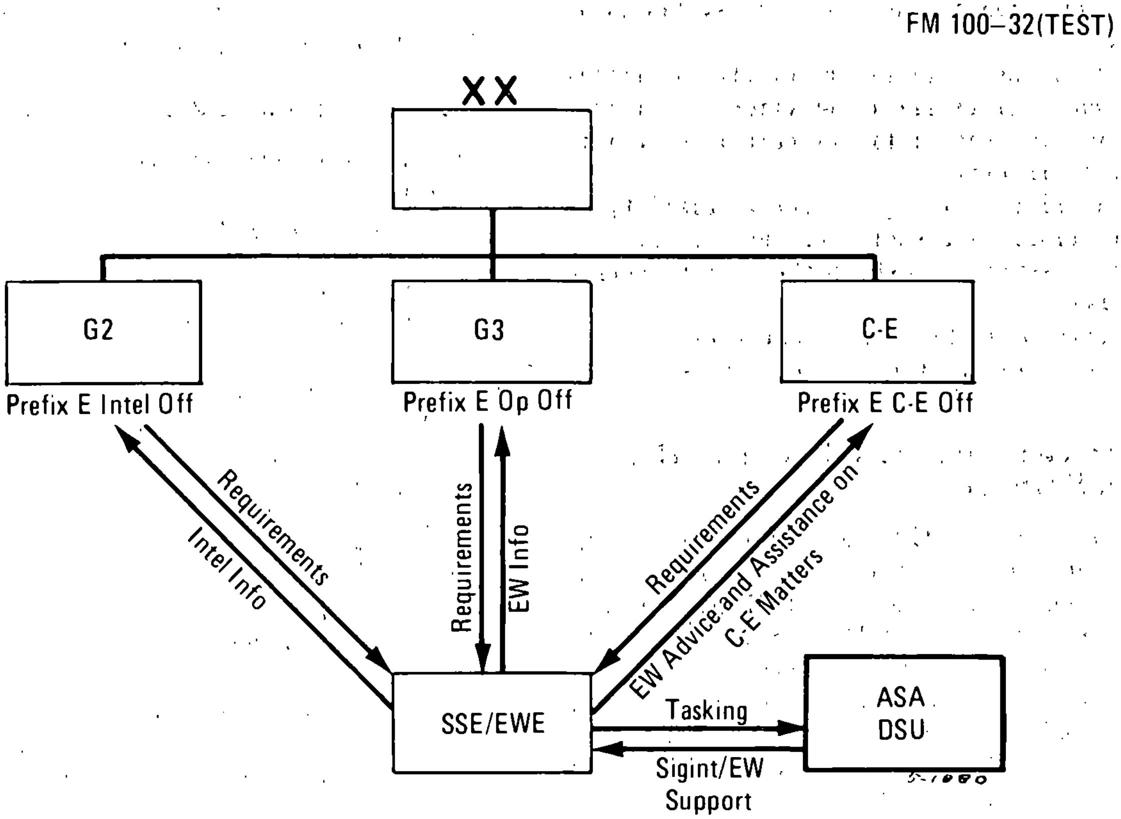

Figure 5–1. EW coordination.

(*c*) Tasks the assigned and attached EW units and other subordinate elements of the command through SSE/EWE.

(*d*) Is responsible for the integration of electronic deception into deception operations.

(*e*) In coordination with the G2, provides the FSE with data on enemy electronic emitter locations as a preplanning measure for their possible destruction.

5–4. The G2

a. General. The G2 advises the commander and his staff on the intelligence aspects of EW, including electronic deception operations conducted as a part of deception plans. The G2 is responsive to the G3's intelligence and information requirements for the planning and execution of electronic disruption actions and for targeting of the EW location systems of the supporting ASA unit.

b. EW Responsibilities. The G2 evaluates planned EW operations for intelligence implications, to include requirements for electronic information and intelligence support to EW. The G2 assists in the preparation of intelligence-related portions of the EW estimate of the situation. The G2 advises and makes recommendations to the commander on the risks and benefits of employing electronic warfare against specified targets. He recommends the use of these techniques against the enemy's signal intelligence and other electronic surveillance resources.

5–5. The G1

The G1's responsibilities for EW operations focus on requirements fpr organic personnel with linguistic skills to support imitative deception operations. The G1 maintains a list of linguistically-qualified personnel, indicating their degree of speech proficiency and mastery of dialects by type, and establishes procedures, in coordination with the G5, for the control and use of host country personnel with special linguistic qualifications.

5–6. The G4

The G4 coordinates logistic support for EW operations and the distribution of organic EW equipment and supplies, excluding cryptographic support which is the responsibility of the C-E officer.

5–7. The G5

The G5—

a. Advises the commander on EW requirements in psychological and counterpsychological operations.

b. Advises the commander and staff concerning the capabilities and employment of psychological operation units for support of electronic warfare operations.

c. Determines and reports the availability of local personnel, materiel, and facilities to support EW missions. Assists in their procurement and/or use.

d. Reports the effects of friendly and hostile electronic actions on the PSYOP program.

5–8. The Communications-Electronics (C-E Staff Officer

As a coordinator of the use of the electromagnetic spectrum for a wide array of communication-electronic resources, the C-E staff officer has numerous responsibilities relating to EW. Staff officers with whom he effects coordination on matters of common interest are the G3 and the G2. Specific coordination responsibilities are:

a. Advise the G3 on the status and capability of tactical C-E equipment suitable for EW use.

b. Maintain listing of RESTRICTED frequencies, and coordinate with the SSE/EWE concerning their impact on planned and ongoing operations.

c. Coordinate electronic deception plans and operations in which assigned C-E resources participate.

d. Assist in the preparation of EW plans and annexes.

e. Coordinate frequency allocation, assignment, and use within the command.

f. Coordinate measures to reduce electronic interference.

g. Prepare the signal portion of the training program, including therein all factors that affect the effective use of friendly C-E equipment in a hostile electromagnetic environment, namely, electromagnetic compatibility, electronic counter-countermeasures and signal security, and manipulative electronic deception.

5–9. The Air Defense Officer

The air defense officer coordinates air defense EW operations with the EWO, the C-E staff officer, and the airspace management element (AME) of the TOC. This includes—

a. Coordinating airspace to preclude interference with airborne EW missions.

b. Coordinating and advising on location and employment of air defense weapons to insure that jamming operations do not conflict with established frequency constraints.

5–10. The Electronic Warfare Officer

The EWO is an assistant G3, prefix-E qualified, who assists the G3 in the carrying out of his staff responsibilities by performing the following tasks and functions:

a. Planning. He determines the capabilities and limitations of available EW resources and makes recommendations for tasking in accordance with capabilities. This includes preplanned EW support and the tasking of EW resources for deception operations. His evaluations include assessments for the commander and the G3 of the probable effectiveness of preplanned electronic offensive operations. The EWO prepares the EW estimate and the EW annexes for operation plans and orders.

b. Coordination. The EWO coordinates ground and air EW operations with the AME to insure conformity with ground and air operations. He is the principal coordinator with supporting and subordinate units in meeting EW requirements and establishing priorities for EW support. He coordinates with and assists the C-E officer in the preparation of plans and recommendations for electronic counter-countermeasures and manipulative electronic deception. He also coordinates with the G2 on cryptologic support for manipulative deception. He assists in the preparation of plans for communications security for EW command, control. and reporting.

5–11. The SIGINT Support Element/Electronic Warfare Element (SSE/EWE) of the TOC

The tactical commander must receive continuous advice on EW operations. To coordinate and control tactical operations, the commanders at corps and division normally establish a TOC. The EW focal point within the TOC is the SSE/EWE. SSE/EWE personnel for the TOC are provided by the ASA direct support unit. The personnel within the SSE/EWE—

a. Maintain information on status and capabilities of assigned, attached, or supporting EW units and organic devices. This information will include disposition of units, current missions and status, capabilities, and limitations. The SSE/EWE maintains information on units operating in areas other than those for which it has responsibility, to include information provided by the EWO concerning operations of counterpart organizations of other Services.

b. Maintain a continuous estimate of the EW situation. The SSE/EWE maintains constant surveillance over EW activities and evaluates pertinent information that influence the current situation. Significant facets of the function include consideration of the C-E order of battle. Significant enemy information that may require prompt response is passed directly to the G3 element through the SSE/EWE. The G3 element, in turn, provides the SSE/EWE with information that assists in its support activities.

c. Translate requirements for information and data into orders and requests to subordinate and supporting SSE/EWE's.

d. Coordinate friendly EW operations. Make recommendations for tasking of EW units. Assist the G3 in resolving problems relating to EW operations that may conflict with operations of subordinate and supporting commands and units. Of particular interest are those problems arising from organic or nonorganic signal activities wherein their performance is susceptible to interference from friendly or enemy EW operations. In this respect, the SSE/EWE coordinates with the C-E officer to implement action required for the maintenance of lists of RESTRICTED frequencies and for the resolution of meaconing, intrusion, jamming, and interference (MIJI) reports.

e. Interpret and advise on enemy EW operations. Interpret data in relation to the current situation to assist in reporting friendly C-E vulnerabilities.

f. Evaluate the effectiveness of EW operations.

