ATP 3-12.3

ELECTRONIC WARFARE TECHNIQUES

JULY 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 3-36, dated 16 December 2014.

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil/), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

*ATP 3-12.3

Army Techniques Publication
No. 3-12.3

Headquarters
Department of the Army
Washington, DC, 16 July 2019

Electronic Warfare Techniques

Contents

		Page
	PREFACE	**v**
	INTRODUCTION	**vii**
Chapter 1	**OVERVIEW OF ELECTRONIC WARFARE**	**1-1**
	Introduction to Electronic Warfare	1-1
	Electronic Warfare Divisions	1-1
	Electromagnetic Environment	1-2
Chapter 2	**ELECTRONIC WARFARE KEY PERSONNEL**	**2-1**
	Electronic Warfare Personnel	2-1
	Theater Army, Corps, Division and Brigade	2-1
Chapter 3	**ELECTRONIC WARFARE PLANNING AND EXECUTION**	**3-1**
	Electronic Warfare Contributions to the Military Decision-Making Process	3-1
	Electronic Warfare Planning Considerations	3-1
	Electronic Warfare Configurations	3-6
	Staff Contributions to Electronic Warfare Planning	3-8
	Targeting	3-11
	Electronic Warfare Execution	3-13
	Special Considerations During Execution	3-14
Chapter 4	**ELECTRONIC WARFARE PREPARATION AND ASSESSMENT**	**4-1**
	Electronic Warfare Preparation	4-1
	Integration of Electronic Warfare and Signals Intelligence	4-2
Chapter 5	**ELECTRONIC WARFARE SUPPORT TECHNIQUES**	**5-1**
	Planning Electronic Warfare Support	5-1
	Preparing Electronic Warfare Support	5-1
	Executing Electronic Warfare support	5-2
Chapter 6	**ELECTRONIC ATTACK TECHNIQUES**	**6-1**
	Planning Electronic Attack	6-1
	Preparing Electronic Attack	6-4
	Executing Electronic Attack	6-5
Chapter 7	**ELECTRONIC PROTECTION TECHNIQUES**	**7-1**
	Commander's Electronic Protection Responsibilities	7-1
	Planning Electronic Protection	7-1

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ATP 3-36, dated 16 December 2014.

Electromagnetic Compatibility 7-5
Electromagnetic Interference 7-5
Staff Electronic Protection Responsibilities 7-10
Equipment and Communications Enhancements 7-10

Appendix A THE ELECTROMAGNETIC SPECTRUM A-1

Appendix B JAMMING CALCULATIONS B-1

Appendix C ELECTRONIC WARFARE EQUIPMENT AND SYSTEMS C-1

Appendix D FORMS, REPORTS, AND MESSAGES D-1

GLOSSARY Glossary-1

REFERENCES References-1

INDEX Index-1

Figures

Figure 1-1. The electromagnetic spectrum and the electromagnetic environment 1-3
Figure 3-1. Electronic warfare in the targeting process 3-13
Figure 5-1. Example of a line-of-bearing 5-3
Figure 5-2. Example of a cut 5-3
Figure 5-3. Example of a fix 5-4
Figure 5-4. Concave baseline 5-5
Figure 5-5. Convex baseline 5-5
Figure 5-6. Baseline distance 5-6
Figure 5-7. Circular error probability 5-7
Figure 5-8. False azimuth indicated by refraction error 5-8
Figure 5-9. Reflection of a radio wave 5-9
Figure 6-1. Spot and barrage jamming 6-9
Figure 6-2. Jamming to disrupt enemy battalion to company communications 6-11
Figure 7-1. Threat use of terrain masking 7-3
Figure A-1. Department of Defense use of the electromagnetic spectrum A-4
Figure A-2. The ionosphere—daytime and nighttime composition A-7
Figure A-3. The electromagnetic spectrum and communication bands A-8
Figure A-4. Relationship between magnetic field strength and current A-9
Figure A-5. Amplitude modulation and frequency modulation A-10
Figure A-6. Pulse modulation A-11
Figure A-7. Antenna heights and line of sight distances A-12
Figure A-8. Electric and magnetic fields of a radio wave A-13
Figure A-9. Vertical and horizontal polarization A-13
Figure A-10. Circular and elliptical polarization A-14
Figure A-11. Planar wavefront reflection A-15
Figure A-12. Super-refraction ducts A-16
Figure A-13. Diffraction of radio waves around a solid object A-17

Figure A-14. Diffraction of radio waves around a hillside A-17
Figure A-15. Phase shift in multipath interference A-19
Figure A-16. Possible routes for ground waves A-20
Figure A-17. Relationship between skip zone, skip distance, and ground wave A-21
Figure A-18. Skywave paths A-22
Figure A-19. Refraction of frequency below the lowest usable frequency A-24
Figure B-1. Example minimum jammer power output calculations B-2
Figure B-2. Example maximum jammer power output calculation B-3
Figure D-1. Sample joint tactical air strike request D-2
Figure D-2. Joint spectrum interference resolution report instructions D-3
Figure D-3. Stop jamming message instructions D-4
Figure D-4. Electronic warfare frequency deconfliction message instructions D-4
Figure D-5. Electronic warfare mission summary instructions D-5
Figure D-6. Electronic warfare tasking message instructions D-7

Tables

Table 3-1. Example of an electronic warfare running estimate 3-3
Table 7-1. Techniques for minimizing transmissions and transmission times 7-4
Table 7-2. Common jamming signals 7-6
Table 7-3. Electromagnetic interference troubleshooting battle drill 7-9
Table A-1. Radio wave bands and frequencies A-1
Table A-2. Atmosphere layers, features, and their effects on radio waves A-5
Table A-3. Ionosphere layers and effects on radio waves A-6
Table A-4. The proportional relationship between amplitude and energy A-9
Table A-5. Propagation characteristics of terrain A-20
Table A-6. Transmission angle and distance A-23
Table B-1. Formula symbols B-1
Table D-1. Electronic attack request format instructions D-1

This page intentionally left blank.

Preface

ATP 3-12.3 complements the electronic warfare tactics presented in FM 3-12. ATP 3-12.3 supersedes ATP 3-36, dated 16 December 2014.

The principal audience for ATP 3-12.3 is electronic warfare professionals, spectrum managers, unit leaders, and Soldiers assigned to echelons theater army and below. Commanders and staffs of Army headquarters serving as a joint task force or multinational headquarters also use applicable joint or multinational doctrine for command and control of joint or multinational forces. Trainers and educators throughout the Army also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement (FM 27-10). They also adhere to the Army Ethic as described in ADRP 1.

ATP 3-12.3 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

ATP 3-12.3 applies to the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

The proponent for this publication is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Branch, United States Army Cyber Center of Excellence. Send comments and recommendations on a DA Form 2028, *Recommended Changes to Publications and Blank Forms*, to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-ID (ATP 3-12.3), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735, by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

This page intentionally left blank.

Introduction

ATP 3-12.3 provides doctrinal guidance and direction to the Army for conducting electronic warfare during unified land operations. This publication provides a description of electronic warfare, roles, relationships, responsibilities, and capabilities to support Army and joint operations.

ATP 3-12.3 nests with and supports joint electronic warfare doctrine and FM 3-12. It provides the doctrinal context to address the relationship between ADP 3-0 and ADP 5-0. Readers need to review ADP 2-0, ADP 3-0, ADP 5-0, ADP 6-0, ATP 2-01.3, ATP 2-22.6-2, FM 3-13, and FM 6-0 to understand the fundamentals of integrating and synchronizing electronic warfare with unified land operations.

ATP 3-12.3 provides details on techniques and procedures for Army electronic warfare. This publication includes the fundamentals and guiding principles for electronic warfare. It provides a cohesive and coherent description of how electronic warfare supports and enables operations as well as other mission tasks and functions at each echelon.

Electronic warfare integrates into operations using already established joint and Army processes such as the intelligence process, targeting and the military decision-making process. This publication includes electronic warfare staff responsibilities, contributions to the military decision-making process and targeting, and the reliance on intelligence preparation of the battlefield. It describes doctrinal techniques to address future operational challenges with current electronic warfare capabilities. Due to rapidly evolving electronic warfare capabilities and techniques, the Cyber COE will review and update ATP 3-12.3 on a frequent basis in order to keep pace with the continuously evolving electromagnetic operational environment.

This publication describes electronic warfare missions and actions within the electromagnetic spectrum and the interrelation of these activities among each other and all Army operations.

Chapter 1 provides an overview of electronic warfare including its three divisions: electronic attack, electronic protection, and electronic warfare support.

Chapter 2 describes the roles of key personnel for conducting electronic warfare at all echelons.

Chapter 3 discusses electronic warfare planning considerations. It includes an example of an electronic warfare-running estimate and describes electronic warfare equipment in man-pack, vehicle-mounted, fixed-site, and airborne configurations. The chapter discusses the reliance on staff products and processes including intelligence preparation of the battlefield, electromagnetic environment survey, and targeting.

Chapter 4 includes electronic warfare preparation, execution, and assessment. The chapter describes electromagnetic spectrum resources and discusses the joint restricted frequency list. This chapter provides techniques to integrate signals intelligence and electronic warfare resources to increase operational flexibility.

Chapter 5 provides techniques for planning and executing election warfare support to operations. The chapter includes descriptions of direction finding techniques.

Chapter 6 includes electronic attack planning and coordination techniques in support of large-scale combat operations. It discusses electromagnetic deception and provides vignettes regarding electronic attack.

Chapter 7 discusses electronic protection techniques. The text includes the integration of electronic warfare and signal planning to conduct electronic protection. The chapter provides radio users and staff with techniques to prevent threat radio interception and detection and targeting of friendly forces.

Appendix A describes radio propagation characteristics and the bands within the electromagnetic spectrum.

Appendix B includes formulas used to determine transmission power requirements for jamming radio receivers.

Appendix C discusses friendly electronic warfare equipment and associated characteristics including ground and airborne electronic warfare platforms.

Appendix D provides forms, reports, and messages used to plan and execute electronic warfare along with electromagnetic spectrum management identities.

Chapter 1
Overview of Electronic Warfare

This chapter discusses the importance of electronic warfare during Army operations. The text provides and introduction to electronic warfare, the electromagnetic environment, definitions, and descriptions relating to electronic warfare.

INTRODUCTION TO ELECTRONIC WARFARE

1-1. From the beginning of the 20th century, pioneers of the radio recognized the military application of the electromagnetic spectrum (EMS). In the decades that followed, state and non-state actors alike used radios to support navigation, command and control, intelligence gathering, and information operations. Radio communications are desirable targets due to their use in military operations. Commanders learned to protect their radios while seeking to exploit, degrade, or destroy the EMS capabilities of their adversaries. *Electronic warfare* (EW) is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). *Directed energy* is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles (JP 3-13.1).

1-2. Historically, EW has significant roles in combat operations. During World War II, British forces used radio transmissions to overpower German radio receivers. The jamming missions successfully disrupted the Germans' command and control systems and navigation capabilities. Following World War II, the Army continued to invest in EW competencies until the early 1990s.

1-3. During Operation ENDURING FREEDOM in Afghanistan and Operation IRAQI FREEDOM in Iraq, the U.S. Army encountered threats to friendly bases, convoys, and dismounted Soldiers as adversaries used radio-controlled improvised explosive devices to attack ground forces. As a countermeasure to the threat, the Army acquired new electronic attack (EA) capabilities to jam radio-activated triggers and defend friendly forces from explosive devices. The success of EW during these conflicts brought a resurgence in EW as a necessity.

1-4. EW is increasingly vital to Army preparations to defeat any potential threat during large-scale combat operations. The Army continues to build EW competencies to support decisive action and win in unified land operations. The Army's focus on large-scale combat operations highlights the need for a robust ground EW force to support multi-domain operations and enable the Army to fight and win in a complex world.

ELECTRONIC WARFARE DIVISIONS

1-5. The three divisions of EW are—

- EA.
- Electronic protection (EP).
- Electronic warfare support (ES).

1-6. Each division of EW has a unique role in supporting unified land operations. *Electronic attack* is the division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-13.1). *Electronic protection* is the division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-13.1). *Electronic warfare support* is the division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate

or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations (JP 3-13.1). For additional information about the EMS, see paragraph A-11.

1-7. Synchronizing EA, EP, and ES activities, among themselves and with other activities, focuses several capabilities to counter or protect from threat actions. Commanders consider EW while planning, integrating and synchronizing operations to increase combat effectiveness, protect the force, and project power throughout the EMS. The EMS is an environment that is a common denominator during all operations, crosses every domain, and affects every Army operation. An example of synchronization is ES identifying nefarious emissions to navigation warfare, offensive actions to stop the emissions, and ensuring friendly use of NAVWAR spectrum dependent resources. Navigation warfare is deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through the coordinated employment of space, cyberspace, and electronic warfare operations (JP 3-14).

ELECTROMAGNETIC ENVIRONMENT

1-8. The Army and potential adversaries increasingly use weapons, threat warning devices, logistical management systems, intelligence, surveillance, reconnaissance, and communications equipment that rely on the assured use of the EMS. The *electromagnetic spectrum* is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (JP 3-13.1). The Army is dependent on the EMS across every domain. To prevail in future conflicts and achieve situational understanding against a threat, it is critical to target threat capabilities at the right time and place and to open windows of opportunity across domains, particularly during large-scale combat operations.

1-9. The Army operates using the EMS in the electromagnetic environment (EME) in all geographic regions. The *electromagnetic environment* is the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emissions that may be encountered by a military force, system, or platform when performing its mission in its intended operational environment (JP 3-13.1). The reliance on the EMS results in a congested and contested EME, and to varying degrees in the different areas of operation. To preserve warfighting capabilities, commanders take actions to maintain an operational advantage with freedom of action in the EMS. Figure 1-1 on page 1-3 shows the distinction between the EMS and the EME.

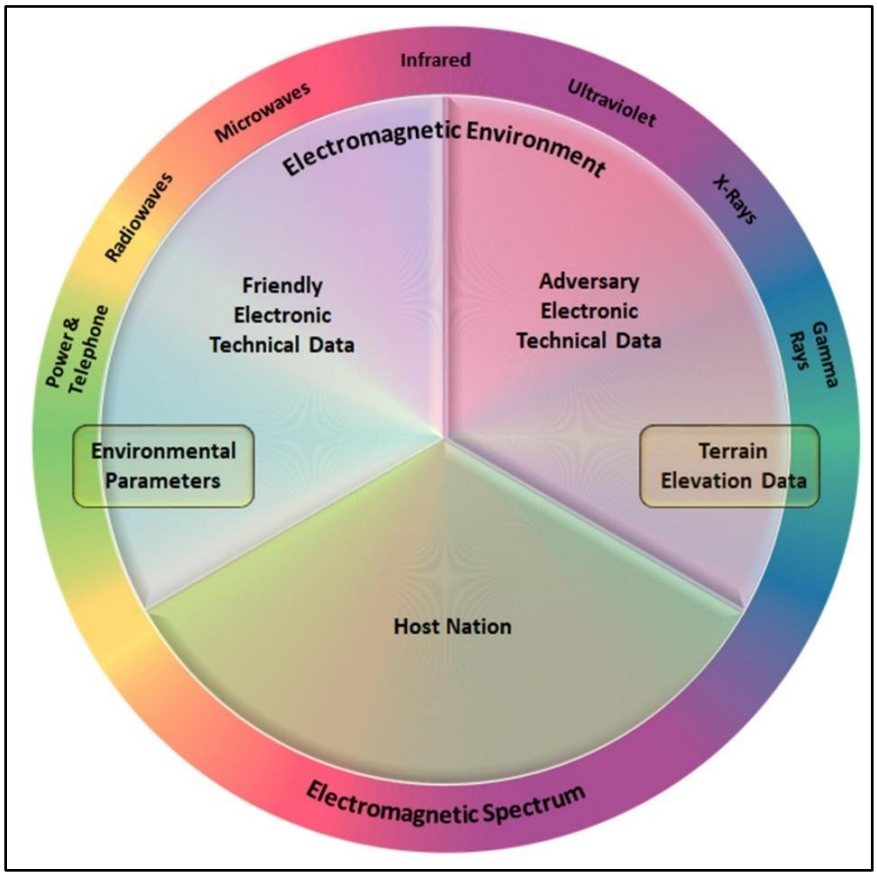

Figure 1-1. The electromagnetic spectrum and the electromagnetic environment

This page intentionally left blank.

Chapter 2
Electronic Warfare Key Personnel

The conduct of electronic warfare requires highly trained and skilled personnel. This chapter discusses electronic warfare professionals and their unique and overlapping duties and responsibilities. This chapter discusses the staff members with roles and responsibilities when planning and conducting electronic warfare operations.

ELECTRONIC WARFARE PERSONNEL

2-1. EW personnel on the staff are in the cyberspace electromagnetic activities (CEMA) section at theater army through brigade and consist of a cyber electronic warfare officer (CEWO), electronic warfare technician, electronic warfare noncommissioned officers, and spectrum manager. The CEMA section includes EW trained personnel, personnel trained in electromagnetic spectrum management, and personnel trained in cyberspace operations. For more information on cyberspace-trained personnel, refer to FM 3-12. *Cyberspace electromagnetic activities* is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). EW personnel are responsible to the chief of staff or the assistant chief of staff, operations (G-3) or battalion or brigade operations staff officer (S-3) staff. Battalions have a single EW representative that is a member of the battalion staff.

2-2. EW personnel in the CEMA section plan and conduct EW during the full range of military operations. EW personnel conduct CEMA with assistance from, and in coordination with, other members of the CEMA working group. FM 3-12 contains more information on the CEMA working group. EW personnel plan the employment of EA, frequencies for targeting, analyze the probability of frequency fratricide, and collaborate with the assistant chief of staff, signal (G-6) or battalion or brigade signal staff officer (S-6) to mitigate harmful effects from EW to friendly personnel, equipment, and facilities.

2-3. The CEWO disseminates key mission status information, such as cancellation of electronic attacks, and coordinates with other staff members within the command post to contribute to situational awareness. The CEWO coordinates with the following sections—

- Assistant chief of staff, intelligence (G-2) or battalion or brigade intelligence staff officer (S-2).
- G-3 (S-3).
- G-5 (S-5).
- G-6 (S-6).
- Fire support coordinator.
- Information operations officer.
- Space support element.
- Special technical operations staff.
- Staff Judge Advocate (SJA) or representative.

THEATER ARMY, CORPS, DIVISION AND BRIGADE

2-4. The Army assigns EW personnel to CEMA sections at theater army, corps, division, and brigade echelons. Each EW professional has specific roles and responsibilities.

CYBER ELECTRONIC WARFARE OFFICER

2-5. The CEWO's EW responsibilities include—

- Integrates, coordinates, and synchronizes EW effects.
- Nominates EW targets for approval from the fire support coordinator and commander.
- Receives, vets, and processes EW targets from subordinate units.
- Develops and prioritizes effects in the EMS.
- Develops and prioritizes targets with the fire support coordinator.
- Monitors and continually assesses measures of performance and measures of effectiveness for
- EW operations.
- Coordinates targeting and assessment collection with higher, adjacent, and subordinate
- organizations or units.
- Advises the commander and staff on plan modifications, based on the assessment.
- Advises the commander on how EW effects can impact the operational
- environment.
- Provides recommendations on commander's critical information requirements.
- Prepares and processes the electronic attack request format (EARF).
- Participates in other cells and working groups, as required, to ensure integration of
- EW operations.
- Deconflicts EW operations with the spectrum manager.
- Coordinates with the CEMA working group to plan and synchronize EW operations.
- Assists the G-2 (S-2) during intelligence preparation of the battlefield (IPB), as required.
- Provides information requirements to support planning, integration, and synchronization of
- EW operations.
- Serves as the Jam Control Authority (JCA) for EW operations, as directed by the commander.

ELECTRONIC WARFARE TECHNICIAN

2-6. The electronic warfare technician—

- Serves as the technical subject-matter expert for EW to the CEWO and CEMA working group.
- Plans and coordinates EW across functional and integrating cells.
- Provides input for the integration of threat electronic technical data as part of the IPB process.
- Coordinates target information and synchronizes EA and ES activities with the G-2 (S-2) staff.
- Integrates EW into the targeting process, monitors EW target requests, and conducts battle damage assessment for EW.
- Recommends employment of EW resources.
- Provides technical oversight and supervision for the maintenance of EW equipment.
- Conducts, maintains, and updates an electromagnetic environment survey.
- Identifies enemy and friendly effects within the EMS.
- Assists in the development and execution of standard operating procedure (SOP) and battle drills.

ELECTRONIC WARFARE NONCOMMISSIONED OFFICER

2-7. The electronic warfare noncommissioned officer—

- Plans, manages, and executes EW tasks.
- Manages the availability and employment of EW assets.
- Serves as senior developer and trainer for EW.
- Distributes, maintains, and consolidates EW staff products.
- Collects and maintains data for electromagnetic energy surveys.
- Coordinates and deconflicts EMS resources with the spectrum manager.
- Operates and maintains EW tools.

SPECTRUM MANAGER

2-8. There are spectrum managers in the CEMA section and G-6 (S-6) staff. The G-6 (S-6) staff spectrum manager manages EMS resources that support the friendly use of the EMS. The CEMA section spectrum manager manages EMS resources for EW activities and provides the EW input to the common operational picture. The CEMA section spectrum manager is responsible for—

- Leads, develops, and synchronizes the EW and EP plan by assessing EA effects on friendly force emitters.
- Mitigates harmful impact of EA on friendly forces through coordination with higher and subordinate units.
- Synchronizes with intelligence on the EA effects to support intelligence gain and loss considerations.
- Synchronizes cyberspace operations to protect radio frequency enabled transport layers.
- Coordinates to support protecting radio frequency-enabled information operations.
- Collaborates with staff, subordinate, and senior organizations to identify unit emitters for inclusion on the joint restricted frequency list (JRFL).
- Performs EW-related documentation and investigation of prohibitive electromagnetic interference to support the G-6 (S-6) led joint spectrum interference resolution program.
- Participates in the CEMA working group to deconflict EMS requirements.
- Provides advice and assistance in the planning and execution of EW operations.

Note. The JRFL is a concise list of restricted frequencies and networks categorized as taboo, protected, and guarded.

BATTALION ELECTRONIC WARFARE PERSONNEL

2-9. Battalions have an EW representative responsible for planning and integrating EW capabilities. The EW representative coordinates with the S-2, S-6 staff, fire support officer, the joint terminal attack controller (JTAC), and other staff sections when assigned. In support of a battalion mission, the battalion EW representative requests effects that require coordination with the brigade CEMA section. Battalion EW representatives' duties and responsibilities include—

- Advising the commander on the employment of EW resources.
- Integrating EW during the military decision-making process (MDMP).
- Recommending and implementing EP activities in close coordination with the S-6.
- Managing the maintenance and employment of EW equipment.
- Establishing battalion EW SOP.
- Submitting EW requests and concept of operations to the brigade CEMA section.
- Coordinating with airborne EW assets to provide the aircraft situational awareness of a ground unit's operational environment including actions on the desired target.
- Establishing and enforcing counter radio-controlled improvised explosive device electronic warfare (CREW) employment. For more information about CREW devices, see paragraph 6-56.
- Conducting all EW related training to battalion and company personnel.
- Managing battalion and company EW resource reprogramming activities more information on reprogramming activities is in chapter 3.
- Conducting operational checks and inspections of EW equipment programs.

COMPANY COUNTER RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICE ELECTRONIC WARFARE SPECIALISTS

2-10. Company CREW specialists, operate, maintain, reprogram, and reconfigure CREW devices for the unit. Commanders rely on CREW specialists to manage the devices within the company. CREW specialists—

- Advise the company commander on the employment of CREW and EW resources.
- Train and assist operators in the use and maintenance of CREW equipment
- Perform pre-combat checks and pre-combat inspections for EW equipment.
- Ensure CREW systems are operational and report deficiencies.

ELECTRONIC WARFARE CONTROL AUTHORITY

2-11. In some instances, EW personnel in an Army headquarters serve as the EW control authority. The EW control authority establishes guidance for EA on behalf of the joint force commander. If designated as the electronic warfare control authority the senior EW staff officer has the following responsibilities—

- Approve, disapprove, and modify EA requests from within the organization and subordinate units.
- Integrate and synchronizing EA activities.
- Maintain a log containing all approved jamming activity.
- Participate in the development of and ensuring compliance with the JRFL and all other EMS use plans.
- Maintain situational awareness of EA capable systems in the area of operations.
- Deconflict EA and ES, in coordination with the G-2 (S-2), to make recommendations to the combatant commander on intelligence gain or loss.
- Coordinate EA requirements with joint force components.
- Investigate unauthorized EA events and implement corrective measures.
- Approve or deny cease jamming requests.

Note. Joint organizations designate EW professionals as an electronic warfare control authority as needed. For more information about EW control authority, refer to JP 3-13.1.

STAFF MEMBERS AND ELECTRONIC WARFARE

2-12. The staff contributes to EW by providing unique products and guidance to the CEWO during all phases of an operation. The same staff members participate in the CEMA working group as necessary.

G-2 (S-2) Staff

2-13. The G-2 (S-2) staff advises the commander and staff on intelligence aspects of EW operations. The G-2 (S-2) staff—

- Provides threat characteristics to support programming of unit EW systems.
- Maintains appropriate threat EW data.
- Maintains the signals intelligence (SIGINT) priorities of collection and informs the staff for situational awareness.
- Ensures electronic threat characteristics requirements are a part of the information collection plan.
- Determines enemy organizations' network structures, disposition, capabilities, limitations, vulnerabilities, and intentions through collection, analysis, reporting, and dissemination.
- Determines enemy EW vulnerabilities and high-value targets.
- Provides intelligence support to targeting operations.
- Assesses the effects of friendly EW activities on the enemy.
- Conducts intelligence gain or loss analysis for EW targets with intelligence value.
- Helps prepare the intelligence-related portion of the EW running estimate.
- Recommends guarded frequencies to the G-6 (S-6) staff for the JRFL.
- Provides updates to the electronic threat characteristics.
- Participates in the CEMA working group to synchronize information collection with EW requirements and deconflict planned EW activities.
- Deconflicts ES and SIGINT operations with the CEMA section.

G-3 (S-3) Staff

2-14. The G-3 (S-3) staff is responsible for the overall planning, coordination, and supervision of EW activities. The G-3 (S-3) staff—

- Plans for and incorporates EW into operation plans and orders, in particular within the fire support plan and the information operations plan (in joint operations).
- Tasks EW activities to assigned and attached units.
- Exercises control over EW, including electromagnetic deception plans.
- Directs EP measures based on recommendations from the G-6 (S-6) staff, the CEWO, and the CEMA working group.
- Coordinates EW training requirements.
- Issues EW support tasks within the information collection plan. These tasks are according to the collection plan and the requirements tools developed by the G-2 (S-2) staff and the requirements manager.
- Ensures, through the CEMA working group, that EW activities support the overall plan.
- Integrates EA within the targeting process.

G-6 (S-6) Staff

2-15. The network defense technician, network management technician, information services technician, spectrum manager, and information security manager participate in planning EW. The G-6 (S-6) staff—

- Assists the CEWO with the preparation of the EP policy.
- Reports enemy EA activity detected by friendly communications and electronics elements to the CEMA working group for counteraction.
- Assists the unit CEWO with resolving EW systems maintenance.
- Identifies and deconflicts electromagnetic interference (EMI).
- Issues the signal operating instructions (SOI).
- Ensures network connectivity for all EW computer systems.
- Provides EMS resources to the unit or task force (refer to ATP 6-02.70).
- Coordinates for EMS usage with higher echelon G-6 (S-6), communications system directorate of a joint staff, and applicable host-nation and international agencies as necessary.
- Prepares the restricted frequency list and issuance of emissions control guidance.
- Coordinates frequency allotment, assignment, and use.
- Supports the CEMA working group by assisting in the development of electromagnetic deception plans and activities that include EMS resources.
- Coordinates with higher echelon spectrum managers for EMS interference resolution.
- Assists the CEWO in issuing guidance to the unit, including subordinate elements, regarding deconfliction and resolution of interference problems and processes involving EW systems.
- Participates in the CEMA working group to deconflict friendly EMS requirements with EW activities and information collection efforts.
- Supports all subordinate unit software updates and communications security (COMSEC) requirements.
- Compiles and distributes the JRFL (Spectrum Manager).
- Assists the EW section with computer maintenance and troubleshooting.

Information Operations Officer

2-16. The information operations officer is responsible for all information operations. To enable information operations, the CEMA section undertakes deliberate actions designed to gain and maintain advantages in the information environment. Typically, but not solely, these actions occur through cyberspace operations and EW. The information operations officer—

- Ensures synchronization and deconfliction with other information operations.
- Considers second- and third-order effects of EW on information operations and proactively plans to enhance intended effects.

Staff Judge Advocate or Representative

2-17. The SJA is responsible for all legal advice. The SJA or representative reviews all EW operations to ensure they comply with existing DOD directives and instructions, rules of engagement (ROE), and applicable domestic and international laws, including the law of war. The SJA may also obtain any necessary authorities that are lacking.

Chapter 3
Electronic Warfare Planning and Execution

This chapter discusses electronic warfare contributions to the military decision-making process when supporting unified land operations. This chapter also provides the techniques for the coordination and synchronization of electronic warfare with nonlethal and lethal effects. This chapter addresses staff contributions to planning electronic warfare and equipment configuration for successful employment.

ELECTRONIC WARFARE CONTRIBUTIONS TO THE MILITARY DECISION-MAKING PROCESS

3-1. EW planners follow the MDMP. In a time-constrained environment, they follow the abbreviated MDMP appropriately. The CEWO ensures planned EW activities contribute to the operation. Staff planners with the necessary expertise, and in some cases access to sensitive compartmented information facilities, are essential for planning EW and related capabilities. Integrating EW into operations requires placing planners at the brigade combat team level with experience in capabilities, such as special technical operations and special access program effects. Throughout the MDMP, the CEWO continuously identifies risks and appropriate risk mitigation techniques.

3-2. The CEWO participates in the MDMP by planning and synchronizing EW and cyberspace operations actions. During planning, the CEWO considers joint, interorganizational, and multinational dependencies and interdependencies of EW resources.

3-3. The members of the CEMA section assist the CEWO during the MDMP by conducting terrain and radio wave propagation analysis relevant to friendly and threat forces within an operational environment. The results of the analysis contribute to staff products, such as map overlays depicting EW assets and their associated range of effectiveness. The staff uses the products to refine the EW portions of the plan. The CEMA section builds and staffs operations order appendices and annexes and submits them to the G-3 (S-3) staff for dissemination. The CEWO provides EA information to the fires staff for inclusion in Annex D of the operations order (FM 6-0).

3-4. The CEMA section considers policies, laws, and ROE that affect EW operations when participating in the MDMP process. The SJA and the CEMA working group develop the ROE for commander review. Planners and the SJA clarify the ROE or develop supplemental ROE when necessary. For more information about EW operations planning and the MDMP, refer to FM 3-12.

ELECTRONIC WARFARE PLANNING CONSIDERATIONS

3-5. Several considerations are important to planning EW operations to include equipment type, configurations, logistics, availability, and risks. The running estimate is a tool to assist with planning and maintaining awareness of EW capabilities, current missions, and future mission requirements.

PLANNING FACTORS

3-6. The CEWO visualizes an operational environment and EME using maps and simulation programs that predict the behavior of radio waves used during unified land operations. The course of action proposed by the CEWO require analysis to determine the capabilities and limitations of the systems. For example, man-pack EW systems are lightweight and highly mobile but also have limited transmit power for EA. Vehicle mounted systems allow for higher power output but have line of sight (LOS) limitation in dense terrain.

Airborne platforms offer the best LOS of EW systems, but are vulnerable to enemy air defense systems and have limited dwell time on target.

ADDITIONAL FACTORS FOR AIRBORNE PLANNING

3-7. Maintenance activities and other missions reduce the availability of aircraft to support EW requirements. Airborne platform unavailability for EW is attributed to—

- Poor weather and visibility that restrict flight.
- Planned and unplanned maintenance.
- Transport missions.
- Intelligence, surveillance, and reconnaissance missions.
- Communications missions.

LOGISTICAL CONSIDERATIONS

3-8. Units conduct scheduled and unscheduled maintenance on EW equipment. Maintenance ensures readiness for current and future operations. The CEWO, with assistance from logistics staff, develops an SOP that includes maintenance procedures. The CEWO or representative prioritizes maintenance efforts ensuring a unity of effort, as maintainers are a limited resource.

3-9. The planner considers—

- An EW capability replacement plan for potential coverage gaps and unexpected outages.
- Parts availability for maintenance to prevent non-mission capable equipment.
- Power resources including:
  - Batteries.
  - Generators and fuel.
  - Shore power.
  - Vehicle or transport power sources

3-10. Commanders allocate EW resources to support various units. When EW resources support another unit, the supported unit—

- Identifies EW requirements.
- Protects and defends EW assets.
- Provides logistical support.

RISK MANAGEMENT

3-11. EW can cause unwanted radio frequency (RF) exposure to personnel. High levels of RF exposure can damage external and internal human tissue. The CEWO identifies risks associated with EW activities and develops mitigating steps to reduce the risk to friendly personnel and equipment. The CEWO then coordinates with the staff to refine the risk mitigating recommendations and presents them to the commander. For more information about risk management, refer to ATP 5-19.

3-12. Planners synchronize EW with lethal and nonlethal capabilities to achieve desired effects. The CEWO uses predetermined formulas to calculate EA and ES. For additional information on predetermined formulas and jamming calculations, see appendix B.

3-13. EW actions can mitigate operational risk, though using EA, both offensively and defensively, has inherent risk associated with the systems due to emissions. The risks include hazards of electromagnetic radiation to personnel, hazards of electromagnetic radiation to fuels, and hazards of electromagnetic radiation to ordnance.

3-14. Hazards of electromagnetic radiation to personnel is the danger to personnel from the absorption of electromagnetic energy by the human body. Personnel hazards are associated with the absorption of RF energy above certain power levels in certain frequency bands for certain lengths of time. DODI 6055.11

specifies the allowable amounts of radiation and personnel exposure time to RF fields at particular intensities and frequencies.