5–12. Reporting

EW reporting procedures are under the staff supervision of the command's ACofS, G3, except for reports on intelligence support. He is assisted by the SSE/EWE in extracting essential data for both evaluation purposes and the maintenance of a data base. Reports are made by assigned and attached units, as well as EW support units, to the TOC by the most expeditious means. The information is verified and coordinated with other staff elements and disseminated to higher, adjacent, and subordinate units as required, with emphasis on rapid dissemination to the lowest possible level to insure no loss of timely or perishable information.

CHAPTER 6

EXPLOITING ENEMY VULNERABILITIES

6–1. General

The ability to degrade enemy electronic systems provides the commander the opportunity to favorably influence the combat power ratio. Effective friendly use of electronic warfare will result in confusion, frustration, and loss of initiative on the part of the enemy force. The enemy's electronic weaknesses or vulnerabilities must be identified and attacked just as decisively as any other weakness. The use of electronic warfare to exploit enemy communications-electronics systems adds another dimension to combat.

6–2. Enemy Vulnerability

Listening and locating provide the bases for decisionmaking applicable to disruption. Enemy vulnerability to electronic warfare is determined basically by three variables: the level of enemy dependence on communication and noncommunication means and his degree of technical sophistication; state of enemy electronic warfare/signal security training and awareness; and enemy equipment design characteristics and limitations.

a. Listening. Exploitation is initiated through listening. Listening develops the information required to support the locate-and-disrupt functions. When listening is unable to provide the required information, neither location nor disruption can be effectively performed. The listening function is designed to satisfy the command's essential elements of information (EEI) and other intelligence requirements (OIR). Thus, listening exploits enemy radio transmissions intended for enemy use only by receiving the energy radiated by noncommunication devices, i.e., radars, navigational aids, heat sources, engines (spark plugs and coils), etc., and collects information that assists in satisfying the command's intelligence requirements. Thus, current and ongoing operations can be better adjusted to retain or seize the initiative based on timely exposure of the enemy situation as portrayed by his electronic systems. The communications-electronics officer derives significant input to the planning of friendly communication through knowledge of the enemy's use of available frequencies.

b. Locating. The locating function exploits enemy electronic emissions and provides significant information relevant to enemy deployment and changes to that deployment. Evaluation of location data concerning enemy emitters will provide a picture or footprint of the enemy electronic order of battle and unit and weapon system deployment. For example, the location of specific radars that are associated with particular enemy missile systems will serve as an indication of the presence of that missile system. Analysis of location information requires a basic knowledge of enemy practices and normal deployment relationships. Habitual remoting of antennas and use of radars or radios to achieve deception or to offer a false footprint are possible enemy practices that must be identified. Location data that identifies enemy activity or lack thereof is of great significance in operational planning and targeting functions.

c. Disruption. The disruption function should be viewed as positive action taken to negate the enemy use of electronic systems. The disruption technique selected dictates the degree of friendly technical sophistication, equipment, and personnel resources required to accomplish this function. Except for deception operations that may be accomplished with information collection, each of the electronic alternatives is mutually exclusive of the other.

6–3. Decisionmaking Considerations

The various alternatives available to the commander differ in impact on the enemy electronic systems, probable enemy reaction, and benefit to the commander. These factors must be recognized if appropriate options are to be considered and effects optimized.

a. Destruction. By its nature, destruction denies the enemy use of a portion of his communication and/or noncommunication means. Such operations require only that the enemy be located and that means be available for his destruction.

Maximum effectiveness is achieved through selective destruction operations that target on key enemy electronic systems, i.e., command and control, and acquisition and guidance systems. Noncommunication emitters should be considered for destruction as a matter of course. These devices may also be jammed or deceived; however, such activity will normally be included in tactical deception operations as discussed in chapter 7. Destruction of communication devices is also desirable; however, jamming and deception operations should also receive consideration. The most difficult aspect of the destruction decision results from the location accuracy combined with such enemy practices as remoting antennas. Since the location data pertains only to the radiating antenna, one must recognize that the unit the antenna represents may be located over some larger area in the general vicinity of the antenna.

b. Jamming. Jamming operations offer an effective method of temporarily interrupting communication activities. Jamming operations require location data to be effective; however, the location accuracy need not be as precise as it must be for destruction. Proper planning of jamming operations recognizes the criticality of timing to gain the greatest benefit from the temporary interruption of the communication system. The time length of the interruption will vary based on the level of enemy training, his ability to change to an alternate means of communications, additional frequencies available, and the flexibility of his equipment, e.g., higher power setting and frequency detuning capabilities. Jamming operations are highly dependent on the distance between the jamming equipment and the receiver to be jammed. The power available to ground-based jamming equipment is rapidly depleted by terrain and distance. However, airborne jammers are effective at significantly greater ranges, since the airborne platform can more readily gain line-of-sight to the intended receiver and the effects of terrain become almost negligible.

c. Deception. Exploitation of enemy vulnerabilities through deception operations relies heavily on data developed through listening operations. Depending on the form of deception to be employed, such operations may pose a threat to long-term information gathering activities.

(1) Where the intent is to deceive the enemy regarding our actions, the threat to the listening effort is minimal. To conduct such deception the intelligence base must provide knowledge of enemy communication and noncommunication intercept capabilities. This activity is discussed in chapter 7.

(2) Where the intention is to disrupt enemy communications through the introduction of false information into his communication systems, the risks to the listening effort must be considered. This type of deception, if discovered by the enemy, will provide clear evidence concerning the friendly listening effort. Thus, the enemy may be expected to improve his communication security and procedures to deny friendly listening success. The type of communication deception available for introduction into the enemy's communication systems ranges from enemy cryptographic systems to very simple, plain language. The more sophisticated efforts are directed at the enemy commander and are designed to cause him to make decisions based on false information, while the simpler efforts are designed to harass the enemy radio operator and impede his mission accomplishment.

6–4. Authorities and Restrictions

Inherent in the conduct of electronic disruption activities are requirements designed not only to preclude undue interference with friendly communications-electronics but also to deny disclosure of friendly EW capabilities to enemy or potential enemy forces. Full prior knowledge of friendly EW capabilities would provide the requisite information to develop and plan appropriate counteractions. For both training and combat situations these authorities and restrictions are identified in the following publications and by appropriate command supplements.

a. AR 105–86, *Performing Electronic Countermeasures in the United States and Canada.*

b. (C) AR 105–87, *Electronic Warfare* (U).

c. (S) AR 380–35, *Security, Use, and Dissemination of Communications Intelligence* (*COMINT*) (U).

d. (S) AR 381–3, *Signal Intelligence* (*SIGINT*) (U).

e. (C) FM 32–20, *Electronic Warfare* (U).

CHAPTER 7

DECEIVING THE ENEMY

7–1. General

a. A commander's proficiency in executing operational plans without the enemy being aware of their intent may well determine success or failure on the battlefield. The use of electronic warfare will play an important part in the commander's ability to deceive the enemy regarding the execution of friendly operations. This chapter will discuss the use of electronic warfare to support deception operations.

b. The ability to achieve surprise—the primary purpose of a deception plan—is becoming increasingly difficult. Advanced technology and equipment sophistication coupled with an increase in the number of personnel have significantly increased the profile of a military force. The many advantages gained from using the new equipment can be significantly reduced or eliminated unless careful consideration is given to its susceptibility to enemy detection devices.

c. Improvement of enemy target acquisition and tactical intelligence means for gathering visual, sound, and electronic information reduces the probability of achieving surprise. The enemy's proficiency in air and land reconnaissance will insure that very little of the battlefield will be exempt from detailed examination by black-and-white film, color film, camouflage-detecting film, infrared film, and low light-level television, as well as an ever-growing number of night-observation devices. Besides better visual and photographic detection methods, the enemy possesses an ever-increasing sound and smell detection capability.

d. A significant vulnerability of friendly units on the modern battlefield will be the enemy's ability to locate and listen to our electronic emitters. As previously mentioned, radios, radars, generators, spark plugs, automatic data processors, ground and air vehicle movement, occupied tents, cooking stoves, and immersion heaters are but a few of the items that can be located by enemy detection devices. The enemy's capability to listen provides him information to associate with other intelligence-gathering sources and emitter locations to determine friendly order of battle and possible intentions.

e. Commanders can use these capabilities to assist in deceiving enemy intelligence about friendly activity. Hiding our intentions, time of attack, location of main attack, etc., while revealing false information of the same type are possibilities available to the commander.

f. Commanders can utilize electronic deception in conjunction with other techniques to enhance the probability of achieving surprise.