3-15. Hazards of electromagnetic radiation to fuels is the hazard associated with the possibility of igniting fuel or other volatile materials through RF energy-induced arcs or sparks. It takes a certain amount of arc energy to ignite a fuel, and modern fuels are much safer than older fuels. This is a major concern when there is limited separation between EW capabilities and fuel, such as airfields, forward armament and refueling point, and refueling on-the-move locations. Fortunately, there are many operational safeguards against this problem.

3-16. Hazards of electromagnetic radiation to ordnance refers to the susceptibility of electro-explosive devices to RF energy. Electro-explosive or electrically-initiated devices are the control devices to detonate explosives, launch ejection seats, cut tow cables, and other similar functions. Modern communications and radar transmitters can produce high levels of electromagnetic energy that are potentially hazardous to ordnance. These environments can cause premature actuation of sensitive electro-explosive and electrically initiated devices.

RUNNING ESTIMATE

3-17. The CEWO prepares and continually updates the running estimate. A running estimate is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Information in the running estimate are committed and reserved assets, maintenance status of EW equipment and training proficiency of EW personnel. Resources that are useful in developing a running estimate are the maintenance report and the commanders' training assessments. Threat information is available from online databases, unit intelligence assets, and national intelligence sources.

3-18. The purpose of the CEMA section running estimate is to provide a consolidated list of information about cyberspace and the electromagnetic spectrum to assist the CEMA section in planning, preparing, and executing operations. The information serves as a foundation for the Appendix 12 to Annex C and tabs, and is dependent on information requirements with other staff such as Operations, Fires, Intelligence, and Signal as sources of information. Some of this information will be redundant with other staff section planning products. Table 3-1 is an example of an EW running estimate.

Table 3-1. Example of an electronic warfare running estimate

CEMA Section Running Estimate
1. Friendly electronic warfare systems. a. System nomenclature and disposition by echelon. i. Planning, modeling, and simulation tools. ii. Organic systems. iii. Echelons above corps and joint assets. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters, data paths, and bandwidth requirements). c. Modeling and simulation of each system based on differing parameters and area of operations i. Differing power ratios. ii. Antenna configuration. iii. Terrain. d. Constraints and limitations associated with each system.

Table 3-1. Example of an electronic warfare running estimate (continued)

CEMA Section Running Estimate (Continued)
2. Friendly spectrum-dependent systems. a. System nomenclature and disposition by echelon. i. VHF radios ii. Satellite communications terminals. iii. Radar sets. iv. Unmanned aircraft systems b. .System characteristics. i. Frequency ranges. ii. Bandwidth requirements. iii. Power. iv. Modulation. c. Modeling and simulation of each system, based on differing parameters and area of operations. d. Constraints and limitations associated with each system.
3. Friendly electronic warfare systems. a. System nomenclature and disposition by echelon. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters, data paths, and bandwidth requirements. c. Threat electronic warfare tactics, techniques, and procedures. d. Modeling and simulation of each system, based on differing parameters and area of operations. e. Critical capabilities and vulnerabilities by system.
4. Threat spectrum-dependent systems. a. System nomenclature and disposition by echelon. b. System characteristics. i. Frequency ranges. ii. Bandwidth requirements. iii. Power. iv. Modulation. c. Tactics, techniques, and procedures. d. Frequency allocations. e. Cueing cycles (radar sets) f. Modeling and simulation of each system, based on differing parameters and area of operations. g. Critical capabilities and vulnerabilities by system.

Table 3-1. Example of an electronic warfare running estimate (continued)

CEMA Section Running Estimate (Continued)
5. Civil infrastructure considerations. a. Networks in the area of operations. i. SCADA. ii. Internet service providers. iii. Fiber (regional, national, and international). b. Spectrum resources and allocations (with characteristics of each). i. Wi-Fi. ii. Broadcast television. iii. Broadcast radio. iv. Satellite ground stations. c. Physical access to structures and equipment.
Legend: SCADA supervisory control and data acquisition VHF very high frequency

3-19. The CEWO analyzes the operation and EW employment considerations early in the MDMP. These considerations include—

- Survivability of personnel and equipment.
- The time required to build or improve the unit's EP posture and position EA and ES capabilities.
- Ability of EW resources to achieve the desired effects.
- Reprogramming of EW assets.
- Capabilities, limitations, advantages, and disadvantages of available EW and SIGINT assets equipped with ES capability.
- Intelligence available for targeting.

Note. The G-2 (S-2) manages SIGINT resources that contribute to EW targeting.

SURVIVABILITY

3-20. Survivability of personnel and equipment rely on force protection and EP techniques. EP enhances force protection efforts as another method to mitigate environmental and adversarial effects. The CEMA section plans the mitigation actions, and the commander decides what risk is acceptable for an EW mission. Force protection risk mitigating techniques include coordinating ground or air escort and configuring EW equipment with organic EP capabilities. EP is not force protection or self-protection. EP is an EMS-dependent system’s use of electromagnetic energy and/or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1).

3-21. EP contributes to survivability. Antennas erected to minimum heights, while maintaining communications, prevent visual observation by the threat. This technique contributes to survivability. Survivability is a useful criterion for course of action analysis during the MDMP. For more information about EP, see chapter 7.

TIME

3-22. The CEWO uses available time to configure and position EW assets for optimal performance. Time also affects the selection of movement techniques for a mission. The CEWO synchronizes EA operations with maneuver and fire to maximize effects at the appropriate time. The CEWO also plans duration of EA effects based on target analysis to support survivability of EW assets.

EFFICACY

3-23. The CEWO considers which EW asset has the appropriate level of efficacy for an EW mission. Efficacy is the likelihood that an EW mission will achieve the desired effect. For example, EA has a minimum transmission power threshold. Transmission power settings below the threshold have reduced levels of efficacy to achieve the desired effect, whereas transmission power settings above the threshold have increased levels of efficacy to achieve the desired effect.

ELECTRONIC WARFARE REPROGRAMMING

3-24. *Electronic warfare reprogramming* is the deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment (JP 3-13.1). When information reveals that the adversary changes frequencies for communications or there are other changes in the EME, the CEWO ensures the reprogramming of EW systems or target sensing systems, to include the employment technique. Reprogramming includes changes to defensive systems, software, firmware, hardware, and information collection systems (JP 3-13.1). The change in the EME may affect friendly communication systems also. The CEWO informs the spectrum manager of the changes to EW requirements to coordinate the adjustment in mission parameters and may recommend friendly communications frequency changes to the G-6 (S-6). The responsibility to reprogram EW equipment is the responsibility of the unit; however, units should be aware of reprogramming efforts when operating with multi-national forces. Reprogramming is a national responsibility due to the effect on the EME. Refer to JP 3-13.1 for more information about reprogramming. EW reprogramming examples include—

- Changing target frequencies for jamming as well as updating restricted frequencies.
- Changes location of sensors due to environmental changes or interference.
- Installing the latest available software, firmware, and hardware for EW and SIGINT equipment.

ELECTRONIC WARFARE VISUALIZATION

3-25. The CEMA section visualizes and simulates the EMS, manmade effects, and environmental impacts. The information the section gains informs friendly actions and may provide insight to possible enemy COAs. There are automated tools to assist the CEMA section with the following tasks:

- Providing input to the common operational picture.
- Displaying sensor information from EW and SIGINT assets including—
  - Detecting emitters and plotting lines of bearing.
  - Analyzing circular error probable ellipse.
- Conducting mission planning and rehearsals.
- Managing EW assets.
- Modeling and visualizing how the EME responds to friendly and enemy EW activities.

3-26. The CEMA section analyzes the EME using—

- EMS sensors.
- Threat system databases.
- Intelligence information.
- Operational environment factors.

3-27. EW personnel require updates as the situation changes. The tools combined with staff interaction and the command and control system provide the updates.

ELECTRONIC WARFARE CONFIGURATIONS

3-28. EW equipment requires configuration for successful deployment. Units use EW equipment in man-pack, vehicle, fixed-site, and airborne configurations. Equipment configuration includes—

- Choosing omnidirectional or directional antennas.
- The physical placement of equipment.

- Selecting power resources for EW equipment.
- Primary, alternate, contingency, and emergency (PACE) plan for tasking and reporting.

3-29. Power sources for EW equipment include—

- Power generators such as gasoline or diesel powered engines.
- Batteries for man packs and vehicle-mounted configurations.
- Shore power for fixed EW assets.

Note. For more information about power considerations, see chapter 4.

MANPACK CONFIGURATION

3-30. Manpack configurations include EA and ES capabilities. For manpack configurations, the CEWO considers the following—

- Limited available transmit power for EA.
- Weight of antennas and batteries carried by the Soldier.

VEHICLE-MOUNTED CONFIGURATION

3-31. Vehicle-mounted EW equipment supports units with EA and ES capabilities. Units use vehicle-mounted EW equipment during maneuver or at the halt. Vehicle-mounted configurations include—

- Mounted and dismounted configurations.
- Jamming capabilities.
- Direction finding (DF) capabilities for locating and targeting threat transmitters.
- PACE plan for tasking and reporting

FIXED-SITE CONFIGURATION

3-32. Fixed-site EW configurations have more available transmitting power than manpack and vehicle EW configurations. Fixed EW configurations have multiple transmitters, receivers, and antennas that enable multiple EW activities to occur simultaneously. A fixed site may include transportable systems that require configuration and operation only at the halt requiring personnel to install or construct the system.

AIRBORNE CONFIGURATION

3-33. Airborne EW is the coupling of EW assets to airborne platforms such as unmanned aerial systems, tethered balloons, and rotary and fixed-wing aircraft. They provide an extended range over ground-based assets and greater mobility than ground-based assets. In addition, they support ground-based units.

3-34. The synchronization of airborne EW missions requires detailed planning. The time on target for airborne EW assets coupled to rotor and fixed-wing platforms is normally brief. Time on target for airborne EW is limited due to the high rate of speed of the aircraft. The short time on target is also a technique used to minimize the threat's abilities to detect the platforms using visual, DF and radar detection techniques.

3-35. Airborne EW activities require liaisons between the aircrews of the platform and the supported ground forces. Liaisons ensure—

- Situational awareness of mission support by platform.
- The supported unit is aware of platform protection tactics, techniques, and procedures to counter threat aircraft and air defense systems.

Airborne Platforms

Airborne platforms are low-density and high-demand resources. The CEWO considers the use of airborne platforms for all missions such as EW, SIGINT, surveillance, and reconnaissance. For example, if a unit has 12 airborne platforms, one assumes three are on a mission while nine are undergoing maintenance, returning from a mission, or in-flight to relieve an ongoing mission.

STAFF CONTRIBUTIONS TO ELECTRONIC WARFARE PLANNING

3-36. EW personnel are dependent on the staff for a variety of products to understand an operational environment, targeting, and EP requirements. The EW personnel can plan EW activities once they have sufficient situational awareness of an operational environment.

G-2 (S-2) STAFF

3-37. EW planners rely on the G-2 (S-2) staff for threat characteristics identified during IPB. The CEWO submits requests for information to address gaps identified during IPB.

3-38. In most cases, the CEWO relies on SIGINT-derived enemy electronic technical data to plan and conduct EW targeting operations. Therefore, the G-2 (S-2) staff supports the CEWO during the alignment of EW and SIGINT assets against the commander's priorities of effort to achieve the best possible outcomes. SIGINT and EW resources, synchronized with the commander's scheme of maneuver significantly, enhances situational awareness while increasing the precision of the targeting process. For more information about a line of bearing (LOB), a cut, and a fix, see paragraph 5-8.

3-39. Useful products G-2 (S-2) creates or assists in creating include—

- High-value target list (HVTL) during IPB.
- High-payoff target list (HPTL) during MDMP.
- Enemy electronic order of battle (EOB).

G-6 (S-6) STAFF

3-40. The CEWO uses the JRFL and friendly network architecture to plan EW and avoid EMI. The CEWO and the G-6 (S-6) use this information to develop the unit EP plan. The JRFL includes—

- Taboo frequencies.
- Protected frequencies.
- Guarded frequencies.

Taboo Frequencies

3-41. Taboo frequencies are friendly frequencies of such importance that must never be deliberately jammed or interfered with by friendly forces. Normally these include international distress, safety, and controller frequencies. They are generally long-standing frequencies, taboo frequencies may be time-oriented, and the restrictions may be removed as the combat or exercise situation changes. During crisis or hostilities, short duration EA may be authorized on taboo frequencies for self-protection to provide coverage from unknown threats or threats operating outside their known frequency ranges, or for other reasons. For more information about guarded, protected and taboo frequencies, refer to JP 3-13.1.

Protected Frequencies

3-42. Protected frequencies are friendly frequencies used for a particular operation, identified and protected to prevent them from inadvertent jamming by friendly forces while executing active EW operations against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless

absolutely necessary or until coordination with the engaged unit is made. They are generally time-oriented and may change with the tactical situation. It is important to update protected frequencies periodically.

Guarded Frequencies

3-43. Guarded frequencies are adversary frequencies currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the list changes as the adversary assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of the technical information.

STAFF JUDGE ADVOCATE

3-44. Conducting EW requires an understanding of the ROE and legal authorities. The CEWO consults the SJA for the standing ROE and interpretation. The SJA or representative reviews EW activities to ensure compliance with existing DOD directives and instructions, ROE, and applicable domestic and international laws, including the law of armed conflict.

3-45. When considering EA or ES, the SJA will assist in the planning of operations and will review past operations. As part of the assistance, the SJA considers what impacts operations may have on host nation communications and legal implications related to the impacts. Refer to FM 1-04 for more information on rules of engagement information and FM 3-12 for more information on authorities.

ELECTRONIC WARFARE CONTRIBUTIONS TO THE STAFF

3-46. The CEWO provides information to other staff sections to aid in planning. This information answers requests for information and aids in refining staff products.

Contributions to G-2 (S-2) Staff

3-47. The CEWO contributes to the IPB and throughout the MDMP by providing input related to EW activities. IPB involves systematically and continuously analyzing the threat and certain mission variables (terrain, weather, and civil considerations) in the geographical area of a specific mission. Commanders and staffs use IPB to gain information that supports understanding. Some of the CEWO's input to the IPB includes the following:

- Information regarding how the EME affects operational environments.
- Input to likely threat COAs by providing information on threat EMS capabilities, tactics, techniques, and procedures.

3-48. When evaluating how the EME affects an operational environment, the CEWO—

- Analyzes the EME and identifies known or suspected threat emitters of interest and neutral emitters in the area of operations.
- Identifies facilities, which may support, operate, or house enemy EW capabilities.
- Contributes to the G-2 (S-2) understanding of the enemy's use of the EMS.

3-49. When describing the effects of an operational environment on EW activities, the CEWO—

- Conducts terrain analysis of both the land and air domains using the factors of observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment.
- Identifies terrain that protects communications and target acquisition systems from activities. Terrain masking reduces friendly vulnerabilities to threat EW actions.
- Identifies how terrain affects LOS, including effects on both communications and noncommunications transmitters. *Line of sight* is the unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another (ATP 2-01.3).
- Evaluates how vegetation affects radio wave absorption and antenna height requirements.
- Locates power lines and their potential to interfere with radio waves.
- Assesses the likely air and ground avenues of approach, their dangers, and potential support that EW activities could provide for them.

- Determines how weather (including visibility, cloud cover, rain, and wind) may affect ground-based and airborne EW activities and capabilities (for example, when poor weather conditions prevent airborne EW launch and recovery).
- Assists the G-2 (S-2) staff with the development of the modified combined obstacle overlay.
- Considers all other relevant aspects of an operational environment that affect EW activities, using the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) and mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations).

3-50. The CEWO contributes to the G-2 (S-2) staff's understanding during enemy course of action development by providing—

- Subject-matter-expert input on enemy EW tactics, techniques, and procedures for situation template development.
- A review of named areas of interest and target areas of interest to confirm EW considerations.
- EW options to support decision points.
- EW input to the event template and event matrix.

Contributions to Other Staff

3-51. During planning, the CEWO provides information to other members of the staff including—

- EW input to IPB [G-2 (S-2)] staff.
- Input to the HPTL (Fires).
- Input to the commander's critical information requirements including essential elements of friendly information and priority intelligence requirements [G-2 (S-2) and G-3 (S-3)] staff.

FIRES

3-52. The targeting working group recommends priorities for the targets according to its judgment and the advice of the fires cell, targeting officer and the field artillery intelligence officer. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting working groups maintain a HPTL and inform the commander of targets that do not support the commander's guidance. The HPTL includes the recommended priority of targets and target engagement sequence. The HPTL includes the target category, a name, or a number.

3-53. The CEWO recommends to the G-3 (S-3) staff and the fire support element whether to engage a target with EW. The fires support element uses decide, detect, deliver, and assess methodology to direct friendly forces to attack the right target with the right asset at the right time. The targeting working group provides the HPTL to the operations, intelligence, and fires support element. The staff employs the HPTL to understand and determine attack guidance and to refine the collection plan. This list may also indicate the commander's operational need for battle damage assessment of the specific target and the time window for collecting and reporting it (ATP 3-60).

3-54. The CEWO integrates EW into the targeting process. After the targeting board has approved an EW target, the CEWO deconflicts the EW activity with the friendly use of the EMS. To support targeting, the CEWO—

- Matches EW resources with specific high-payoff targets and high-value targets.
- Ensures EW activities meet targeting objectives.
- Synchronizes EA with friendly use of the EMS.
- Coordinates with the SIGINT staff to gain targeting information that supports ES and EA.
- Provides EW mission management through the command post or joint operations center and the tactical air control party for airborne EA.
- Provides EW mission management as the EW control authority for ground or airborne EA when designated.
- Requests theater EW support.

- Informs the commander, staff, and subordinate units of current and planned locations of EW resources.

TARGETING

3-55. The CEWO integrates EA into targeting to achieve desired effects in support of unified land operations. The CEWO considers the variables of decide, detect, deliver and assess for targeting.

DECIDE

3-56. The decide function begins the targeting cycle by establishing the focus and priorities for targeting and information collection. The decide function for EW uses threat information from the CEMA and G-2 (S-2) sections including their tactics, techniques, and procedures. A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60).

3-57. The CEWO plans the integration of EW into standard targeting products identified by the fires cell. The planning products include the following—

- HPTL.
- Target selection standards.
- Attack guidance matrix.
- Target list worksheet.
- Annex C, Appendix 12 of the operation order.

DETECT

3-58. The targeting working group identifies high-payoff targets. The G-3 (S-3) tasks assets to detect the targets. The collection manager pairs assets to targets based on the collection plan. The CEWO coordinates with the collection manager to synchronize ES and SIGINT assets to detect high-payoff targets. ES and SIGINT assets provide data that includes the location of transmitters and receivers, transmitter signal strength, and frequencies used by the targeted receiver to deliver lethal or non-lethal fires against the target.

DELIVER

3-59. Once friendly force capabilities identify, locate, and track the high-payoff targets, the next step in the process is to deliver fires against those targets. EW assets deliver EA and may use ES or SIGINT resources to observe the effectiveness of the EA. ES and SIGINT assets also serve as observers when the commander directs lethal fires against enemy transmitters. Close coordination between those conducting SIGINT and EA is critical during the engagement. This coordination assists the CEWO in avoiding unintentional interruption of an ongoing SIGINT effort. The CEWO continually coordinates with adjacent unit CEWOs to mitigate and deconflict effects during cross-boundary operations.

ELECTRONIC WARFARE ASSESSMENT

3-60. EW assessment is continuously monitoring and evaluating the impact of EW on the current situation and the progress of an operation. CEWOs continually assess the current situation and progress of the operation and compare it with the concept of operations, mission, and commander's intent. Assessment occurs throughout planning, preparation, and execution; it includes three major tasks:

- Continuously identifying threat vulnerabilities and reactions to friendly EW activities.
- Continuously monitoring EW activities to ensure alignment with the commander's desired end state.
- Evaluating the operation against measures of effectiveness and measures of performance and making necessary adjustments.

3-61. The targeting working group synchronizes EW effects with other effects. The CEWO coordinates and synchronizes joint and multinational air and ground EW capabilities. The CEWO also manages the organic EW activities within the main command post.

MEASURES OF PERFORMANCE AND EFFECTIVENESS

3-62. The CEWO develops the measures of performance and measures of effectiveness for evaluating EW activities during execution. Measures of effectiveness measure the degree to which an EW capability achieved the desired result. Normally, the CEWO measures this by analyzing data collected by both active and passive means.

3-63. Measures of effectiveness help define whether a unit is creating the desired effect(s) or conditions in an operational environment. Example questions to measure EW effectiveness include—

- Did the EA disrupt enemy radar assets?
- Is the enemy radar retuning?
- Is there increased radio traffic on the radar command and control network?

3-64. Measures of performance help evaluate whether a unit is accomplishing tasks to standard. In the context of EW, example questions of measures of performance include—

- Is the EA asset transmitting at the necessary power?
- Is the EA asset transmitting in the required bandwidth?
- Is the EA asset transmitting using the correct polarization?
- Are all assets for a given mission operating in proper synchronization?

3-65. CEWOs use caution when selecting measures of effectiveness to avoid flaws in an analysis of the EW mission. For example, the lack of enemy electronic activity, such as communications or improvised explosive device initiation, does not necessarily mean it was the result of the EW mission; other factors may be the cause. Another example of a flawed measure of effectiveness is the premature conclusion that an EA degraded or disrupted a radio communication that resulted in an enemy commander not being able to direct the maneuver of subordinate forces using a specific frequency during a battle engagement. The enemy commander may have an alternate means of communication.

3-66. Effective EW Planning continues during all phases of an operation. The planning of EW requires significant preparation to achieve successful execution of EW tasks. The CEWO uses assessment techniques to measure success. Figure 3-1 on page 3-13 illustrates the CEWO’s use of decide, detect, deliver, and assess variables.

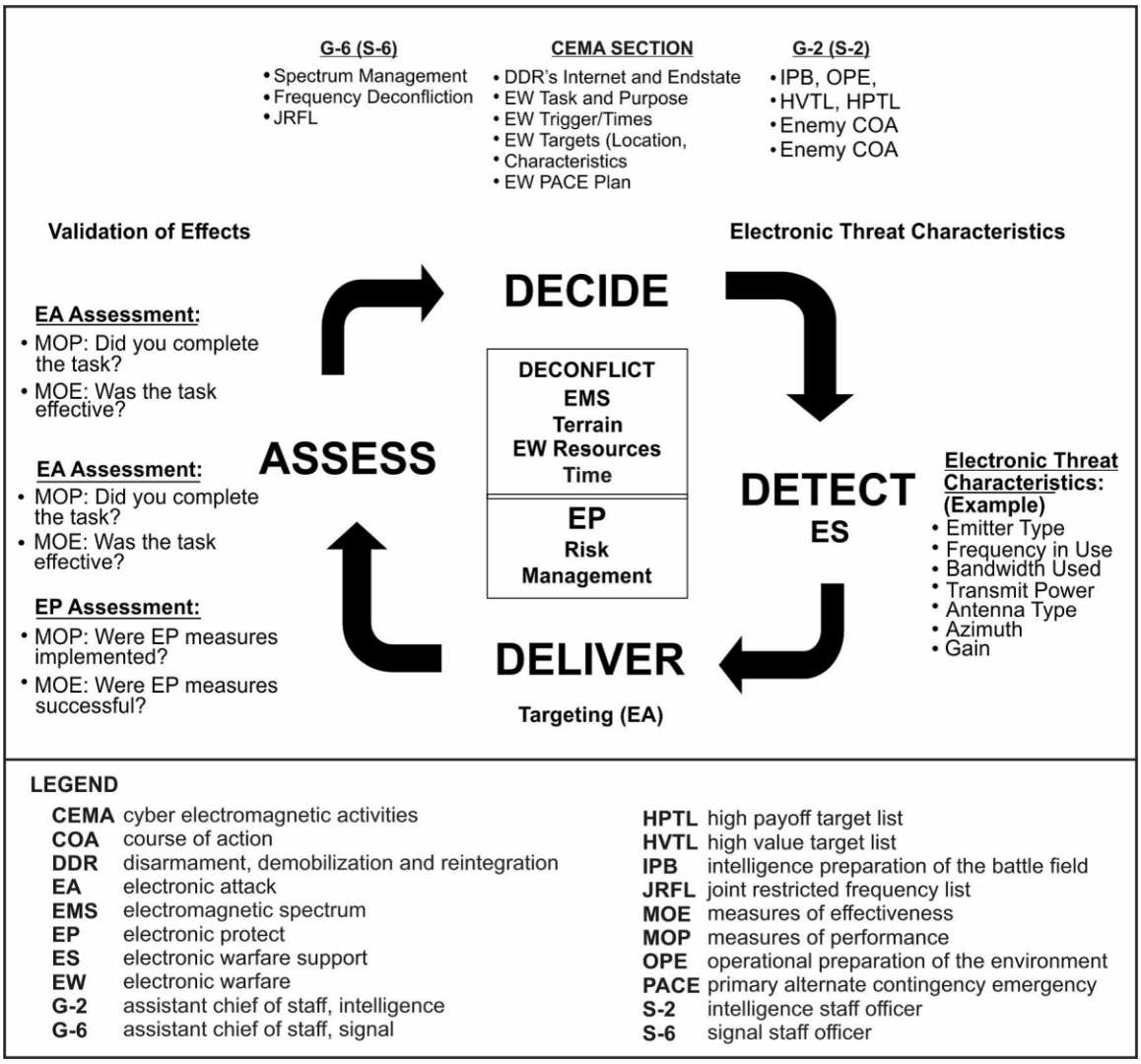

Figure 3-1. Electronic warfare in the targeting process

ELECTRONIC WARFARE EXECUTION

3-67. The CEWO addresses targets and employs EW assets in support of an operation. Targeting requires continuous involvement from the CEWO. After planning, the CEWO participates in the targeting board and assesses the effects using measures of effectiveness. During execution the CEWO—

- Prosecutes approved EW targets in support of the operation.
- Evaluates the effectiveness of EW.
- Maintains situational understanding of EW activities and associated effects.
- Oversees the movement and placement of EW assets in support of operational requirements.
- Continues to identify and assess risk.
- Receives information from EW assets and disseminates to the staff:
  - Detection and location of targeted and potential enemy emitters, including enemy EW assets.
  - Indicators and warnings of enemy activity from EW.
- Maintains direct liaison with the fires cell, G-2 (S-2) and G-6 (S-6) staff to ensure integration and deconfliction of EW activities.

- Coordinates and manages EW missions tasked to subordinate units and requests for nonorganic EW support.
- Continues to assist the targeting working group in target development and to recommend targets for attack and reattack.
- Anticipates EW equipment outages and initiates the capability replacement plan.
- Validates and disseminates cease-jamming requests.
- Coordinates and expedites EMI reports with the G-2 (S-2) and G-6 (S-6) staff for deconfliction.
- Serves as the EW controlling authority when designated.

3-68. The CEWO portrays radio wave propagation and EW effects using modeling and simulation techniques with software.

SPECIAL CONSIDERATIONS DURING EXECUTION

3-69. EMS resources are congested and contested with friendly and enemy use. EMS resource availability also shifts during an operation. The CEWO updates any changes within the EME and puts them into the common operational picture. During execution, EW planners continually consider—

- The EOB.
- The SOI.
- The JRFL.
- Anticipated or reported EMI.

Chapter 4

Electronic Warfare Preparation and Assessment

Preparation, execution, and assessment are interdependent parts of electronic warfare. This chapter discusses the techniques and resources to prepare, execute and assess electronic warfare effectively. This chapter provides electromagnetic spectrum resource coordination procedures and techniques to mitigate electromagnetic interference.

ELECTRONIC WARFARE PREPARATION

4-1. Peer threats continue to mature their command and control and EW capabilities. To overcome the adversary, units prepare for the contest to dominate the EMS. Preparation begins before arrival on the battlefield and continues through redeployment.

4-2. The EW professionals gain proficiencies in EW activities from a combination of military education, doctrinal references, and experience. EW preparation ensures timely support for the commander's scheme of maneuver. Preparation consists of activities that units perform to improve their ability to execute a mission. Preparation for EW includes—

- EW training that includes actual and simulated resources and environments.
- Maintenance activities to ensure that EW equipment is clean and serviceable.
- Practicing the MDMP with other members of the staff. Practicing MDMP fosters teamwork and establishes expectations regarding what the CEWO provides to, and receives from, the staff.
- Rehearsals that include the integration of SIGINT and EW resources and capabilities.
- Planning, initiating, and reporting movement of EW resources.
- Coordinating route clearance and escort requirements to mitigate risk and prevent delays during a maneuver.

4-3. During preparation, the CEMA section—

- Updates the EW running estimate in coordination with the SIGINT running estimate.
- Requests changes or exceptions to the JRFL and SOI through the G-2 (S-2) and G-6 (S-6) staff.
- Completes risk assessments and develops a risk mitigation strategy.
- Leads the CEMA working group.
- Develops and rehearses battle drills and staff processes including—
  - Staffing the EARF and measuring the effectiveness of EW activities.
  - Developing EW ground and airborne control authority procedures.
  - Integrating information collection activities [G-2 (S-2)] staff.
  - Coordinating for external maintenance and reprogramming support for EW assets.
  - Initiating EP procedures to counter EMI and enemy jamming actions.
  - Developing SOPs.
  - Establishing reporting procedures.
- Executes pre-combat checks and inspections of EW assets.

DECONFLICTING THE ELECTROMAGNETIC SPECTRUM

4-4. Deconflicting the EMS requires an understanding of the SOI, JRFL and mission requirements. The CEWO considers the distance, location and the purpose of equipment that is reliant on friendly or restricted

frequencies and recommends exceptions to the SOI or JRFL. The SOI contains call signs, call words, frequency assignments, signs, and countersigns for friendly forces. For more information regarding the SOI and JRFL, refer to ATP 6-02.70.

4-5. *Frequency deconfliction* is a systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management (JP 3-13.1).

4-6. Mission requirements may drive modifications to the SOI and JRFL. Modifications require staffing and approval through the G-2 (S-2) and G-6 (S-6) staff. For SOI and JRFL deconfliction, the CEWO considers the following—

- The purpose of the frequency.
- Waveform characteristics.
- Location and time of use.

Note. When EW activities conflict with the SOI or JRFL, the commander decides which has priority.

4-7. Due to security concerns, frequencies employed in intelligence roles may not be included in the SOI. The CEWO maintains awareness of the frequencies used in support of SIGINT activities through coordination with the G-2 (S-2) staff.

ELECTROMAGNETIC SPECTRUM RESOURCES

4-8. The authorization to use EMS resources is not always available. The G-6 (S-6) section spectrum manager uses the EMS certification process to gain the use of previously unallocated EMS resources, which requires completing a standard frequency action format.

4-9. Host nations have EMS usage plans that assist in the management of frequencies. The spectrum manager assigned to the G-6 (S-6) assists the CEMA section in frequency use authorization for EW activities. The G-6 (S-6) spectrum manager requests frequency resources through an online database. The online database enables managers to determine the historical EMS supportability of like systems. The hyperlink to the DD Form 1494, *Application for Equipment Frequency Allocation*, to request frequencies is in the references section of this publication. For more information about DD Form 1494 and frequency management, refer to ATP 6-02.70 and appendix C for information about spectrum management systems.

INTEGRATION OF ELECTRONIC WARFARE AND SIGNALS INTELLIGENCE

4-10. Integrating EW and SIGINT is a force multiplier for unified land operations. EW and SIGINT have similar capabilities that are mutually beneficial. Integrated EW and SIGINT assets present an efficient, holistic approach that reduces duplication of effort, enables additional information collection, and provides flexibility in the employment of EW and SIGINT resources. EW and SIGINT teams collaboratively use DF techniques to locate transmitters, achieving a higher level of fidelity on the location of emitters. Integration techniques take advantage of similar capabilities and the placement of EW and SIGINT resources to increase operational flexibility, such as co-locating capabilities. SIGINT teams can exploit enemy communications characteristics such as verbal content of a transmission and positively identify an emitter as an approved target. The SIGINT teams can inform the EW team for immediate target engagement.

DISTINCTIONS BETWEEN ELECTRONIC WARFARE AND SIGNALS INTELLIGENCE

4-11. Though EW and SIGINT are similar, there are important distinctions between them. Legal considerations distinguish EW and SIGINT activities, and the authorization for each to support operations, that if not observed, can complicate and delay the execution of electronic warfare effects and SIGINT operations. Commanders and planners should collaborate closely with the SIGINT enterprise and legal authorities to ensure compliance with SIGINT policy when planning electronic warfare.

SENSING ACTIVITY DISTINCTIONS

4-12. Commanders have the option to employ SIGINT sensors to support ES activities. The task and purpose are the main factors to decide to use SIGINT or ES capabilities. SIGINT sensors perform ES activities when used to provide immediate threat information including threat warning, avoidance, targeting, and jamming (refer to CJCSI 3320.01D). However, when the SIGINT sensor intercepts, identifies, and locates or localizes sources of intentional and unintentional radiated electromagnetic energy for intelligence purposes, it is no longer supporting an ES task but is conducting a SIGINT mission to satisfy intelligence requirements. These distinctions are identified when answering questions—

- Who tasks or controls the SIGINT sensors?
- What are the sensors tasked to provide?
- What is the purpose of the task driving the employment of the sensors?

4-13. ES and SIGINT employ the same or similar capabilities. ES includes actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations (JP 3-13.1).

4-14. Units retain some data from ES to support immediate threat recognition, targeting, and planning of future operations. Units transfer select data from ES activities to the United States SIGINT System for the production of foreign intelligence. Foreign intelligence is information that relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons (JP 2-0). The CEWO and the G-2 (S-2) staff develop a structured procedure within each echelon to facilitate information exchange. Units rehearse this procedure during exercises and pre-deployment planning.