7–2. Purpose

a. The purpose of a deception operation is basically to display the false and conceal the real. Operation security includes those measures designed to provide security to a plan, operation, or activity. It includes special measures taken to shield the real plan, operation, or activity as well as to intensify normal security and passive defense measure. Deception is used in conjunction with security activities to mislead an enemy by manipulating, distorting, or falsifying information to induce him to react in a manner prejudicial to his own interest.

b. Tactical military deception will normally have a limited, well-defined mission; be local in character; and be sustained over a relatively short period of time.

c. Electromagnetic deception is used to suppress, control, alter, or simulate electromagnetic radiations associated with friendly systems. When successful, it denies an enemy a source of knowledge as to the location of these combat elements or misleads him as to their capabilities and intentions. Electromagnetic deception techniques include emission control, electronic camouflage, and electronic deception used to assist friendly units to display the false and conceal the real.

7–3. Target

The enemy commander is the target for all deception operations. The way the enemy commander reacts will determine the success of our efforts. Our deception objective is the desired reaction by the enemy commander. The deception story is the intelligence estimate that the friendly force desires the enemy to develop.

7–4. Commander's Considerations

a. Successful deception depends on the ability of the deceiver to predict the enemy's probable reaction. Proper assessment of the enemy's probable reaction requires a thorough understanding of the enemy's culture, his psychology as it applies to war, and his military system. The enemy's command organization must be understood to determine at what levels decisions are to be made and, consequently, who must be deceived. The enemy's intelligence system must be carefully evaluated as one of the vehicles carrying the deception story to the enemy commander. The enemy commander's personality is of paramount concern in evaluating the means and methods to be used in deceiving him.

b. Adequate time must be allowed for the enemy to react to the friendly deception plan. Time must be allowed for him to collect the information, to analyze the friendly pattern of activities, and to react in a detrimental manner. The planning and initiation of the deception operation must be carefully timed to permit the enemy to react when desired.

c. Consideration must be given to how long a deception operation must remain in effect. Success may be achieved in several hours, or it may require several days. Ongoing deception operations should be planned to facilitate future operations.

d. The security applied to a deception plan is critical to insure the success of the operation. Information concerning the plan should be disseminated on a strict need-to-know basis. It is imperative that no suggestion of deception be conveyed to the enemy that could compromise the plan. Care must be taken to insure that all involved personnel fully understand the need for security, realism, and enthusiastic participation in the deception operation.

e. Tactical deception measures must be in consonance with past and future operations. This basic consideration, therefore, requires a carefully planned and executed "fadeout" phase for deception operations.

f. Deception may produce a reaction contrary to the planners' expectations. The tactical plan must be flexible enough to exploit unexpected successes or to protect against unexpected failures as a result of the deception plan.

g. Realism cannot be overemphasized. Unless the situation portrayed is reasonable and within friendly capabilities, it has little chance of causing the enemy to react. The enemy employs several means to gather intelligence, so the plan must include deception techniques against multiple collection capabilities.

h. Deception cannot be achieved by following a rigid pattern. Patterns are determined and developed by making the most of ingenuity and available resources. The effectiveness of tactical deception depends more on the variety of the techniques used in its application than on the number of times employed. Repeated or stereotyped employment of a particular method or means will quickly terminate its usefulness unless this repeated employment is itself intended as a method of deception.

i. The enemy's knowledge of friendly tactical doctrine can prove to be an asset to deception planners. Stereotyped operations make plausible and realistic deception stories. This situation also provides an excellent environment for innovative imagination in the development of methods to conceal our real intentions and reveal the false.

j. Deception planning should be conducted simultaneously with normal command and staff planning procedures. This relationship is depicted in figure 7–1.

7–5. Electronic Warfare Support to Tactical Deception

a. Deception operations inherently require electronic warfare support. Careful integration of electronic deception with the deception story is critical to the successful attainment of friendly deception objectives.

b. Manipulative and imitative electronic deception are used in support of the deception plan. Staff planning considerations are:

(1) Imitative electronic deception planning should include:

(*a*) *State of enemy signal security.* Imitative electronic deception is most likely to succeed when enemy signal security measures are unsophisticated or electronic equipment operators are lax and undisciplined. The state of signal security generally decreases with each echelon of command, creating more opportunities for deception at lower echelons. Imitative deception at higher echelons is difficult to achieve primarily due to the use of sophisticated cryptographic systems. When accomplished, it will probably be successful for brief periods.

(*b*) *Available resources.* Electronic equip-

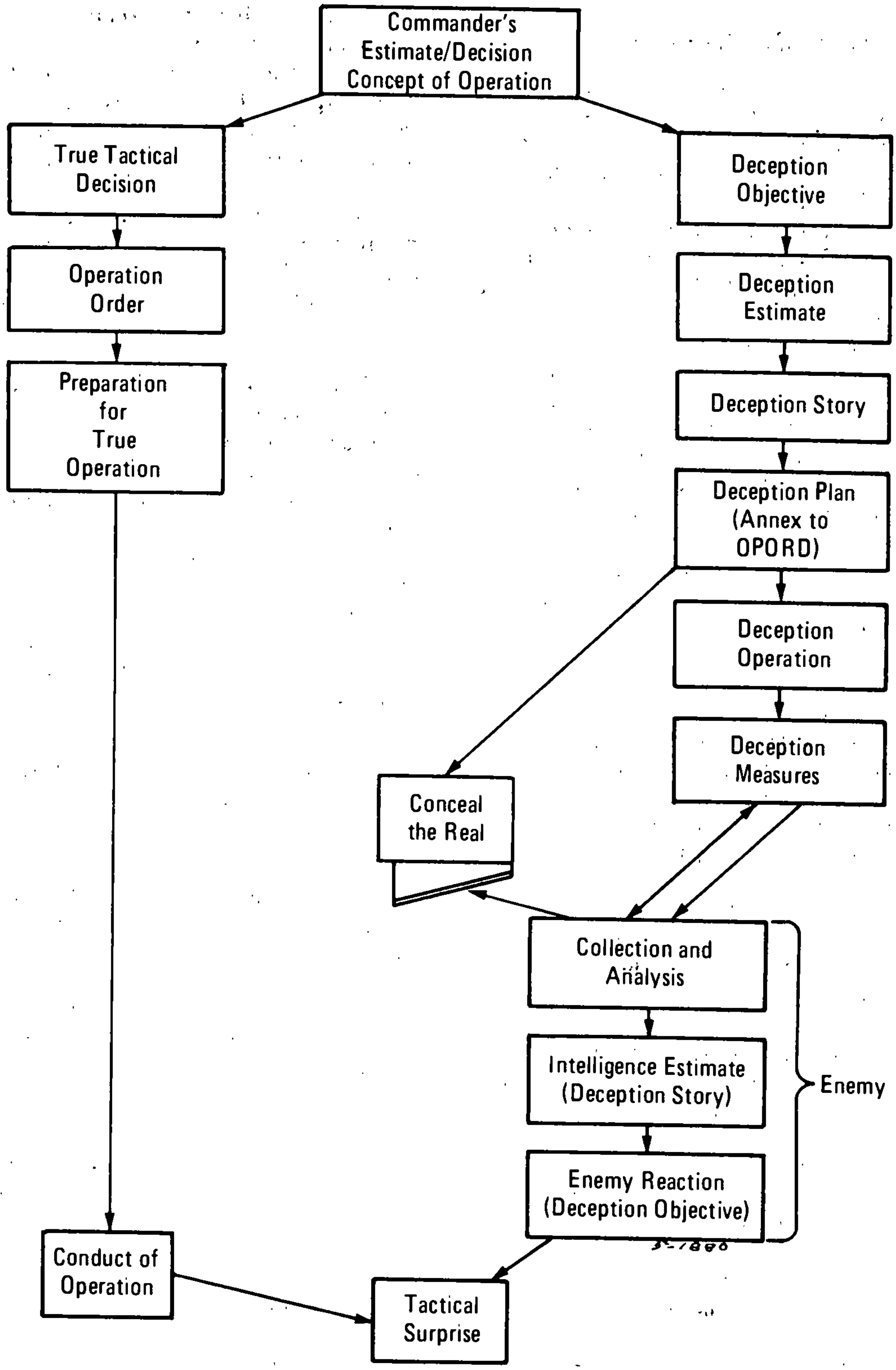

Figure 7–1. Command and staff.

ment capable of convincingly duplicating the functions of target enemy equipment should be available for use in the deception operation. Where possible, captured enemy equipment should be used to further insure that the signals are authentic. A proficient linguistic capability is required if voice is used, and an operator capable of convincingly imitating the transmitting style of enemy operators is required when CW manual Morse is used

(*c*) *Tactical environment.* Consideration should be given to a number of factors existing in the tactical environment that affect technical and doctrinal aspects of imitative electronic deception. Weather, terrain, and tactical deployments that degrade the functioning of enemy electronic equipment will increase the opportunities for deception and influence the selection of deception targets. Level of combat action and type of tactical operation being conducted determine, to a considerable extent, the possibilities for electronic deception and the method used to achieve it.

(2) Manipulative electronic deception planning includes:

(*a*) *Enemy intelligence capabilities.* Enemy signal intelligence and collection elements offer the primary means for delivering the manipulative electronic deception story to the enemy commander. These elements must be capable of collecting the deceptive information presented but not capable of immediately determining that such information is false. The deception must be presented in sufficient detail to be convincing to enemy intelligence analysts. For example, when technical considerations prevent enemy intercept of lower echelon units, it might be necessary to duplicate only those emitters used by a battalion to communicate with a higher headquarters to present a notional battalion. Conversely, portraying a notional battalion to enemy intelligence elements capable of intercepting all electronic emissions within the national battalion's area of operation would require duplication of all nets normally used by a deployed battalion. While electronic deception is aimed at enemy signal intelligence elements, planning should anticipate enemy use of information derived from other sources to confirm or deny his signal intelligence. Optimum manipulative electronic deception is achieved when it is part of an overall deception plan, and extensive coordination with all other elements of the command involved in the deception is achieved.

(*b*) *Enemy intelligence estimates.* In conducting deception operations it is less important to base planning on what the "truth" is concerning friendly forces than on what the enemy thinks that "truth" to be. It is, therefore, essential that a firm knowledge of the enemy's intelligence methodology be obtained and studied prior to initiation of planning.

(*c*) *The operational environment.* Planning should insure that the deception is plausible when compared to the tactical situation. For example, it must be logical for notional units to have arrived at their locations without being detected previously by enemy intelligence, or their arrival must be time-phased to simulate the electronic pattern presented by an actual move of such units. Complexity and resource requirements tend to limit the practical scope of using such deception at lower command echelons. In instances where the ground and air situation prevents or severely inhibits enemy reconnaissance and surveillance activities, many opportunities will exist for manipulative deception with limited resources. However, when the situation is reversed, fewer manipulative deception opportunities will exist, and plans usually must be limited to those of very short duration that which can be supported by available resources.

(*d*) *Enemy reaction.* While the deception plan is aimed at causing the enemy to react in a manner advantageous to friendly forces, the outcome of the supported operation must not depend entirely on enemy reaction being as anticipated. Deception can be a valuable adjunct to combat power, or it may prevent disclosure of a weakness; but electronic deception plans that do not at least consider enemy reactions other than those desired are hazardous. Nevertheless, the plan must be calculated to cause the enemy to react in a definite manner. A poorly presented deception story may trigger a reaction more adverse than helpful to friendly forces. For example, the simulation of an overwhelming numerical superiority may not convince an enemy to withdraw as intended but could provoke a preemptive nuclear attack instead.

(*e*) *Security.* The planner should make necessary security arrangements to prevent compromise of the deception plan. All elements of the command, including those directly participating in the deception effort, should remain unaware of the plan unless its execution requires such knowledge. Security measures contribute to the realistic appearance of the deception as well as prevention of compromise to enemy forces.

(*f*) *Restrictions.* Manipulative electronic deception may be conducted at any time using systems over which the commander has control. Manipulation of systems not totally within the commander's control must be coordinated with the appropriate headquarters. Consequently, commanders at all levels should carefully consider all aspects, to include prossible disruption of friendly communications, before initiation of such operations.

7–6. Ideas for Commanders

a. Consider the use of planned communication security leaks. Perhaps, while flying over an area, one could criticize a commander for poor use of camouflage in one of the decoy areas. This, accompanied by corrective action in the decoy area, provides rather strong confirmation of the realism of that installation.

b. At critical times, consider having all nets except the command net shut down. Command nets may have separate transmitters and receivers allowing transmission on one frequency and reception on another. Call signs and new operators should be changed at random.

c. Radio transmission time could be reduced while passing routine traffic. Provide the radio operators with tape recorders. Have the routine messages taped; pass the message at a faster speed. The recipient of the message records the message on tape recorders and plays it back at a normal speed.

d. Probably the primary source of enemy information concerning tactical operations is radio communications. This provides a tremendous opportunity for the use of deception in communication activities. One means would be to insure radio operator chatter when activities are minimal, passing false information concerning movements, operations, or logistic problems.

e. If you find that the presence of countermortar radars act as a deterrent to mortar attack, establish decoy radar positions to show a greater capability. Using the method described above, a system of dummy positions can be established on previously used positions. "Credibility" can be improved by periodically rotating actual countermortar radars into these positions for short periods.

7–7. Example—Notional Order of Battle and Intentions

Figure 7–2 portrays the real friendly situation and intentions for a main attack in the west to secure a deep division objective. Also depicted is the deception story for a main attack in the east with a supporting attack in the west. Shown are some of the electronic support measures that can help to sell the deception story.

7–8. Examples—Stereotyped Habits That Negate Electronic Deception Operations

a. Dummy headquarters, simulated units and supply depots, etc., set up without considering the electronic signature that goes with them.

b. Planning and coordination over the radio prior to an attack causes an increased traffic pattern that indicates an impending operation.

c. Units concealed, camouflaged, and restricted from moving; yet their radio nets are allowed to remain operational.

d. Patterns of vehicle reconnaissance and movement are made to deceive the enemy visually, but reports by these units never appear to enemy EW listeners.

e. Artillery fire missions conducted on notional objectives with out the normal radio communication in the conduct of fire, i.e., from the forward observer to the fire direction center, etc.

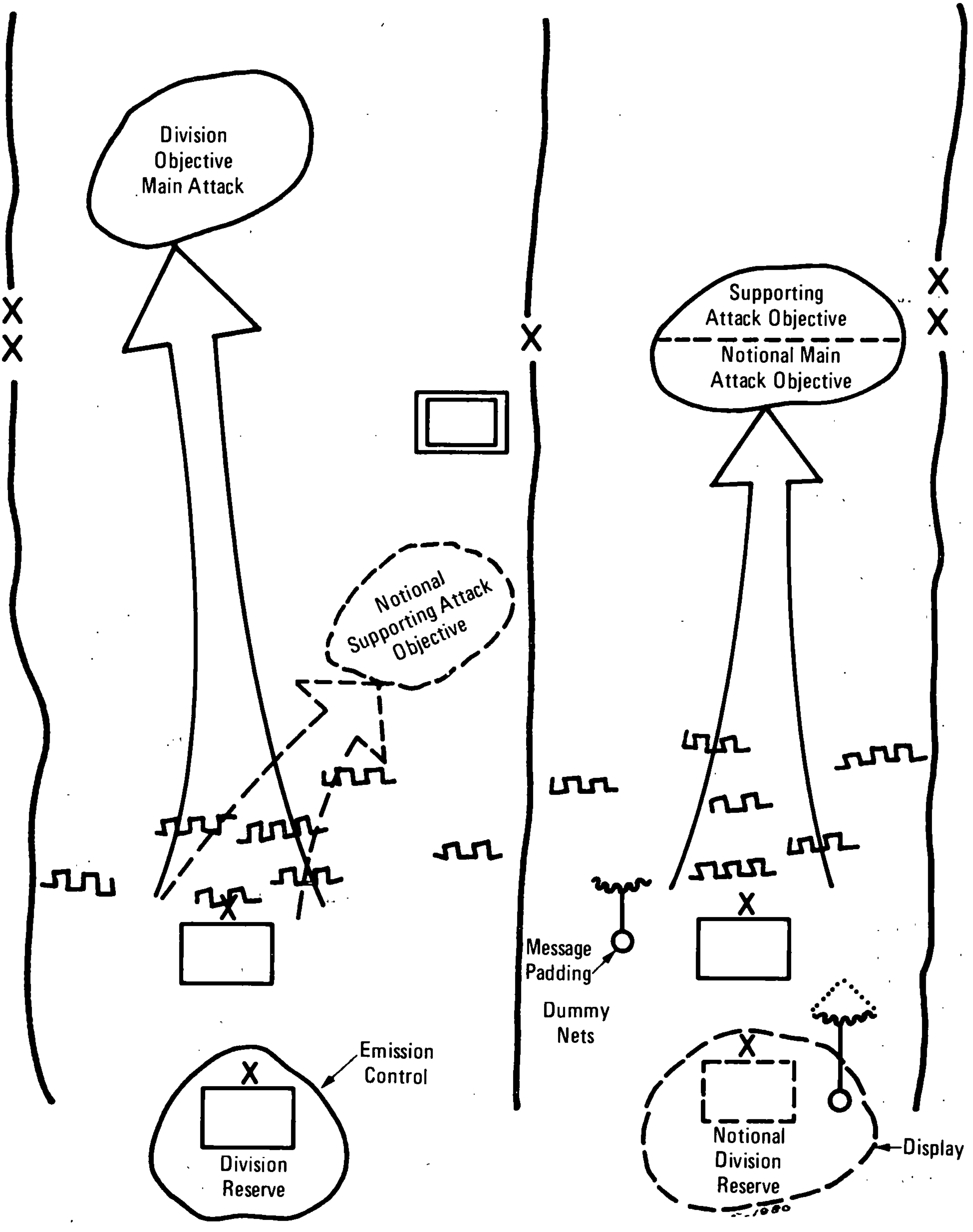

Figure 7–2. Notional order of battle sketch.