4-15. ES includes the retention and processing of information for the search, intercept, identification, and location of electromagnetic radiation information. The CEWO protects and retains ES information in accordance with established policies and procedures (CJCSI 3320.01D).

This page intentionally left blank.

Chapter 5
Electronic Warfare Support Techniques

This chapter describes electronic warfare support planning, preparation, and execution techniques to include synchronizing signals intelligence resources to complement electronic warfare support activities. This chapter outlines a line of bearing, cuts, fixes, establishing a direction finding baseline, and what causes direction finding errors.

PLANNING ELECTRONIC WARFARE SUPPORT

5-1. Threat forces use the EMS to give orders, monitor and manage operations, detect aircraft using radar, and conduct DF. Locating threat transmitters aids in the development of situational understanding and assists with targeting. ES uses direction-finding techniques to find threat transmitters. Once located, the commander can direct fires in the form of lethal attack, request offensive cyberspace operations or use EA to gain the desired effects.

ELECTRONIC RECONNAISSANCE

5-2. Electronic warfare personnel conduct electronic reconnaissance to understand the types of threat emissions. *Electronic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-13.1). The CEWO acquires electronic threat characteristics from the G-2 (S-2). The electronic threat characteristics provide technical data including—

- Threat EMS resources in use.
- Antenna orientation and polarization.
- Radio transmit power levels.
- Radio range.

ELECTRONIC WARFARE SUPPORT CONSIDERATIONS

5-3. The task and purpose of the mission determine whether a SIGINT or EW asset is appropriate for a given mission. ES assets conduct immediate threat recognition, targeting, future operations planning, and other tactical actions such as threat geolocation for avoidance.

5-4. The adversary employs electronics security measures to prevent the detection of emitters. *Electronics security* is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar (JP 3-13.1). When the adversary employs electronic security measures, the CEWO may require assistance from SIGINT to understand the nature of the emissions.

PREPARING ELECTRONIC WARFARE SUPPORT

5-5. The CEMA section uses ES assets to scan the EME for transmissions and then illustrates the results in a manner that the commander and staff can understand. Units develop an electromagnetic environment survey using air, ground, and sea platforms. The G-2 (S-2) staff assists the CEMA section by developing and maintaining the electromagnetic environment survey (refer to FM 2-0). The electromagnetic environment survey aids the CEWO to understand the nature, limitations, and sources of EMI in an operational environment and plan the employment of ES equipment. The CEMA section submits requests for information to address information gaps to the G-2 (S-2) staff.

5-6. The electromagnetic environment survey provides input, and the CEMA section enters the information into automated tools to maintain a current environment survey.

EXECUTING ELECTRONIC WARFARE SUPPORT

5-7. The CEWO and G-2 (S-2) mutually develop the SOPs and battle drills for integration of EW support and SIGINT information collection activities. Integration techniques take advantage of similar equipment capabilities and fuse EW and SIGINT resources to increase flexibility. SIGINT teams pass targeting information to EW teams. The SIGINT DF equipment compliments geolocation efforts and transitions a LOB into a cut or a fix for targeting. Integration facilitates immediate sharing of information and reduces delays in targeting.

ELECTROMAGNETIC ENVIRONMENT SURVEY

5-8. Like weather reports for aircraft pilots, the EME survey informs the CEWO about the activities and conditions of the EME, enabling the CEWO to choose optimal COAs for EW.

5-9. EME surveys begin with the enemy EOB. The enemy EOB provides the CEWO with an initial overview of threat EMS capabilities derived from IPB. The enemy EOB assists the CEWO in making EW plans that exploit adversary vulnerabilities while preserving friendly capabilities. The enemy EOB is the baseline for the EME survey.

Electromagnetic Environment Survey

A unit tasks an airborne EW asset to support suppression of enemy air defense missions. During mission planning, the crew receives the EOB for the area of operations. The airborne EW crew identifies threat emitters they will likely encounter during the mission by priority, and de-conflicts friendly and neutral emitters.

As the airborne EW crew enters the target area of operations, they conduct an EME survey that confirms the presence of friendly, neutral, and threat emitters. Conducting and EME survey allows the crew to prioritize their activities against confirmed threat emitters by only targeting systems that are active.

DIRECTION FINDING

5-10. When conducting DF, the CEWO leverages the arrayed ES assets and coordinates support from the G-2 (S-2) for SIGINT resources to sense transmitters, collect information and triangulate the location of specified emitters of interest. The CEWO provides targeting requirements to the targeting board. Additionally, the CEWO shares the information collected from ES assets during DF activities with the G-2 (S-2). The G-2 (S-2) considers information derived from ES when developing intelligence.

5-11. DF provides LOBs, cuts, and fixes to locate transmitters. A LOB is a single approximate azimuth from a sensor providing the approximate azimuth to the transmitter. A cut is two approximate azimuths providing the general location of a transmitter by determining where two LOBs intersect. A fix is three or more approximate azimuths providing a location using a triangulation method. A cut or fix may use approximate azimuths from one sensor receiving the signal multiple times from different locations, or from different sensors. Figure 5-1 on page 5-3 illustrates a LOB approximate direction.

Note. The CEWO uses circular error probable ellipse in DF activities. For more information about circular error probable ellipse, see paragraph A-39.

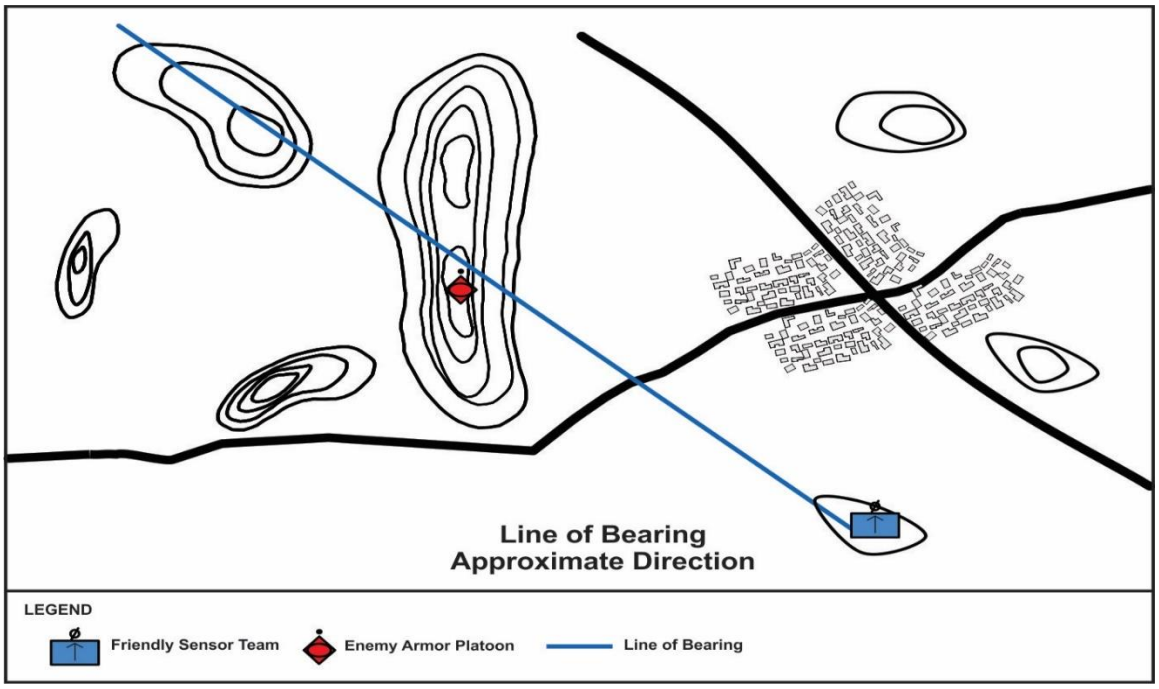

Figure 5-1. Example of a line-of-bearing

5-12. Figure 5-2 illustrates a cut general location.

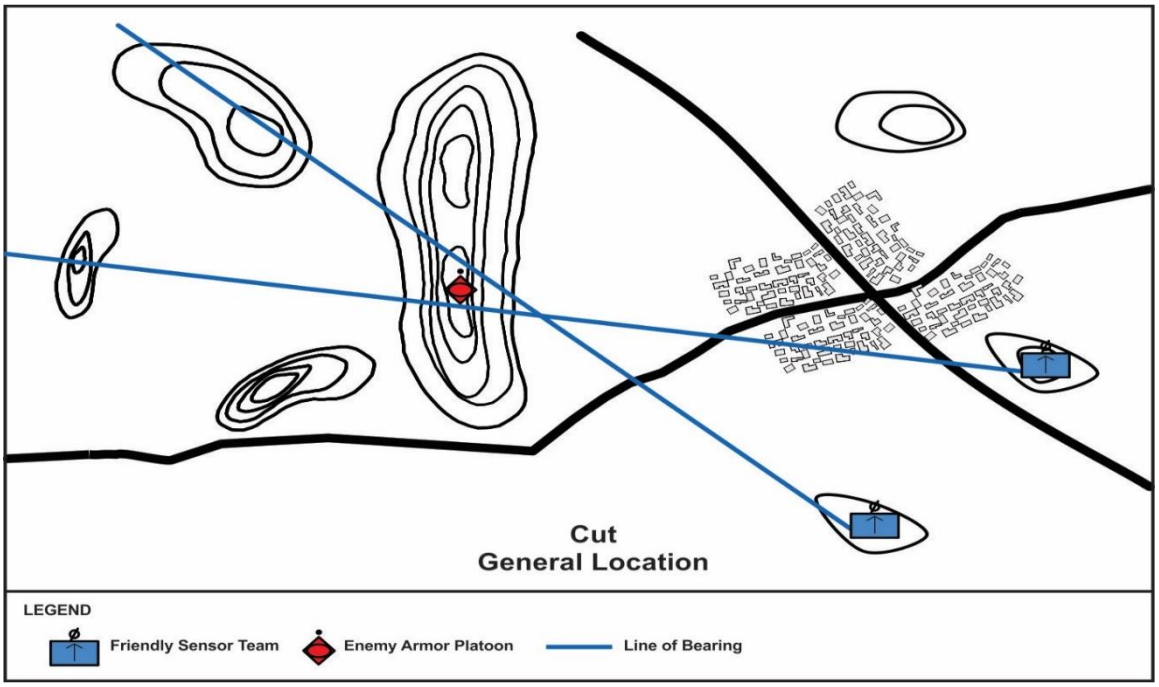

Figure 5-2. Example of a cut

5-13. Figure 5-3 illustrates a fix more precise location.

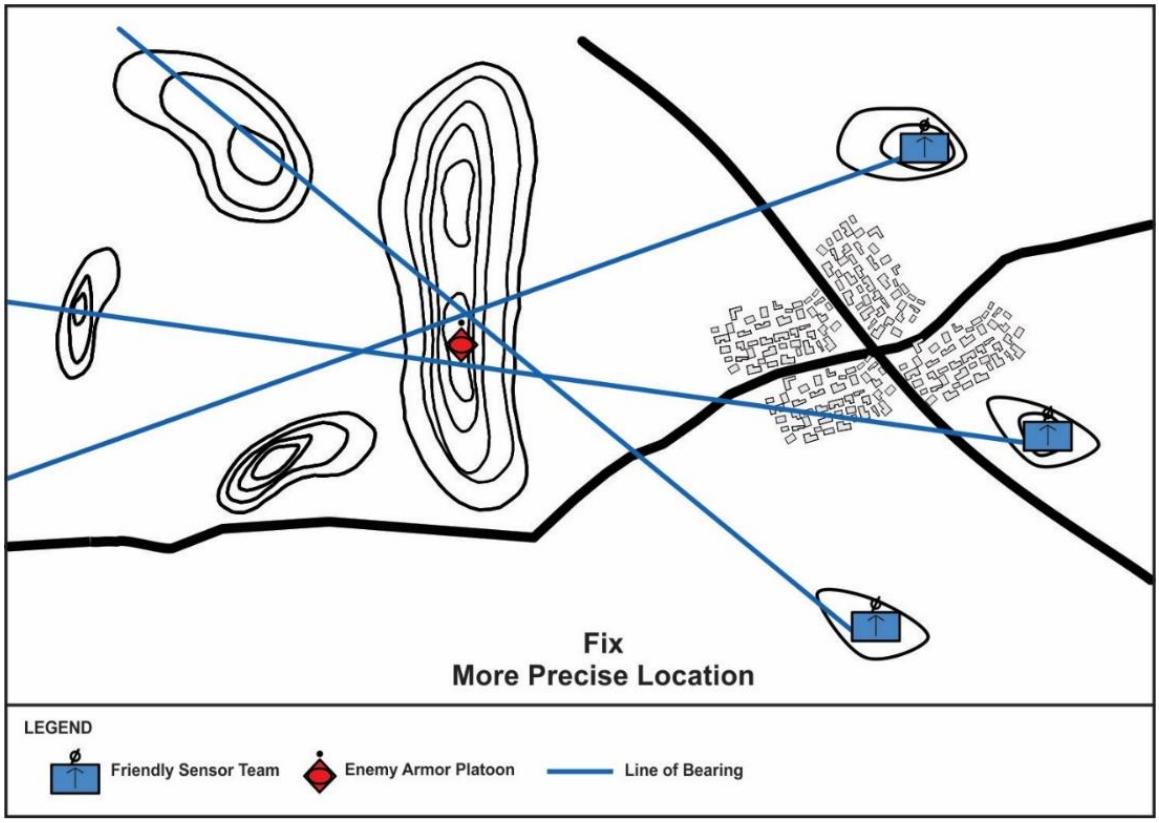

Figure 5-3. Example of a fix

Direction Finding Baselines

5-14. A ground-based DF baseline is that imaginary line or axis along which the DF equipment of a DF network deploy. A DF network consists of three or more individual DF sites. The establishment of a DF baseline is a matter of placing the DF equipment so that good bearing angles for triangulation within the target are possible. Triangulation is the intersection of bearings at the target area.

5-15. EW personnel ensure that each DF site has an unobstructed path between the DF antenna and any point in the target area. More often than not, the tactical situation precludes a clear path. EW personnel plan tactical DF baselines to ensure masked or hidden portions of the target area are still visible to at least three sites.

5-16. There are two types of baseline configurations used to establish a ground-based DF network—concave and convex. DF networks use concave baselines when the expected target location will be in a compact, narrow but deep frontal area. Concave baselines offer satisfactory bearings at longer ranges, and excellent triangulation at short ranges. See figure 5-4 on page 5-5 for an illustration of a concave baseline. Convex DF baselines provide reasonable azimuth angles over a wide front. Convex baselines will satisfy the average tactical or strategic situation.

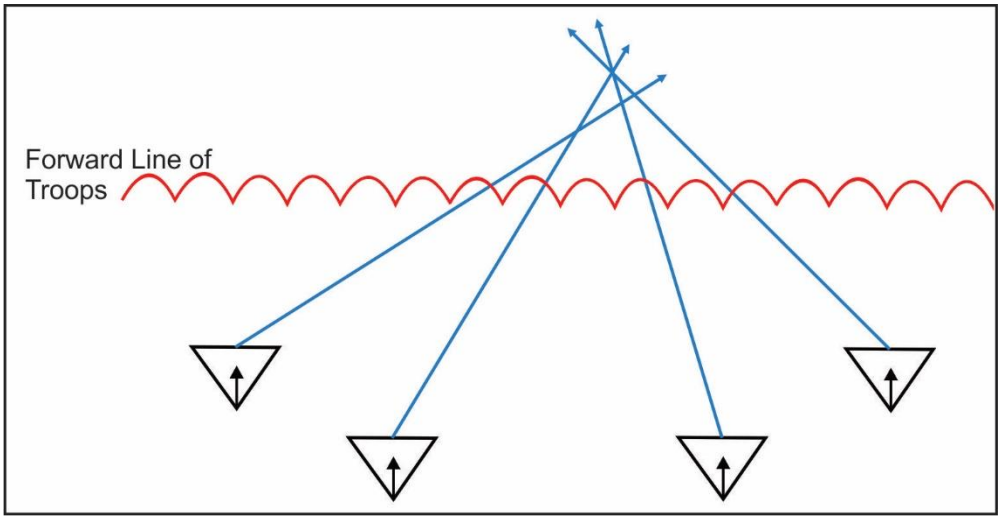

Figure 5-4. Concave baseline

5-17. See figure 5-5 for an illustration of a convex baseline.