CHAPTER 8

REDUCING FRIENDLY VULNERABILITIES

8–1. General

Units must counter the threat posed to friendly forces by enemy listening, locating, and disruptive activities. If the enemy can hear the signal, he can also locate and possible disrupt friendly communications and operations. The action available to the commander to reduce these vulnerabilities is to give command emphasis to the basic elements of security. Effective security does not require a wealth of resources, a great deal of time, or an inordinate amount of special training to implement. Instead, it involves discipline and command interest in the basic application of easily understood and easily implemented actions. Countering the enemy EW threat requires command attention and, when appropriate, command action. This chapter stresses those mandatory techniques designed to reduce friendly vulnerability.

a. An indication of friendly communication vulnerability is the distance forward of the FEBA that tactical radio signals are detectable (fig 8–1). The large number of emitters on the battlefield have provided the enemy with unlimited opportunities. Not only radios but other electronic items emit energy that is detectable. With proper equipment, power generators, spark plugs of vehicles, automatic data processors, and electrical tools are detectable at great ranges. Heat and infrared energy emitted by occupied tents and positions, cooking stoves, immersion heaters, and hot engines provide signals for exploitation. However, of primary interest to the enemy are friendly communication and noncommunication systems. Listening—undetected—may be more valuable than the destruction of friendly emitters; the enemy has that option. Friendly communications are vulnerable, and the enemy will exploit EW to the fullest extent. The enemy threat is always present and must never be forgotten.

b. To minimize enemy exploitation, the commander must enforce a strict plan for communication and operational security. The commander must insure that communication personnel plan, install, and operate systems properly. Command guidance plays an important role in determining the overall communication requirements and friendly vulnerability.

8–2. Planning

a. The planning phase is initiated when communication requirements are identified, and radio nets and systems are organized.

b. Once communication nets and systems have been organized, appropriate frequencies and call signs must be assigned for operation. These tasks require a thorough understanding of radio frequency compatibility. Furthermore, the effectiveness of these assignment tasks and activities greatly reflects the degree of security obtainable at the organizational level. The following management techniques relative to frequency and call sign assignments are mandatory for successful operations.

(1) The allocation of frequencies for use within the division must be coordinated to insure compatibility with adjacent and other theater units. This task is normally accomplished prior to issuing frequency lists—an allocation—to the division.

(2) Assignment and changes of frequencies and call signs should be accomplished in a manner intended to deny the enemy information regarding identification and description of tactical units. Call sign and frequency assignments must be random and changed frequently. Security absolutely requires that this be done. It doesn't take the enemy long to determine that a particular call sign belongs to a specific unit. This can be accomplished through inadvertent disclosures by friendly units or through the enemy's transmission-intercept analysis efforts. The longer an assignment remains unchanged, the greater the chance of compromise. Retention of the same frequency over a period of time improves the enemy's capability to search, locate, and intercept friendly transmissions.

(3) The frequency of changes will depend to a great extent on the nature of friendly operations. In a static, garrison-type situation, assign-

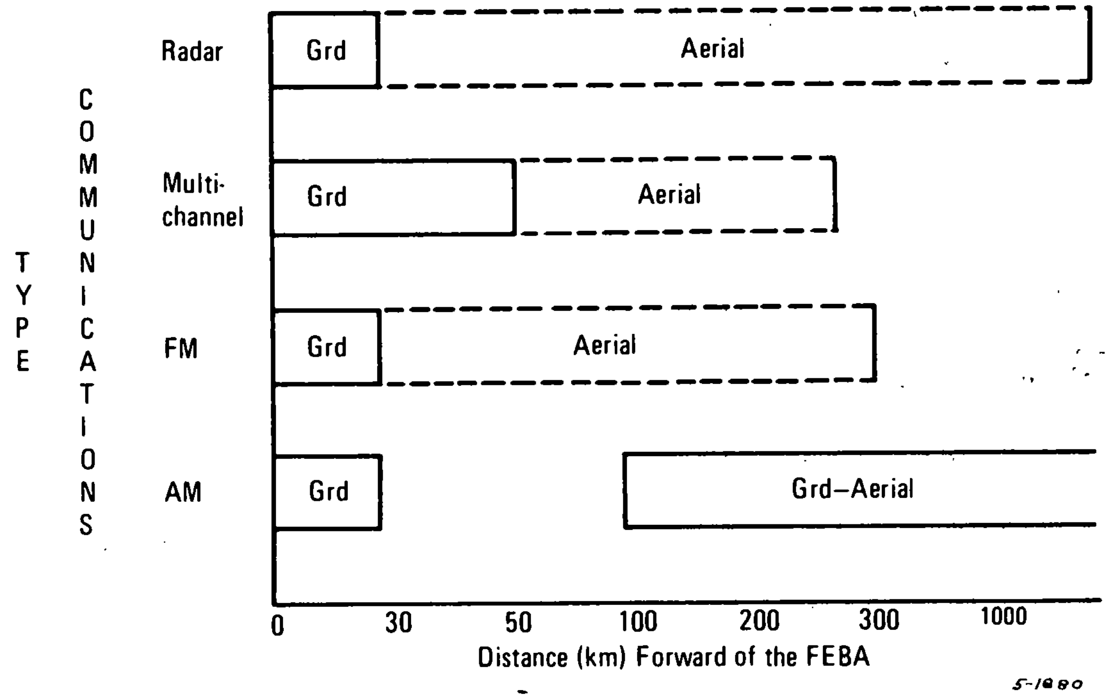

Figure 8–1. Friendly signal range.

ments should probably be changed daily. In a highly mobile situation, such as an exploitation or in the pursuit, tactical considerations may dictate that call signs and frequencies be changed four or more times daily. Changing calls and frequencies does require a certain degree of effort to accomplish; however, practice leads to proficiency. If identities of friendly units are to be afforded any degree of protection, and if intelligence information is to be denied the enemy, the required effort must be expended. The important point to remember is that changes must be made as frequently as the situation demands. The greater the frequency of change, the less likely the enemy will exploit friendly systems.

(4) Uniformity of call signs, in appearance and construction, within major tactical commands is imperative. Differences in call signs among nets or units as well as personalized calls produce command uniqueness and allow identification by the enemy.

(5) The designation of letter-number suffixes to a unit's basic all sign must be on a random basis. The habit of using 6, 3, 10, and 4 to represent the unit commander, operations officer, communications officer, and logistics officer respectively, negates the security inherent in the assignment technique. Patterns may also appear among suffix assignments of similar units.

(6) The dissemination of radio frequency assignments in the form of C-E operation instructions (CEOI) must be protected. Call signs and frequency assignment documents are normally classified CONFIDENTIAL to protect the compiled information; individual assignments must be classified on their own merits depending on the degree of sensitivity. Assignments that constitute a portion of a conscientiously applied plan for changing frequencies and call signs must be classified. Additionally, security is required to protect the fact that changes are occurring or planned. Likewise, the association of planned assignments with current ones must be avoided.

(7) Implementing instructions must be protected and prearranged. An index reflecting the current or planned use of CEOI items of information is published to insure understanding. If a frequency change must be made by radio, the most secure means available should be employed for notification. Unpredictable and undetectable changes increase friendly operational security. When the specific operating frequencies are not known, the enemy is forced to conduct listening operations over a wide range of intercept possibilities. A random change in operating frequen-

cies greatly compounds the search problem. For example, if an enemy listening unit detects a friendly emitter just prior to shutdown, so that complete signal analysis and accurate locating information are not achieved, a lengthy frustrating period of time might be lost while closely searching the region of that specific net. Additionally, the intergration of periods of radio or listening silence during these frequency-changing operations and the switching of operators increases the enemy's frustration. The shuffling of a limited number of available frequencies among the same nets on a prearranged, periodic, and announced schedule, usually on the first of the month, negates the security intended to allow a false sense of protection to exist.

(8) Additional protection is afforded the assignments by the publication of separate communication instructions. A unit's C-E signal instructions (CESI) explain the use of information contained in the CEOI. An explanation of net operations and instructions regarding authentication, codes, and emergency communications facilitate more effective use and provide greater security for the frequency assignments.

(9) Additional assignments must be readily available for use in event of a compromise of current assignments. Reserve editions (extracts) of the CEOI are prepared in advance to facilitate rapid replacement. Normally, a second edition (extract) of the CEOI will be distributed to all units to which the current one is issued. This first reserve will be protected by the holding unit until implementing instructions are received from the issuing agency. The C-E officer will prepare and hold a third edition while a fourth is being planned.

c. Planning radio communications also requires a degree of proficiency in the techniques of selecting individual frequencies to insure electromagnetic compatibility. Attempts to operate while resolving problems stemming from malassigned frequencies increase friendly vulnerability. The frustration and confusion, as well as the lack of communication capability, that results during these situations greatly reduce friendly command and control capabilities.

(1) Associated with each type of radio equipment are certain electronic characteristics that limit fully random selection of frequencies. The most apparent limitation is the range of frequencies over which the equipment will operate. Other characteristics that must be considered when assigning frequencies to tactical radio nets are: type of signal or emission; output power; the antenna and associated radiation characteristics; and method of controlling the operating frequency. Additionally, the interaction that results among electronic circuits placed in close proximity to each other must be understood.

(2) The division radio officer must have a thorough understanding of radio wave propagation for proper selection of net operating frequencies in light of the specific net requirements of: operating range; duration of operation (i.e., continuous or daylight hours only); and characteristics of equipment. This is particularly critical for AM/SSB and RATT nets. Radio-wave propagation prediction charts are available. Manually selecting individual frequencies to satisfy the requirements of the division is complicated and time consuming. However, systematic methods are required to minimize possible interference and allow some degree of random assignment. During recent years, automated techniques have been developed to assist in managing these activities.

8–3. Training

a. Instill Awareness/Consciousness. One of the most important actions that should be taken to reduce friendly vulnerabilities is to insure that all personnel are made aware of and appreciate the enemy EW threat. Personnel should know the threat exists and the devastating effects it can have on military operations. It is not enough to inform personnel of the threat and leave it at that. What is required is a meaningful level of continuous command interest that permeates the organization and instills a conscious awareness among commanders, staff officers, NCO's, and soldiers. This awareness must be sufficiently strong to guide and motivate personnel to develop good, sound security practices in everything they do. Every soldier is responsible for security. Make sure he knows and fully understands this.

b. Emphasize Operator Training.

(1) It is the friendly operator (radio, telephone, manual Morse, radar, etc.) that must meet the enemy EW threat daily. He constantly faces this threat and it is, therefore, essential that his training reflect a high degree of education and proficiency in recognizing and countering enemy EW attempts. The operator is the key element. He can negate an effective security posture that has been developed. He must know what preventive measures to take and how to employ them. He must be able to recognize enemy EW activities and how to counter them, and he must know how and where such attempts expeditiously.

(2) The friendly operator must be able to recognize enemy jamming attempts. He must be able to differentiate jamming from normal atmospheric interference. He must know precisely what to do when he is being jammed. He must be able to change to alternate frequencies quickly or be technically proficient to read through a jamming signal.

(3) The friendly operator must be able to recognize enemy attempts to intrude into friendly nets. The best way to accomplish this is to insure that established techniques and procedures are followed, such as the proper use of call signs and authentication measures.

(4) In short, the friendly operator is the cornerstone in the development and maintenance of an effective security posture to counter enemy attempts to obtain intelligence information through EW exploitation.

8–4. Installing

a. Although radio communications allow commanders more freedom of movement on the battlefield and thus greater combat power, the supporting communication equipment must be installed in a manner that will not unduly increase friendly vulnerability. The possibility that a division or brigade headquarters location can be closely approximated by the signature of supporting communication systems allows the enemy to exploit this knowledge at critical times. The multichannel and SSB/RATT communication systems are difficult to conceal. These systems must be located relatively close to their respective headquarters. They move with the headquarters. When the enemy locates the multichannel terminals, he can be assured that the headquarters is near. Their movement may divulge the intentions of the division—increasing friendly vulnerability.

b. Proper locating or siting of antennas can do a great deal to reduce friendly vulnerabilities. Headquarters and communication sites should take advantage of those features of the surrounding terrain that shield the antenna from the enemy. This will reduce the amount of radiated energy available for the enemy to intercept and exploit.

c. The type of antenna used will also influence friendle vulnerabilities. An omnidirectional antenna, for example, radiates in all directions and increases friendly vulnerabilities. A highly directional antenna should be used when available to reduce the amount of radiation toward the enemy. Variations in orientation and height of the antenna can be used to result in a favorable increase in the desired signal. Remoting transmitting equipment also increases the security of the headquarters supported. Some armies require as much as 2,000 meters separation. Our equipment has similar capabilities—insist on its employment.

8–5. Operating

a. Transmission Discipline. Transmission discipline is more than a set of procedures to follow. If friendly vulnerabilities are to be reduced, it is a state of mind that must exist. Adherence to tactical communication procedures is critical and determine to a very large degree the success of enemy listening, locating, and disruptive activities. The only truly effective way to create this state of mind is through continuous emphasis and command interest at all levels. Remember, this procedure also applies to telephones. They are normally connected to the multichannel radio systems linking higher and subordinate headquarters. Transmission discipline involves a number of operator-related actions that must be taken, and these actions must be understood and enforced by all commanders. Some of the more important techniques are discussed below.

(1) Users and communication technicians, alike, must operate in accordance with prescribed procedures and security instructions. Individual acts of poor radio discipline may not be classified as breaks of security. However, the cumulative effect may result in a pattern identifiable with a given operation, organization, or net.

(2) Transmissions should be as short as possible. This requires messages to be brief, clear, and concise. It also requires operators to refrain from engaging in unnecessary chatter. The longer the transmission, the greater the probability that the enemy will intercept that transmission. Shortening transmissions will reduce the amount of time enemy intelligence units have available to search and intercept friendly transmissions. Transmitting information is, of course, absolutely essential to the commander if he is to succeed on the battlefield; this is not to say, however, that unlimited transmissions should be tolerated in the name of combat success. When timeliness is not important, consider the use of messengers or other means of transmitting information that will not provide the enemy lucrative sources of intelligence information.

(3) Operating schedules for transmitting in-

formation should be random. If operating schedules are consistent, the enemy is better able to plan EW activities in advance and thus better able to exploit friendly transmissions. Avoid establishing any form or pattern that the enemy can discern, for it will only aid his exploitation efforts.

(4) Using maximum transmitter power will increase the capability of enemy EW units to intercept friendly transmissions. The lowest level of power-setting necessary to effectively transmit information should be used in all cases. The high power-setting should be reserved for use in emergency situations or when operating under adverse conditions caused by natural interference or enemy activity. Keep the power-setting low and you will make it just that much more difficult for the enemy to locate and intercept your transmission.

(5) Authentication is the best defense against enemy intrusion. Readiness to authenticate accurately is extremely important and must be emphasized. AR 380–52 prescribes the rules for acquisition and use of Army-approved authentication systems.

(6) Emergency instructions for communication operations must always be immediately available. Operators must be prepared to continue with new codes, authentication systems, call signs, and frequency assignments. Instructions for reestablishing communications must also be known.

b. Secure Modes.

(1) Secure transmission modes, such as voice encryption or ciphers, offer the tactical commander an extremely high degree of operational security and should be used whenever possible. The voice encryption devices associated with the FM radios provide the commander with a new dimension in command and control. However, the following characteristics must not be overlooked.

(2) Using encryption systems does not preclude the enemy from intercepting and locating friendly units. If a transmitter is being keyed, be it in plain language or encrypted, the enemy is capable of locating that transmitter. Additionally, valuable information can be obtained by enemy intelligence units evaluating traffic flow, volume, and precedence. Therefore, basic rules of transmission discipline previously discussed still apply. Most important, transmissions should be short, random, and with low power. Continued use of secure modes, however, may increase the likelihood that the enemy may elect to destroy or jam rather than wait for a less frequent, plain-language transmission—keeping him interested may require special communication plans.

(3) Only approved codes should be used to transmit classified information. Unauthorized brevity codes or point-of-origin codes may be simpler, faster, and easier to use; but they simply do not provide the requisite degree of security necessary to protect information relating to military operations. Unauthorized codes should not be used, for they provide a lucrative and easily exploitable source of intelligence. Personnel at all levels should recognize the inherent security problems created by the use of unauthorized codes.

c. Operations against any enemy will expose communication equipment and personnel to disruptive actions. Operator skill, confidence, and remedial actions are essential for maintaining communications in these situations. The commander and staff must likewise understand the consequences associated with employment in an active EW environment and be able to direct actions designed to minimize the disruptive effects. A communicator's EW checklist for commanders, staff, and communication personnel is at appendix B.

8–6. Noncommunication Systems

Like communication systems, noncommunication systems—radar, navigation aids, and optical systems—are vulnerable to enemy action. These equipments radiate energy that can be detected at distances much greater than normal operating range. Consequently, transmission discipline is essential. Use the lowest power-setting possible and avoid operations that unnecessarily expose noncommunication systems to enemy detection. Turn them off when not needed. Likewise, operators—including pilots—must be alert to enemy attempts to provide false signals designed to entice or lure friendly units astray. Techniques must be developed to provide a quick doublecheck of suspected signals or returns from radars and report these events accordingly.