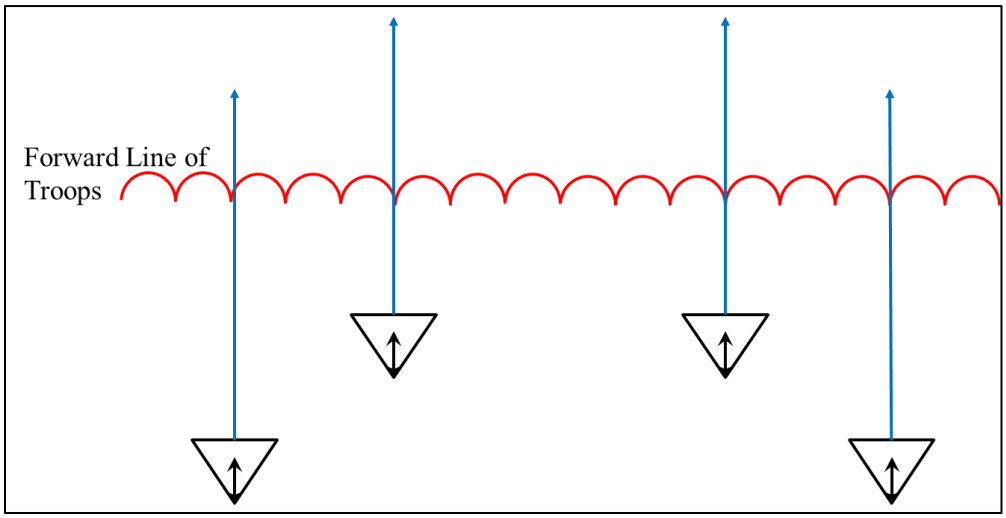

Figure 5-5. Convex baseline

Baseline Distance

5-18. The baseline distance is a straight-line distance that separates the two outermost DF sites. As a rule of thumb, the depth at which a DF network can effectively locate enemy transmitter antennas is equal to the total distance of the baseline joining the two outermost DF sites. This distance is from the center of the imaginary baseline to the target area. For example, if the DF baseline is 80 kilometers in length, the net fix location capability is 80 kilometers in depth.

5-19. Establishing a tactical DF baseline is dependent on the mission, enemy, terrain, troops, time, and civilians on the battlefield. Tactical commanders determine areas available for siting DF equipment within an area of operations. EW personnel dictate the baseline configuration employed in most situations. See figure 5-6 on page 5-6 for an illustration of baseline distance.

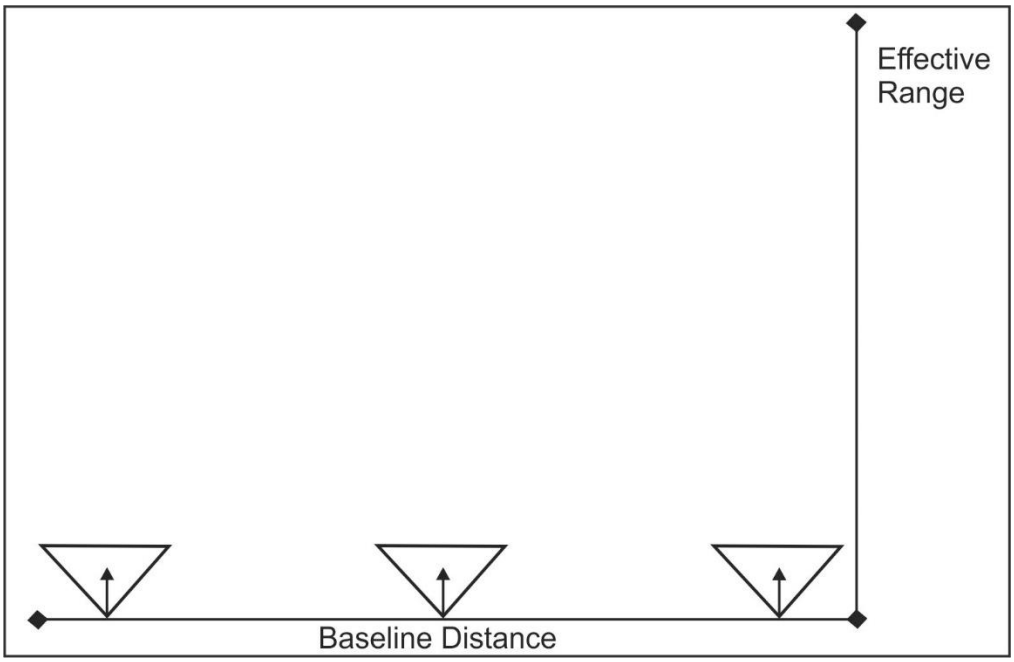

Figure 5-6. Baseline distance

PROBABILITIES AND ERRORS

5-20. The reception of a LOB on a target signal by a DF receiver does not always determine the exact azimuth to a transmitter. Because of weather and terrain effects on radio signals, the angle of the target signal varies upon arrival.

5-21. For DF missions, the further the receiver is from the transmitter, the greater the error associated with the intercept angle. When the CEWO plots the LOBs of three or more receiving stations on a map, there is a triangular area of overlap where the LOBs intersect to form a fix. A circle drawn with a radius that covers all the points of the triangle represents the location of the transmitter. The circle is the circular error probability. Because there is circular error probability, the precise location of the transmitter cannot be certain. Figure 5-7 on page 5-7 illustrates a circle error probability.

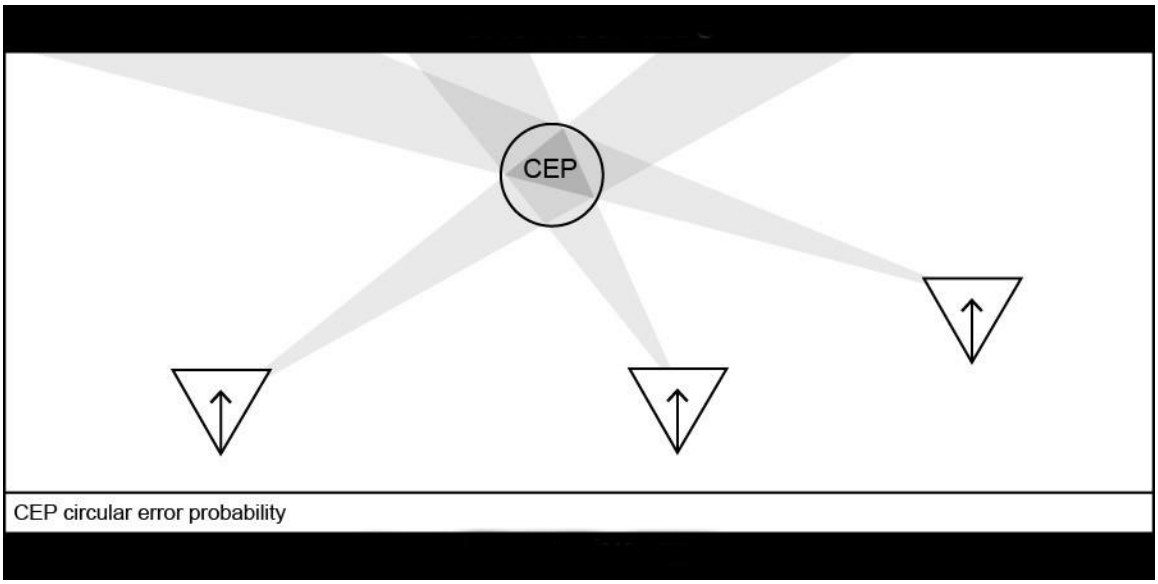

Figure 5-7. Circular error probability

5-22. The CEWO minimizes the circular error probability of a fix by using multiple LOBs of the same signal and plotting the angles to obtain location. The more LOBs used to obtain a fix, the smaller the circular error probability.

Errors Affecting Intercept Angles

5-23. The CEWO encounters errors that affect intercept angles. The following includes types of signal errors that affect the intercept angle when conducting DF missions—

- Source error.
- Path error.
- Polarization error.
- Site error.
- Instrument error.

Source Error

5-24. A source error is a disruption of radio waves introduced near the targeted transmitter. The type of directional antenna used or the terrain conditions at the antenna site may cause this type of error. If the DF equipment is farther than 15 kilometers from the transmitting antenna, the size of the source error is usually small. If the DF equipment is closer than 15 kilometers, the source error causes an inaccurate DF LOB.

Path Error

5-25. Deviations between the transmitter and DF system are path error. Important sources of path error include—

- Scatter.
- Refraction.
- Reflection.
- Reradiation.

5-26. For more information about path error, see appendix A.

Scatter

5-27. A small portion of the radio wave entering the ionosphere is scattered instead of bending and returning to the Earth's surface. A scattered wave projects in any direction, returning to the Earth at random angles. The scatter phenomenon accounts for signals sporadically received in skip zone regions. An error caused by scattering has a greater impact on strategic DF sites. An error caused by scatter has little impact on tactical DF sites. For more information about path error, see appendix A

Refraction

5-28. Refraction occurs when waves bend or refract from their normal path as they pass from one medium to another. For example, the velocity of a radio wave over salt water is greater than its velocity over land or fresh water. When a radio wave crosses a coastline at an oblique angle, as illustrated in figure 5-8, it changes direction. Refraction error is evident when either a DF site or the transmitting antenna is near the coast. This effect also varies with the transmission frequency.

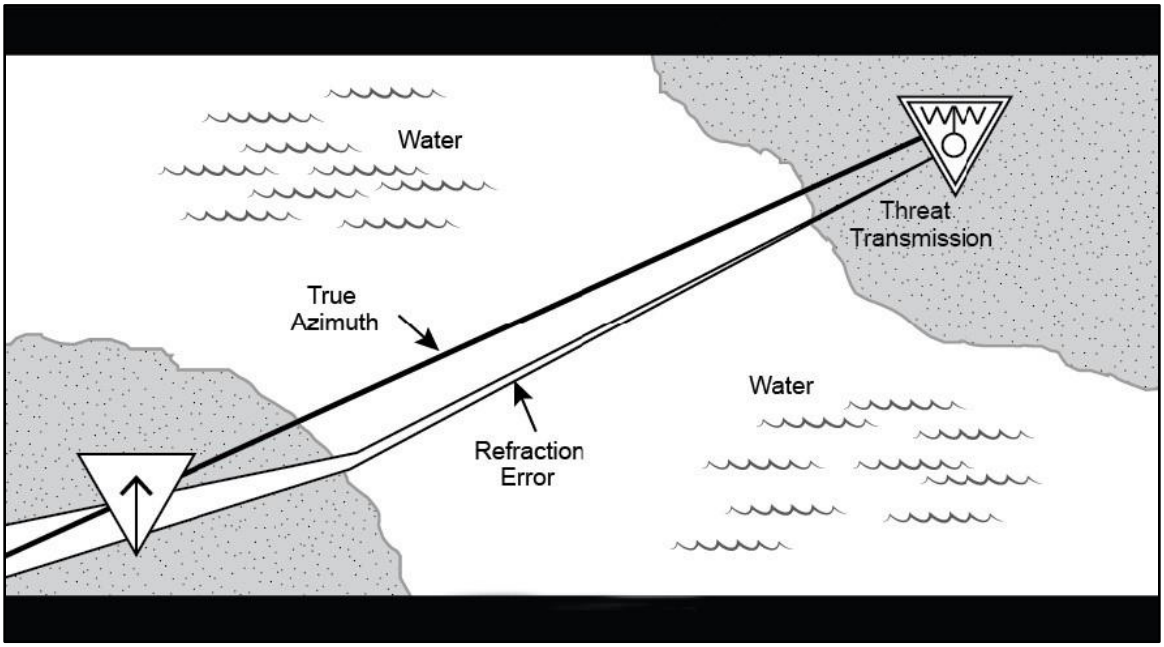

Figure 5-8. False azimuth indicated by refraction error

Reflection

5-29. Reflection occurs when radio waves strike and reflect off an artificial or natural surface (see figure 5-9 on page 5-9) illustrates the reflection of a radio wave. The degree of reflection is not measurable as it depends upon the obstruction and the frequency of the transmitted wave. Generally, DF errors are greatest from reflection when the reflecting mediums are located near the transmitter or the DF equipment. Reflection error affects strategic and tactical DF systems.

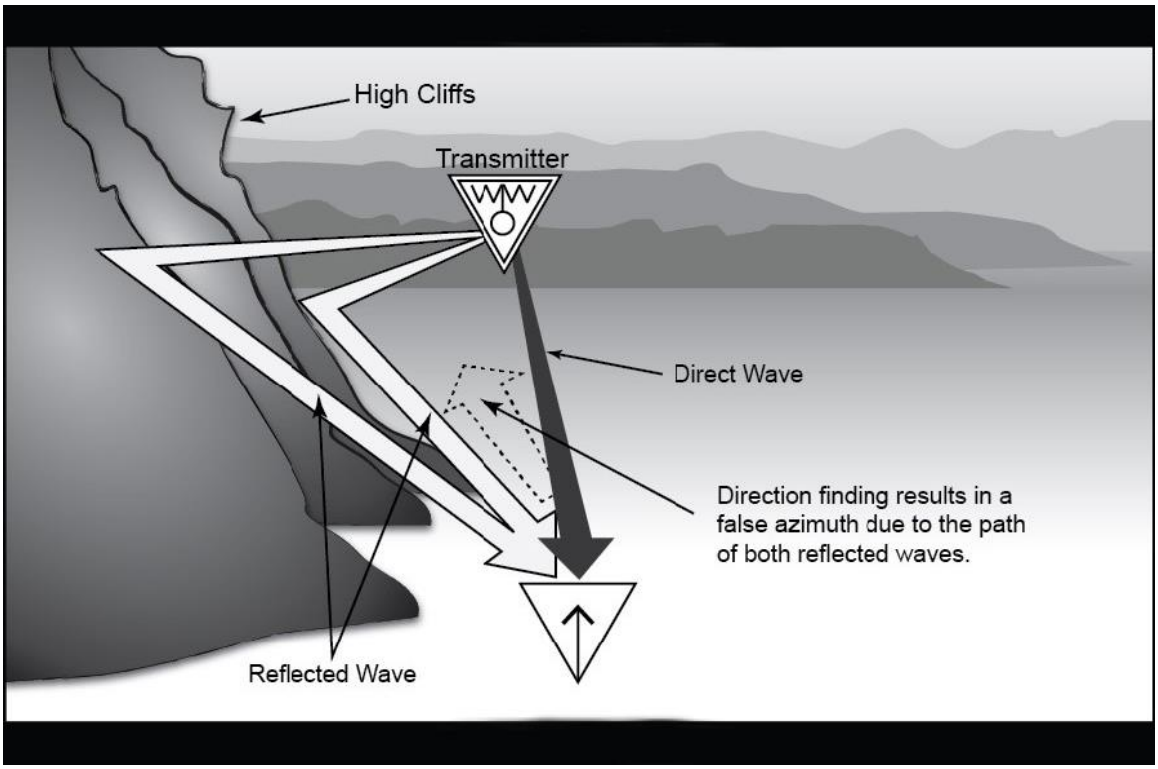

Figure 5-9. Reflection of a radio wave

Reradiation

5-30. Reradiation occurs when a wave strikes a metallic object that resonates at the wave's frequency. Abnormally polarized, reradiated signals make it difficult for DF equipment to determine an accurate azimuth. Reradiation error occurs near the DF site. Barbed wire, trucks, tanks, other combat vehicles, and metal buildings can cause a reradiation error. At DF sites, it is essential to consider obstacles when selecting sites for missions. For more information, refer to ATP 2-22.6-2 and appendix A.

POLARIZATION ERROR

5-31. Polarization error occurs when a DF antenna receives an undesired voltage induced by component of a radio wave. This undesired voltage blurs the bearing and makes an azimuth reading difficult to determine. For example, a DF antenna, such as a vertical loop, receives vertically polarized radio waves. If the received wave is abnormally polarized, the voltage induced by the two components may combine. The azimuth reading on the signal is difficult, if not impossible, to determine. The polarization error effect depends on the DF antenna's ability to discriminate between the vertically polarized wave and the horizontally polarized wave of the received signal. Polarization error is common in most DF activities. For more information, see appendix A.

SITE ERROR

5-32. Site error occurs in the immediate vicinity of the DF site. The proper orientation of the antenna is critical to obtaining accurate DF; therefore, at each new location, the operator precisely orients the antenna to a known reference point such as true north. Adapting the antenna reference point produces an accurate measurement of the arrival angle of the wavefront. Obstructions near DF sites contribute to a site error. The closer the obstruction is to the DF site, the greater its adverse effect on the accuracy of the site's LOBs.

INSTRUMENTATION ERROR

5-33. Poor maintenance or improper calibration of DF equipment results in instrument error. DF equipment requires calibrations and adjustments at regular intervals. Maintenance, calibrations, and equipment adjustments, improve performance and achieve accurate DF results. These procedures are available in associated DF equipment technical manuals (ATP 2-22.6-2).

Chapter 6
Electronic Attack Techniques

This chapter discusses the techniques for conducting electronic attack and describes their characteristics. Electronic attack enables the commander to dominate the electromagnetic and supports the scheme of maneuver during Army operations.

PLANNING ELECTRONIC ATTACK

6-1. Commanders use EA to affect threat communications and noncommunications capabilities and for defense. EA is a single action or supplements other lethal or nonlethal attacks. Dynamics in an operational environment require the CEWO to employ different EA techniques based on operational variables. EA techniques include countermeasures and electromagnetic deception. Army operations employ offensive and defensive EA such as—

- Jamming adversary radar or command and control systems.
- Using antiradiation missiles to suppress adversary air defenses.
- Using electronic deception to confuse adversary surveillance and reconnaissance systems.
- Employing self-propelled, towed, or stationary decoys.
- Using self-protection and force protection measures such as use of expendables (e.g., flares and active decoys)
- Employing directed energy or infrared countermeasures systems.