8–7. Reporting Difficulties

a. A prompt, accurate, and complete report of enemy EW action is important, since an enemy disruptive attack is usually part of a well-organized plan and frequently precedes important tactical maneuvers. Reports from individual radio operators often provide intelligence on the extent and importance of enemy actions. Properly correlated disruptive information may serve as a warning of impending enemy action. Therefore, operators or users must never reveal in any manner an awareness of enemy disruption activities. Such an admission advises the enemy of the effectiveness of his effort, a determination otherwise difficult to make.

b. AR 105-3 establishes procedures for reporting and evaluating information concerning incidents of enemy disruptive activities and interference to US military communications. An enemy may attempt to meacon, i.e., transmit or similate radio navigation signals for the purpose of confusing airborne navigation, or he may intrude into our communication system by intentionally inserting false signals with the objective of deceiving operators or causing confusion. These attempts should be reported. The AR contains a universally applicable outline of information to be reported. SOP's should contain an abbreviated format including only the mandatory items and locally appropriate procedures.

c. Actions should be initiated to eliminate recognized deficiencies in communication equipment and procedures. Inadequate or low performance of equipment may be combatted by development of fixes or new systems. Consequently, repeated occurrences of suspected malfunctions should be reported to the equipment developer and research agencies. The field commander is in the best position to evaluate, and it is incumbent on him to provide timely feedback in order to develop improvements.

APPENDIX A

REFERENCES

A–1. Army Regulations (AR)

(C)	10–122	United States Army Security Agency (U)
	11–13	Army Electromagnetic Compatibility Program
	70–1	Army Research, Development and Acquisition
	105–1	Telecommunications Management
(C)	105–2	Electronic Counter-Countermeasures (ECCM) (U)
(C)	105–3	Reporting, Meaconing, Intrusion, Jamming, and Interference of Electromagnetic Systems (U)
(C)	105–5	Electromagnetic Cover and Deception (EC&D) (U)
(C)	105–7	Quick Reaction Capability for Electronic Warfare (U)
	105–16	Radio Frequency Allocations for Equipment Under Development, Production, and Procurement.
	105–63	Army Electromagnetic Spectrum Usage Program
	105–86	Performing Electronic Countermeasures in the United States and Canada
(C)	105–8	Electronic Warfare (U)
	310–25	Dictionary of United States Army Terms (Short Title: AD)
(S)	380–35	Security, Use and Dissemination of Communications Intelligence (COMINT) (U)
(S)	381–3	Signals Intelligence (SIGINT) (U)
(C)	530–1	Operations Security (U)
(C)	530–2	Communications Security (U)
(C)	530–3	Electronic Security (U)
(C)	530–4	Control of Compromising Emanations (U)

A–2. Field Manuals (FM).

	24–1	Tactical Communications Doctrine
(C)	31–40	Tactical Cover and Deception (U)
(C)	32–5	Signal Security (SIG SEC) (U)
(S)	32–10	USASA in Support of Tactical Operations (U)
(S)	32–15	Broadcast Countermeasures (U)
(C)	32–20	Electronic Warfare (U)
	101–5	Staff Officers Field Manual: Staff Organization and Procedure
	105–5	Maneuver Control

A–3. Army Subject Schedules (ASubjScd).

	32–1	Electronic Warfare for Ground Surveillance and Target Acquisition Radars
(C)	32–200	Team and Section Training of the Electronic Warfare Element, Army, Corps and Divisional Tactical Operations Centers (U)

A–4. Army Training Programs (ATP).

(C)	32–500	Army Security Agency Units, Detachments, and Teams (U)

A–5. Army Training Tests (ATT).

	32–400	Electronic Warfare (EW) Army Type Divisions, Brigades, Battalions, Other Units and Teams

(C)	32-500	Army Security Agency Units and Teams (u) (TOE 32-Series)

A-6. Training Bulletins, Circulars and Manuals (TB, TC, TM).

(C)	TB 380-3	Signal Security Improved Electronic Counter-Countermeasures Through Electronic Security (U)
(S)	TB 380-4	Improved Electronic Security Through Emitter Design (U)
(C)	TB 380-6-1	Improved Electronic Security for the Hawk Air Defense Guided Missile System (U)
(C)	TB 380-6-2	Improved Electronic Security for the Improved Nike-Hercules Air Defense Guided Missile System (U)
(C)	TB 380-6-3	Improved Electronic Security for the AN/MPQ-4A Radar Set (U)
(C)	TB 380-6-4	Improved Electronic Security for the AN/TPS-25A Radar Set (U)
(C)	TB 380-6-5	Improved Electronic Security for the AN/FPN-40 Radar Set (U)
	TC 32-05-2	Communication Electronics Counter-Countermeasures Procedures
	TC 32-20	Electronic Warfare Training

APPENDIX B

TACTICAL COMMUNICATOR'S EW CHECKLIST

COMMANDERS AND STAFF

—Stress radio discipline and security.
—Use brevity codes to direct plans.
—Keep messages as short as possible.
—Always inform the next higher headquarters of enemy disruptive activities.
—If possible, study and plan all communications in advance.
—Reduce the use of radio messages to an absolute minimum.
—Destroy enemy jamming stations, if possible.

COMMUNICATION OFFICERS

—Enforce radio discipline and security to the maximum.
—Use the radio only when necessary.
—Site radio stations and antennas to evade enemy signals.
—Always include alternate call signs and frequencies and prearranged plans for their use in the CEOI.
—Use minimum power to get the message through.
—Train radio operators to readjust equipment and continue copying through disruptive signals.
—Always report enemy disruptive activities to the commanding officer and his staff.
—Arrange nets so that satellite stations can communicate with each other, as well as with the control station.
—Provide alternate routing or alternate channels of radio communication.
—Correct communication deficiencies caused by:
  —Too great a distance between radio sets.
  —Poor choice of location (siting) at one or both ends of the circuit.
  —Terrain—hills or mountains.
  —Noise and interference.
  —Not enough transmitter power.
  —Defective equipment.
  —Improper adjustment of equipment.
  —Ineffective antenna.
  —Improper frequency assignment.
  —Improperly maintained and operated equipment.

EACH RADIO USER AND OPERATOR

—Observe radio discipline at all times.
—Learn to recognize enemy disruptive signal, and report details to the officer in charge of the radio station. Keep calm and keep trying to operate through the interference.
—Learn to readjust the set to minimize the effects of enemy signals.
—Operate with minimum power until jammed—then, increase power.
—Shift to alternate frequencies and call signs as directed.
—Authenticate all transmissions.
—Use a dummy antenna, when one is provided, to tune the transmitter.
—KEEP OFF THE AIR as much as possible. Transmit only when absolutely necessary.
—Keep transmissions as short as possible.
—Listen prior to transmitting to avoid interference with the transmissions of other stations.
—Use a handset or headset, rather than a loudspeaker, if the incoming signal is weak.
—Speak directly into the microphone.
—Keep the radio set clean and dry. Handle the radio with care.
—Study the technical manuals—know your equipment.

—Set up routine inspection and maintenance procedures for the following:

- —Keep plugs and jacks clean.
- —Make sure that antenna insulators are dry, clean, and free of cracks.
- —Insure that antenna connections and power connections are tight and cables are not torn or cut.
- —Check knobs and controls to insure that they operate easily without binding.
- —Make sure that dry batteries are fresh, and remove batteries when the equipment is in storage or not in use.

GLOSSARY

Authentication—A security measure designed to protect a communication system against fraudulent transmissions.

Babbled Voice Jamming—A modulating signal composed of mixed voices engaged in simultaneous conversations.

Barrage Jamming—Simultaneous electronic jamming over a broad band of frequencies.

Brevity Code—A code that provides no security but has as its sole purpose the shortening of unclassified phrases, sentences, or groups of sentences frequently employed, rather than concealment of their content. The vocabulary may remain in effect for an indefinite period of time. This type of code must be used in conjunction with a means of encipherment to provide security.

Chaff—Radar confusion reflectors that consist of thin, narrow, metalic strips of various lengths and frequency responses, used to reflect echoes for confusion purposes. To be most effective, the strips are cut to a half wavelength of the desired radar frequency.

Communication-Electronics Operation Instructions (CEOI)—A series of orders issued for the technical control and coordination of the signal communication activities of a command.

Communications-Electronics Signal Instructions (CESI)—A series of instructions explaining the use of items included in the CEOI. The CESI may also include other technical instructions required to coordinate and control the communications-electronics operation of the command.

Communications Intelligence (COMINT)—Technical and intelligence information derived from foreign communication by other than the intended recipients.

Communications Security (COMSEC)—The protection resulting from all measures designed to deny to unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretations of the results of such study. COMSEC includes cryptosecurity, physical security, and transmission security.

Compromise—In communication usage, the knowledge or belief that cryptographic material has been captured, stolen, lost, or exposed to observation by enemy elements, thereby endangering the security of messages encrypted in that system.

Continuous Wave (CW)—A continuous, constant amplitude radio frequency wave.

Corner Reflector—A device consisting of three mutually perpendicular intersecting planes whose right angles meet at a point. Electromagnetic waves striking any one of the planes will be reflected back to the source of radiation.

Countermeasures—That form of military science that by the employment of devices and/or techniques has as its objective the impairment of the operational effectiveness of enemy activity.

Deception—Operations undertaken to support tactical and strategic plans and orders to deny enemy surveillance true information while providing the enemy false information to achieve surprise.

Electromagnetic—Pertaining to the combined electric and magnetic fields associated with radiation or with movements of charged particles.

Electronic Counter-Countermeasures (ECCM)—That major subdivision of electronic warfare involving actions taken to insure our own effective use of electromagnetic radiations despite the enemy's use of countermeasures.

Electronic Countermeasures (ECM)—That major subdivision of electronic warfare involving actions taken to prevent or reduce the effectiveness of enemy equipment and tactics employing or affected by electromagnetic radiations and to exploit the enemy's use of such radiations.

Electronic Deception—The deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic radiations in a manner intended to mislead an enemy in the interpretation of data received by his electronic equipment or to present false indications to electronic systems.

Electronic Intelligence (ELINT)—The intelligence information product of activities engaged in the collection and processing, for subsequent intelligence purposes, of foreign, noncommunication, electromagnetic radiations emanating from other than nuclear detonations and radioactive sources.

Electronic Security (ELSEC)—The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of friendly noncommunication electromagnetic radiations.

Electronic Warfare (EW)—That division of the military use of electronics involving actions taken to prevent or reduce an enemy's effective use of radiated electromagnetic energy, and actions taken to insure our own effective use of radiated electromagnetic energy.

Electronic Warfare Officer (EWO)—A deputy to the G3 responsible to the G3 for the planning and supervising of EW operations, preparing and coordinating EW annexes to plans and orders, assisting in determining EW support requirements, and advising on EW matters.

Electronic Warfare Support Measures (ESM)—That division of EW involving actions taken to search for, intercept, locate, and immediately identify radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, ESM provides a source of EW information required to conduct ECM, ECCM, threat detection, warning, avoidance, target acquisition, and homing.

Electro-Optic (EO)—Term used to describe the technology achieved through the union of optics and electronics. As presently applied, the term includes lasers, photometry (light intensity measurement), infrared and various other types of visible and infrared imaging systems, i.e., low light level television (LLTV), optical contrast sensors, and signal processing devices.

Emitter—Term used to describe any device that radiates electromagnetic energy.

Gigahertz (GHz)—1,000-megahertz.

Guarded Frequency—See *Restricted Frequency.*

Gulls—A reflector device near ground or water level used in electronic countermeasures.

Gulls Jamming—This jamming signal is generated by a quick rise and slow fall of a variable audio frequency. Nuisance effect on voice-modulated circuits.

Hertz (Hz)—International unit of frequency, equal to one cycle per second. ("Hertz" replaces obsolete term "cycle," e.g., kilocycle, megacycle, and gigacycle become kilohertz, megahertz, and gigahertz respectively.)

Initative Electronic Deception—The intrusion on the enemy's channels and the introduction of matter in imitation of his own electromagnetic radiations for the purpose of deceiving or confusing him.

Interception—The act of listening in on and/or recording signals intended for another party for the purpose of obtaining intelligence.

Interference—Any electrical disturbances from a source external to the equipment that causes undesirable responses in electronic circuits.

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.

Jamming to Signal Ratio (J/S Ratio)—The ratio of the jamming signal power to the target signal power measured at the target receiver antenna.

Kilohertz (KHz)—1,000 hertz.

Kite—A reflection device suspended high in the air; used in electronic countermeasures.

Manipulative Electronic Deception—The use of friendly electromagnetic radiations in such a manner as to falsify the information that a foreign nation can obtain from analysis of these electromagnetic radiations.

Meaconing—A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

Megahertz (MHz)—1,000 Kilohertz.

Noise—Interference whose energy is distributed across a wide band of frequencies. It is received along with desired signals or generated within the equipment receiving the signals. It may be caused by natural radiation or man-made equipment.

Padding—Words or phrases, unrelated to the text of a message, added prior to encryption and deleted on decryption, or addition of random code groups to increase group count.

Protected Frequency—See *Restricted Frequency.*

Pulse Jamming—This signal resembles the monotonous rumble of high-speed rotating machinery. Nuisance effect on voice-modulated circuits.

Pulse Modulation—A method of modulation where the transmitter is turned on and off or pulsed. The amount of time the transmitter is on is normally short compared with the amount of time it is off. The amplitude, width, or position of the pulse and the number of pulses within a time frame may be varied to increase its information-carrying capability.

Pulse Repetition Frequency (PRF)—In radar, the number of pulses that occur each second. Not to be confused with transmission frequency which is determined by the rate at which cycles are repeated within the transmitted pulse.

Radar—Application of radio principles to detect the presence of an object, its character, direction, and distance. The word is derived from the term radio detection and ranging.

Radiate—To send out energy, such as radio frequency waves, into space.

Radio—Communication by electromagnetic waves transmitted through space.

Radio Direction Finding (RDF)—The process of determining the location of an electronic emitter through the intersection of azimuths or bearings obtained from three or more locations.

Radio Fix—The location of a friendly or enemy radio transmitter, determined by finding the direction of the radio transmitter from three or more direction finding stations.

Radio Frequency—A frequency in which radio transmission is possible. The useful range is from approximately 10 KHz to 100,000 MHz.

Radio Spectrum—The entire range of useful radio waves.

Radio Wave—A combination of electric and magnetic fields varying as a radio frequency and capable of traveling through space at the speed of light.

Random Noise Jamming—Synthetic radio noise which is random in amplitude and frequency. It is similar to normal background noise.

Random Pulse Jamming—Jamming technique where random noise pulses are transmitted at irregular rates.

Reflected Wave—Any wave reflected from a surface.

Refracted Wave—The wave that is bent (refracted) as it travels into a second medium of propagation, as from the lower atmosphere into an ionized layer of the atmosphere.

Repeater Jammer—Jamming system that receives a target signal, amplifies and modifies it, and retransmits it back to the source causing errors in the data obtained from the radar.

Restricted Frequencies—Frequencies against which intentional jamming or other forms of interference are prohibited.

Rope—An element of chaff consisting of a long roll of metallic foil or wire that is designed for broad low frequency response.

Rotary Jamming—This signal is a low pitched, slowly varying audio frequency. Effective against voice-modulated circuits.

Signals Intelligence (SIGINT)—A generic term which includes both communications and electronic intelligence.

SIGINT Support Element/Electronic Warfare Element (SSE/EWE)—At echelons above corps, corps, division, and separate brigade/regiment, participates in the planning, controlling, and evaluating of SIGINT and EW activities in support of impending or current tactical operations. Personnel to man the SSE/EWE are provided by the supporting USASA unit.

Signal Security (SIGSEC)—A generic term that includes both communication and electronic security.

Signal-to-Noise Ratio—The ratio of the amplitude of the desired signal to the amplitude of noise signals at a given point in time.

Spark Jamming—A burst of noise of short duration and high intensity that is repeated at a rapid rate. Effective against all types of radio communications.

Spoofing—A deception technique of transmitting a series of pulses to simulate target echoes and create several false targets on a radar indicator.

Spot Jamming—The jamming of a specific channel or frequency.

Stepped-Tones Jamming—Sometimes called bagpipes, the signal consists of separate audio tones in varying pitch. Effective against FM and AM radios.

Susceptibility—The degree to which a device, equipment, or weapon system is open to effective attack because of one or more inherent weaknesses.

Sweep Lock-on Jamming—A jamming system that sweeps a wide range of frequencies with a receiver. When a signal is detected, the sweep stops and transmitter is activated.

Synchronized Pulse Jamming—A jamming technique where jamming pulses are timed to arrive at the receiver when the receiver gate is open.

Taboo Frequency—See *Restricted Frequency.*

Transceiver—A radio transmitter and receiver combined in a common housing containing common components that are switched between the transmitter and receiver.

Transmission Security—That component of communication security that results from all measures designed to protect transmissions from unauthorized interception, traffic analysis, and imitative deception.

Transmitter—Term applied to any of the electrical equipment used for generating, amplifying, modulating, and radiating the modulated RF carrier into space.

Vulnerabilities—The characteristics of a system that cause it to suffer a definite degradation (incapability to perform designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) environment.

Wobbler Jamming—This jamming signal is a single frequency modulated by a low and slowly varying tone. Nuisance effect against voice-modulated radio circuits.

By Order of the Secretary of the Army:

FRED C. WEYAND
General, United States Army
Chief of Staff

Official:
VERNE L. BOWERS
Major General, United States Army
The Adjutant General

Distribution:

Active Army, ARNG, USAR: To be distributed in accordance with DA Form 12–11B requirements for Electronic Warfare (U) (Qty rqr block no. 325), and DA Form 12–12 requirements for all 30-series TOE (Qty rqr block no. 36).

DEPARTMENT OF THE ARMY
US ARMY AG PUBLICATIONS CENTER
2800 EASTERN BOULEVARD
BALTIMORE MARYLAND 21220