6-2. EA includes both offensive and defensive activities. Offensive EA disrupts or destroys threat capability. Defensive EA protects friendly personnel and equipment. When planning EA, the CEMA section, in conjunction with the staff consider—

- Interference of friendly communications.
- Intelligence gain or loss.
- EMS use by locals and non-hostile parties.
- The persistence of effects.
- Electronic signatures.

6-3. EA depends on ES and SIGINT to provide targeting information and battle damage assessment. Throughout the MDMP and the targeting process, the CEWO coordinates and deconflicts spectrum requirements with the CEMA working group. Refer to JP 3-13.1 for more information about EA and defensive EA planning.

ELECTRONIC ATTACK EFFECTS

6-4. EA denies the enemy or adversary the ability to use the EMS, use equipment, or affects personnel and their decision making or courses of action. The effects that EA creates include denying, destroying, degrading, deceiving, delaying, diverting, neutralizing, or suppressing enemy or adversary EMS capabilities. These effects are mutually exclusive, and these terms are common when describing the desired effects. There may be other terms appropriate to describe desired effects other than those listed. For more information on effects, refer to JP 3-60.

6-5. The different EA systems have varying capabilities. The EW personnel planning and employing the variety of systems consider each of the system-specific parameters, the environment, and mission requirements. Each system has specific capabilities and may require ingenuity during planning to ensure mission success.

ELECTRONIC ATTACK CONSIDERATIONS

6-6. The CEMA working group plans and rehearses EMS deconfliction procedures. When EA conflicts with the G-2 (S-2) information collection efforts, the commander decides which has priority or the G-3 (S-3) decides based on commander's guidance.

6-7. The potential for threat intelligence collection also affects EA planning. A well-equipped adversary can detect EA by employing ES techniques to gain intelligence on U.S. force locations and intentions. To develop an understanding of the adversary's intelligence collection capability, the CEWO and the G-2 (S-2) staff develop the enemy EOB. CEWOs protect EA assets through EP and risk mitigation techniques to counter threat ES and EA. For more information about EP, see chapter 7.

6-8. A red team provides an independent capability to explore alternatives in plans and operations in the context of an operational environment and from the perspective of enemies, adversaries, and others (JP 2-0). In conjunction with the red team, the CEWO and the G-2 (S-2) staff determine what intelligence the adversary can gain.

Threat Electronic Warfare Persistence

6-9. Aside from antiradiation missiles, the effects of jamming are less persistent than effects achieved by lethal means. The effects of jamming persist as long as the jammer itself is emitting and is in range to affect the targeted receiver. These effects last a matter of seconds or minutes, which makes the timing of such missions critical. Timing is important when units use jamming in direct support of aviation or ground platforms. For example, in a mission that supports suppression of enemy air defense, the time on target and duration of the jamming must account for the speed of attack of the aviation platform. They must also account for the potential reaction time of threat air defensive countermeasures. Because jamming may cause the threat to take unexpected actions or use other means of communications to avoid the intended effect, the CEWO uses ES techniques to sense and validate the persistence of known threat transmissions.

Electronic Attack to Destroy

6-10. An electromagnetic pulse creates a permanent effect and destroys equipment rendering it useless until the threat repairs or reconstitutes the capability. An *electromagnetic pulse* is the electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges (JP 3-13.1). Units at echelons theater army and below seeking to destroy a target using an electronic pulse rely on strategic level decisions and support to achieve this effect.

Countermeasures

6-11. The Army uses countermeasure techniques to mitigate threat EW sensing and attack activities. *Countermeasures* are that form of military science that, by the employment of devices and techniques, by design impairs the operational effectiveness of threat activity (JP 3-13.1). Countermeasures can be active or passive and deployed preemptively or reactively. Countermeasure devices and techniques include flares, chaff, radar jammers, CREW systems, and decoys. Chaff is radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion (JP 3-13.1).

Electromagnetic Deception

6-12. Deception mission techniques include misleading transmissions that present false indications of friendly force battle rhythms. Control and coordination are necessary to avoid confusing friendly activities with deception missions. When planning an electromagnetic deception mission, the EW planners consider activities that support the current, friendly operation as well as those that will support the deception mission and perform integration and deconfliction. EW supports all deceptions plans, both military deception and tactical deception, using the electromagnetic deception and scaling appropriately for the desired effect. Electromagnetic deception is the deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information

to an adversary or to adversary electromagnetic dependent weapons, thereby degrading or neutralizing the enemy's combat capability (JP 3-13.1). Electromagnetic deception can increase or decrease ambiguity affecting the enemy decision maker's understanding. This can prove to an enemy commander the certainty of a course of action or create confusion on their behalf.

6-13. The G-3 (S-3) staff plans and supervises deception missions. The information operations officer develops deception plans. Integration of electromagnetic deception with information operations is necessary when conducting deception missions. EW supports information related capabilities and deception plans using electromagnetic deception techniques. The CEWO is responsible for the EW portion of the deception plan.

6-14. Time is a critical factor in deception planning. A deception plan intended to deceive the adversary for two or three days usually includes a well-coordinated electromagnetic deception that uses as many friendly transmitters as reasonable. Regardless of the duration, the adversary's ability to detect emitters is essential to the success of an electromagnetic deception. False emissions require—

- A frequency that is compatible with threat receivers.
- Signals strong enough to reach threat sensors.
- Modulation techniques employed and detected by threat equipment.
- Planning and deconfliction for electromagnetic deception broadcast locations.

6-15. Each piece of electronic and associated equipment has an electronic signature. The unit executing deception presents the signatures to the threat providing a false environment. The three types of deception are—

- Simulative electromagnetic deception.
- Manipulative electromagnetic deception.
- Imitative electromagnetic deception.

Simulative Electromagnetic Deception

6-16. Simulative electromagnetic deception attempts to represent friendly notional or actual capabilities to mislead threat forces. Simulative electromagnetic techniques require extensive command and staff collaboration to present a believable deception plan. What the threat detects electronically should be consistent with other sources of intelligence reports. Simulative electromagnetic deception transmissions require close attention. Electromagnetic deception effects are often of short duration.

6-17. Simulative electromagnetic deception includes the use of systems that give off emissions indicative a particular organization. A counter-mortar or counter-battery radar is organic to an artillery unit. By turning on that type of radar, you can identify the probable location of an artillery unit. Simulative electromagnetic deception also includes using emitters to imply a type or change of activity by a unit, for example, placing surveillance radars in a typical defensive array, when in fact the intent is to attack.

Manipulative Electromagnetic Deception

6-18. Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit is going to attack when it is going to withdraw, the unit might transmit false plans and requests for ammunition. CEWO's use manipulative electromagnetic deception to mislead the enemy to misdirect their EA and ES assets, while interfering less with friendly communications. Manipulative electromagnetic deception seeks to eliminate, reveal, or convey misleading indicators of friendly intentions. Success in manipulative electromagnetic deception and simulative electromagnetic deception depends on understanding how friendly transmitters appear to the threat. The EW planners consider what is occurring with the friendly transmitters. Then the EW planners determine how to portray the friendly command's transmission infrastructure (JP 3-13.1).

Imitative Electromagnetic Deception

6-19. Imitative deception mimics threat emissions with the intent to mislead them. Imitative electromagnetic deception, if recognized by the enemy, can compromise SIGINT efforts. Imitative deception normally requires approval from higher echelon commands.

6-20. An example of imitative electromagnetic deception includes entering the adversary's communication nets by using their call signs and radio procedures and then giving threat commanders instructions to initiate actions, which are to the advantage of friendly forces. Targets for imitative electromagnetic deception include any threat receiver and range from cryptographic systems to plain-language tactical nets. Imitative electromagnetic deception can cause a unit to be in the wrong place at the right time, to place ordnance on the wrong target, or to delay attack plans. Imitative deception efforts foster decisions based on false information that, to the enemy, appears to have come from within. Imitative electromagnetic deception can be decisive on the battlefield. However, to be effective, imitative electromagnetic deception requires electronic equipment capable of convincingly duplicating the emissions of enemy equipment (JP 3-13.1).

PREPARING ELECTRONIC ATTACK

6-21. In preparation for EA, the CEWO gathers target information from ES sensors and the EOB. The information includes the location of the targeted asset, electronic characteristics, and the frequencies in use. Using location, characteristics and frequency, the CEWO determines which assets are best to conduct EA. The CEWO then completes calculations to determine the power required to jam the targeted receiver. The CEWO gives guidance to subordinate units about EA. The guidance includes information that allows the subordinate unit to prepare for the EA. EA guidance includes—

- Target identification.
- Target location.
- Special coordination requirements and procedures.
- Jamming technique.
- Jamming duration.
- Desired effect.
- Battle damage assessment method of delivery and prescribed format.

Note. The CEWO uses formulas to determine minimum power output requirements used for targeting. Appendix A includes the formulas for calculating minimum power output.

ELECTRONIC ATTACK REQUESTS

6-22. EARFs include brevity codes and procedures. Units develop SOPs for EA requests and incorporate the standard format referred to as an EARF. Refer to ATP 3-09.32 and appendix D for more information about the EARF.

6-23. The objective of EA is to disrupt or degrade the threat's ability to receive electromagnetic signals radiating from their transmitters, or process signals from other sources, such as friendly transmissions, with confidence. CEWOs integrate EA into the tactical plan by coordinating with the targeting board and the CEMA working group. The targeting list is an output from the targeting board and specifies the targets and times of attack regardless of the method used. When preparing for EA, the CEWO considers—

- The commander's intent.
- The ROEs.
- The location and identity of the targeted receiver and associated transmitter.
- The electronic threat characteristics of the targeted receiver and associated transmitter.
- The target engagement calculations.
- The associated risk when targeting with EA.

6-24. The CEWO makes coordination with the staff to plan EA. The G-2 (S-2) staff provides electronic threat characteristics to aid in the development of targets. The electronic threat characteristics include the technical characteristics of the target. The CEWO maintains electronic threat characteristics for future targeting efforts. Threat characteristics regarding targets include—

- Threat's unit or organization.
- Frequencies in use.
- Call signs.
- Location.
- Power of transmitters.
- Bandwidth.
- Equipment nomenclature.
- Modulation type.
- Multiplex capability.
- Pulse duration.
- Pulse repetition frequency.
- Antenna type.
- Antenna height.
- Antenna orientation.
- Antenna gain.

6-25. The CEWO determines the minimum power output required to attack the target receivers. Excessive EA power makes it easier for the threat to locate and attack the friendly EA asset. Distances between the threat transmitter and receiver and the friendly EA asset are critical considerations for EA asset placement.

6-26. Terrain is a factor because LOS is necessary between the EA asset and the location of the targeted receiver. The adversary uses terrain to mask transmitted signals from friendly detection and attack. Other terrain considerations include—

- Urban infrastructure.
- Bodies of water.
- Soil composition.
- Vegetation density.

ELECTRONIC ATTACK CONSIDERATIONS

6-27. The selection of EA assets is a significant factor when preparing to conduct EA. EA considerations include—

- Concealment characteristics.
- Power output capability.
- Availability of physical protection.
- Time available for the mission.
- Route clearance and escort requirements to conduct friendly maneuver.
- Augmented security coordination.
- Airspace considerations for airborne EW assets.

EXECUTING ELECTRONIC ATTACK

6-28. The CEWO has multiple options to choose from when executing EA. The CEWO prosecutes EA from air and ground (including fixed and mobile) platforms and monitors the EA activities during the mission. Mobile platforms consist of vehicular mounted and dismounted configurations. Units conduct EA using the chosen jamming technique and report the results of the jamming efforts to the CEWO.

CLOSE AIR SUPPORT

6-29. Close air support (CAS) delivers EA using a variety of air platforms. There are two types of CAS requests: preplanned and immediate. The CEWO reviews the air tasking order (ATO) calendar when resourcing EA requirements. When CAS is available, the CEWO submits a request to use CAS for the EA mission.

6-30. The air support operations center provides the ATO calendar, which has detailed information on aircraft, crews, and missions. Preplanned CAS requests occur during planning. The ATO calendar is broken down into 24-hour duty cycles. The specific theater or joint operations area supporting joint air operations command and control center will establish cut-off times to receive preplanned air support requests for inclusion in the ATO. Immediate air support requests arise from situations that develop outside the planning stages of the joint air tasking cycle. It is important to understand that air assets available to satisfy immediate air support requests already exist in the published ATO. For more information about CAS and the ATO calendar, refer to JP 3-09.3.

AIRBORNE ELECTRONIC ATTACK

6-31. Airborne EA delivers jamming from rotary, fixed-wing and unmanned aircraft systems. Although some of these platforms are organic to the Army, much of the airborne EA capability resides in other Services. Requesting airborne EA often requires coordination with joint forces. Effective airborne EA requires integrating procedures and communications between the supported unit and the airborne EA asset owner. The EARF includes the prescribed communications method.

6-32. Communications between the aircrew, CEWO, and JTAC throughout the mission is beneficial for maintaining situational understanding and for retasking an asset. Best practices include active communications between the CEWO and the aircraft that is delivering the EA.

6-33. When the CEWO cannot communicate with the aircrew or the JTAC, the supporting aircraft continues with the airborne EA mission specified in the EARF. A technique is to note in the EARF regarding what to do in the event of a communication failure (FM 3-12).

Canceling and Retasking Airborne Electronic Attack

6-34. Changes within an operational environment and EA missions make it necessary for reprioritization of assets. Air platforms are in demand for other purposes such as surveillance supporting intelligence missions or signal missions. The CEWO can request dynamic retasking of airborne EA assets and requests retasking with the JTAC and the air operations center.

Joint Tactical Attack Controller

6-35. The JTAC conducts air and ground coordination. The JTAC initiates requests and maintains communications with the designated airborne EA point of contact for the duration of the mission.

Air Operations Center

6-36. The air operations center, which can be joint or allied depending on the task organization, coordinates all assigned aerospace forces. The air operations center conducts the following activities—

- Coordinates and approves airspace.
- Coordinates aerial refueling.
- Makes ATO changes.
- Issues retasking instructions.

Airborne Electronic Attack Cancellations at the Battalion and Brigade

6-37. Sometimes it is necessary to cancel airborne EA missions. CEWOs communicate cancellations to the asset owner and requestor points of contact. Reporting cancellations ensures the most efficient use of EA assets and availability for other missions.

Advanced Cancellation of Preplanned Mission

6-38. When a CEWO cancels an airborne EA mission more than six hours before a preplanned mission is a routine task. The requestor includes the reason for cancellation. The CEWO immediately communicates a cancellation of a mission to release the airborne EA asset for other missions. The CEWO also notifies the

fire support officer and the air liaison officer. Cancellations made during operations include direct voice communications when possible to ensure someone is available and ready to process the cancellation.

Short Notice Cancellation of Preplanned Mission

6-39. Short notice airborne EA cancellations are cancellations that occur less than six hours before a preplanned mission. Short-term cancellations require immediate action to avoid mission launch and the unnecessary employment of an asset. The CEWO informs the designated point of contact that a cancellation is coming by the most expeditious means available. Following the initial notification, the CEWO sends the official cancellation joint tactical air strike request (JTASR) to the appropriate point of contact as soon as possible. Since the cancellation may require communications that bypass normal chain of command relationships, CEWOs include the process in the written unit SOPs and battle drills.

Immediate Cancellation of Preplanned Mission

6-40. CEWOs use this technique for canceling missions within one-hour of the expected execution time. CEWOs use the fastest communication means possible, such as Internet relay chat or voice communications, to distribute the necessary cancellation information. Immediately following an immediate cancellation, CEWOs contact the prescribed point of contact and provide an official cancellation using the points of contact on the JTASR and EARF to ensure units receive information promptly. Effective units include this process in the unit SOP and battle drills.

Dynamic Retasking

6-41. The staff makes every effort to provide immediate EA in response to an urgent request, including the allocation of available airborne EA assets. The retasking of airborne EA assets fulfills requests for on-demand requirements.

6-42. The process for retasking airborne EA platforms varies depending on joint command and control and Army mission command arrangements, task organization, force disposition, and unit boundaries. The requesting unit submits a request to their supporting EW representative. The retasking format is available in ATP 3-09.32.

6-43. If the requesting unit previously submitted a JTASR for EA support, the CEWO modifies the existing JTASR with a numbered change. Some units make the change using red for easier identification. If the requesting unit has not submitted a JTASR for the mission, the CEWO creates a new JTASR. The CEWO provides status updates to the requesting unit. Effective units address the knowledge management processes for maintaining updated JTASRs in their SOPs and battle drills.

6-44. Due to the dynamic nature of an urgent requirement, there is no way to calculate the amount of time needed for coordinating the airborne EA. The CEWO or JTAC notifies the appropriate EW representative and air support operations center when it is apparent that the duration of EA will exceed the initially anticipated time. The air support operations center notifies the airborne EA asset and coordinates any additional fuel requirements or determines the need to re-task another airborne EA asset. The air support operations center then informs the CEWO and JTAC of what support to expect. The JTAC or CEWO contacts the air support operations center to release airborne EA assets upon mission completion or cancellation.

JAMMING TECHNIQUES

6-45. CEWOs use jamming techniques to disrupt the threat's ability to effectively receive or process electromagnetic signals by overcoming the threat receiver with higher power transmissions. Successful jamming of receivers requires an understanding of available jamming techniques. CEWOs consider which technique is appropriate to support the commander's intent. Jamming techniques include—

- Electromagnetic jamming.
- Electromagnetic intrusion.
- Electromagnetic pulse.
- Electronic probing.

Electromagnetic Jamming

6-46. CEWOs apply jamming techniques as an alternative to lethal fires or in conjunction with lethal fires. *Electromagnetic jamming* is deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability (JP 3-13.1).

6-47. The primary effects of jamming persist when the jammer is within range of the target and emitting. Effects of jamming are evident in the actions of the adversary during or following the EA mission. The CEWO can use differing jamming techniques to support EA. Jamming techniques include—

- Standoff jamming.
- Escort jamming.
- Spot jamming.
- Sweep jamming.
- Barrage jamming.
- Follower jamming.

Standoff Jamming

6-48. Standoff jamming supports operations by disrupting or degrading threat command and control systems and sensors that operate in the EMS. A standoff jamming mission projects from a stationary and protected location within a friendly area of operations. Standoff jamming—

- Affords maximum protection to EW professionals and the systems they deploy from threat actions.
- Generally requires high power and large antennas to provide reach deep into an adversary's area of operations.
- Requires precise intelligence on threat frequencies and receiver locations to maximize jamming effects promptly.
- Creates windows of opportunity for Army and joint forces to conduct maneuver.

Escort Jamming

6-49. Escort jamming supports friendly operations when the jamming platform accompanies maneuver forces. Escort jamming is defensive in nature and protects maneuver forces from threat weapons systems that use RF receiving triggers. Successful escort jamming requires precise intelligence regarding threat use of frequencies. Escort jamming usually does not require the same level of power or large antennas as standoff jamming. Escort jammers use similar vehicle configurations of maneuver vehicles to screen them from visual identification.

Spot Jamming

6-50. The CEWO can conduct EA by jamming one specific frequency using a technique referred to as spot jamming. Spot jamming is the least intrusive form of EA, as it does not jam untargeted frequencies. The CEWO requires specific electronic threat characteristics to plan and execute spot jamming successfully.

Sweep Jamming

6-51. The CEWO employs sweep-jamming techniques when electronic threat characteristics provide a frequency range but not the specific frequency in use. Sweep jamming is the jamming of a specified portion of the EMS, by sweeping the known frequency range at a predetermined rate. Sweep and spot jamming have a higher level of transmitting power applied than barrage jamming.

Barrage Jamming

6-52. Some EA assets can jam more than one frequency at a time. For example, if the adversary incorporates frequency hopping, which uses two or more frequencies at different times during a single transmission, barrage or sweep-jamming techniques are considered. Barrage jamming is the jamming of all frequencies within a specified portion of the EMS, at the same time. Barrage jamming techniques apply less power to

each jammed frequency because the power extends across the targeted frequency range. Barrage jamming generally requires the EW asset to be closer to the target receivers than sweep or spot jamming techniques. Figure 6-1 illustrates barrage jamming.

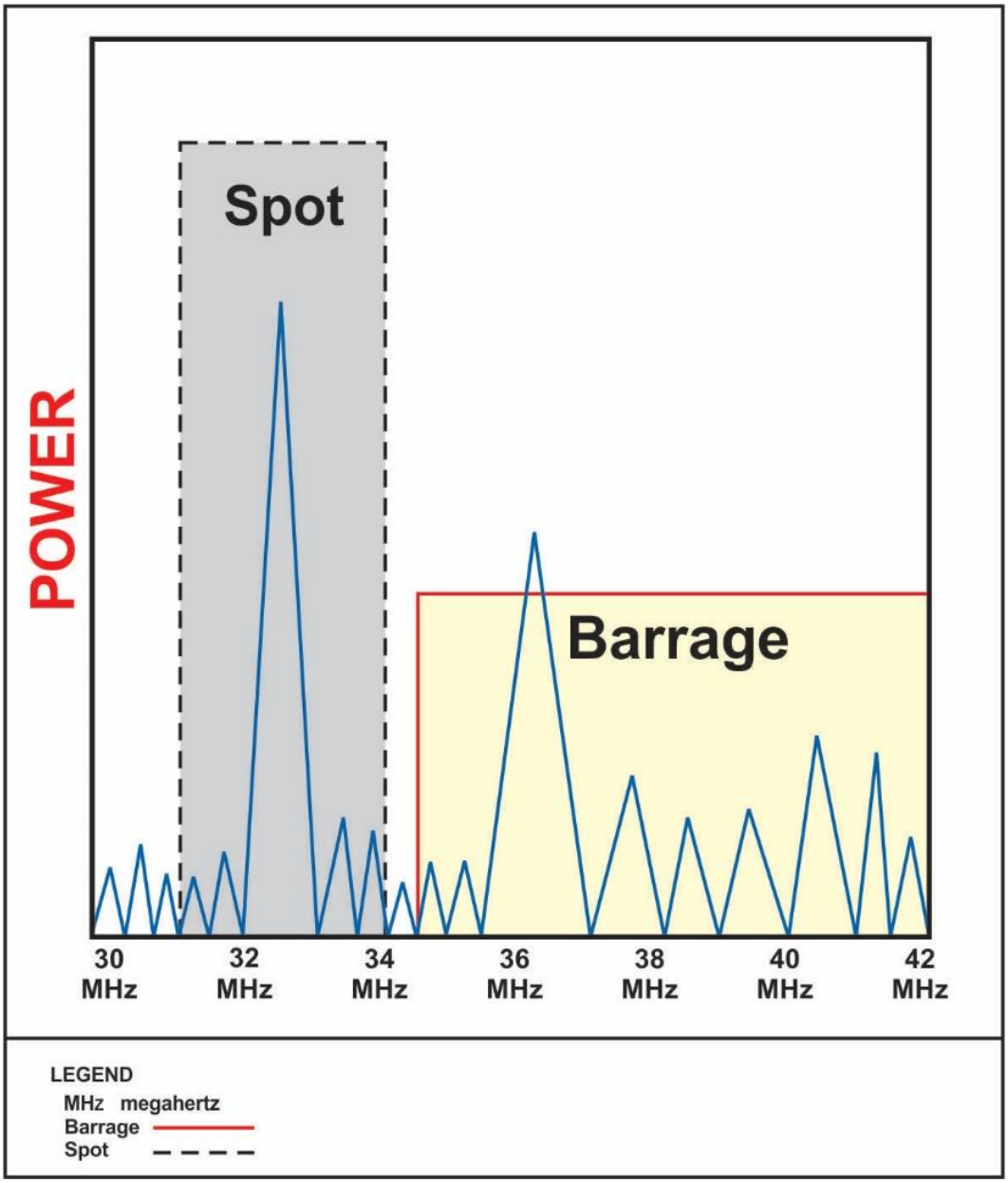

Figure 6-1. Spot and barrage jamming

Follower Jamming

6-53. Follower jamming is a form of EA to target receivers automatically when the system detects a threat transmission. Follower jamming is passive until a transmitter emits a signal. Follower jamming uses spot, barrage, and sweep-jamming techniques. EW professionals configure the jammer to attack a specific frequency or range of frequencies. The G-2 (S-2) staff compiles electronic threat characteristics and determines the frequencies employed by the threat. The CEWO ensures the proper equipment configuration to jam the prescribed frequencies. Follower jamming also jams the threat frequency-hopping receivers.

Because the asset is not always transmitting, the follower jamming technique allows a jammer to maximize its resources against a target while minimizing the threat's ability to sense and locate the jammer.

Electromagnetic Intrusion

6-54. *Electromagnetic intrusion* is the intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion (JP 3-13.1). The CEWO employs electromagnetic intrusion based on electronic threat characteristics identifying a specific type of emitter. These electronic attack techniques are discrete and tailored to specific target systems as opposed to more broad techniques such as spot, sweep, or barrage jamming.

DEFENSIVE ELECTRONIC ATTACK

6-55. Defensive EA degrades the threat's ability to employ weapons that use electromagnetic activated triggers. Defensive EA protects friendly personnel and equipment. Counter radio-controlled improvised explosive device (RCIED) systems implement this EA technique.

6-56. Defensive EA uses the EMS to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as the use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasures, and counter RCIED systems (FM 3-12).

Counter Radio-Controlled Improvised Device

6-57. A common form of defensive electronic attack is counter radio-controlled improvised explosive device electronic warfare (CREW). CREW systems jam threat radio frequencies to prevent RCIEDs from receiving a triggering signal, thus stopping the RCIED from detonating. Units program CREW systems with threat-specific loadsets based on various sources of intelligence, including the technical exploitation of recovered RCIEDs. The loadset is what the device uses to determine its operational frequency range, change rate, and other attributes of the system. The loadset is essentially what programs the system to operate under predetermined parameters based on an operational environment. The Army employs mounted, dismounted, and fixed CREW systems as electronic countermeasures to RCIED attacks.

Cyber Electronic Warfare Officer Role

6-58. The CEWO is the commander's subject matter expert on CREW. The CEWO plans the inclusion of CREW in support of operations, establishes maintenance procedures and ensures reprogramming and configuration of CREW devices.

ELECTRONIC ATTACK TECHNIQUES IN LARGE SCALE COMBAT OPERATIONS

6-59. Peer and near-peer adversaries rely on the EMS for command and control, sensing and targeting, and EW. Units require EA capabilities during large-scale combat operations to counter adversary communications and noncommunications emitters.

6-60. When jamming threat communications, the CEWO aligns EW capabilities with targets. The EA does not jam every threat communication. The EA is only disrupting the communication between the enemy battalion and enemy company. The close proximity and transmit power of the radios of the enemy tanks in a company formation allows them to maintain uninterrupted communications. The battalion transmissions to the company have a greater distance to travel and weaker signal at the receiving antenna leaving the communications vulnerable to EA. In this illustration, the enemy brigade can still effectively communicate with the enemy battalion. Figure 6-2, on page 6-11 is an example of jamming technique during large-scale combat operations.

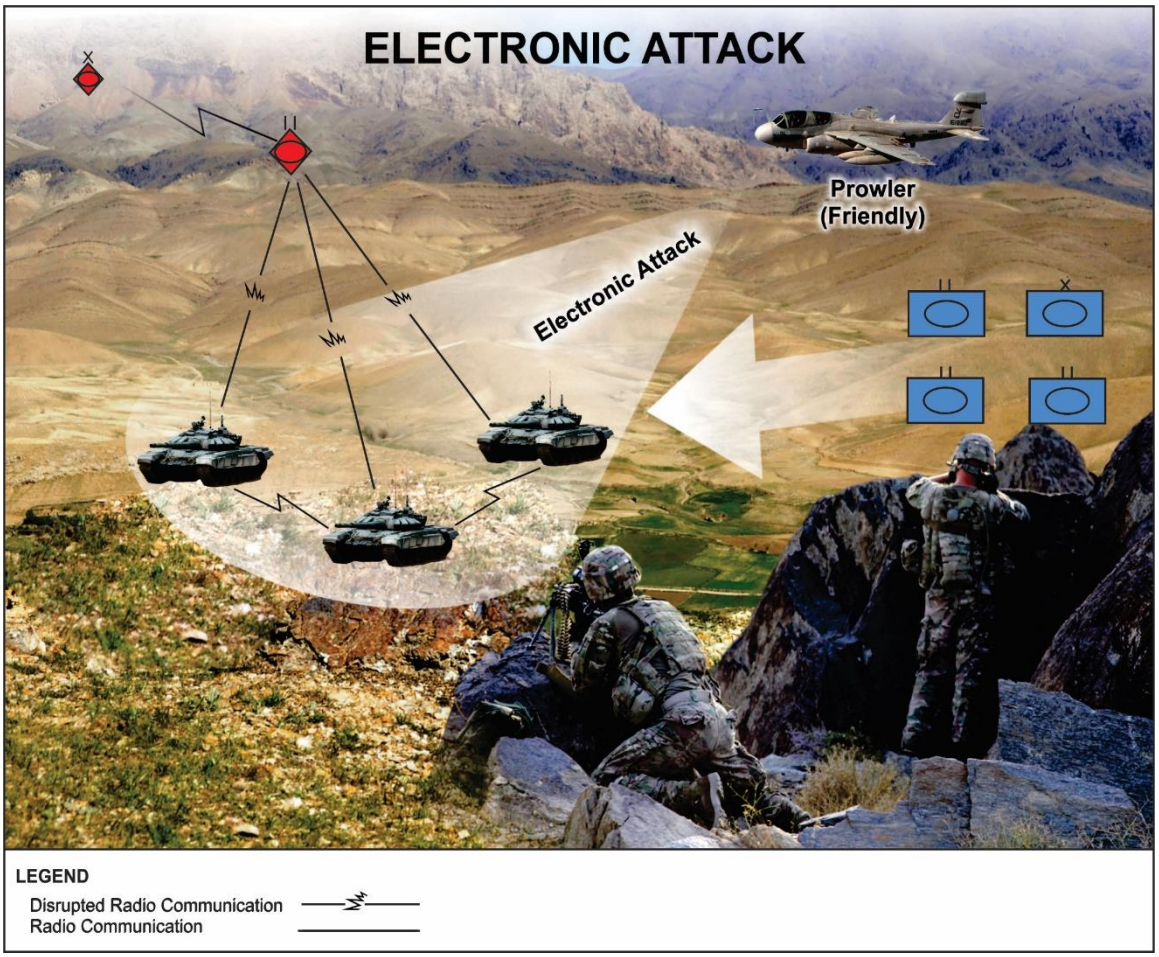

Figure 6-2. Jamming to disrupt enemy battalion to company communications

6-61. Adversaries employ multiple sensors and noncommunications emitters, such as radars, to detect and locate friendly forces during large-scale combat operations. The CEWO uses EW activities, such as electromagnetic deception, combined with EW techniques to disrupt the adversary's ability to target friendly forces. The CEWO also disrupts adversary SIGINT and ES sensors to prevent detection, locating, and exploitation of friendly transmitters

Electronic Attack Targets

A common misperception with EA is that jammers affect every emitter on the battlefield. Factors that limit jamming effectiveness include antenna type and power.

EW personnel require an understanding of the characteristics of links between nodes such as frequencies in use, transmission power levels, modulation type, and available bandwidth. The EOB includes these characteristics and ties them to a node. The G-2 (S-2) provides the EOB to the EW planner to support targeting. The EW planner uses the EOB to assess which targets to engage with EA at a time and place that supports the commander's intent and scheme of maneuver. The EW planner then determines how to engage targets based on threat characteristics and capabilities of assets available.

In the example in figure 6-2, the EW planner uses an aerial EA asset to jam a formation of enemy tanks. The intent is to disrupt the ability of the tanks to receive transmissions from their higher headquarters element. The EA does not prevent the tanks from being able to transmit. Because of transmission power levels, and the distance between the tanks in the formation, the tanks will still be able to communicate with each other. The higher headquarters element can still receive transmissions from the tanks. However, the power of the jammer is strong enough to stop the tanks from receiving the communications signal from the headquarters.

6-62. The CEWO understands that during large-scale combat operations, the threat has EW capabilities that can negatively affect friendly operations. The threat conducts EA to degrade communications and achieve a tactical advantage during operations. Units must incorporate EP techniques to counter threat EA activities.

Chapter 7
Electronic Protection Techniques

The greatest threat to mission command information systems at the tactical level is the enemy's use of electronic warfare assets to geolocate and jam friendly communications. This chapter discusses electronic protection and the techniques used to overcome electromagnetic interference. Successful electronic protection requires planning and execution by all members of the unit.

COMMANDER'S ELECTRONIC PROTECTION RESPONSIBILITIES

7-1. EP is a command responsibility. Commanders ensure that all Soldiers in their units' train to apply EP techniques. Commanders rely on the staff to mitigate electronic vulnerabilities. The staff continuously measures the effectiveness of the applied EP techniques. Commanders' EP responsibilities are—

- Read after action reviews and reports about threat jamming or deception efforts and assess the effectiveness of EP.
- Ensure the staff reports and analyzes EMI, deception, or jamming.
- Analyze the impact of threat efforts to affect friendly communications.
- Ensure the unit incorporates appropriate EP techniques such as—
  - Changing network call signs and frequencies in accordance with the SOI.
  - Using approved COMSEC devices.
  - Loading and using prescribed encryption keys.
  - Using planned authentication procedures.
  - Controlling emissions.

7-2. EP is the sum of technology, equipment, and techniques used to counter threat EW activities. EP is not force protection or self-protection. EP is an EMS-dependent system's use of electromagnetic energy or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1).

PLANNING ELECTRONIC PROTECTION

7-3. Electronic protection uses techniques such as limiting transmissions and using natural or manmade objects to mask radiated energy from traveling to undesirable destinations. Electronic protection is essential to prevent the adversary from learning behavior and intentions within the EMS.

7-4. The CEWO considers friendly communications asset characteristics, their priorities for protection and their purpose of employment when planning EP. Additionally, the CEWO considers adversarial EW and SIGINT capabilities and their use against friendly systems. The G-6 (S-6) is the primary source for gaining the characteristics of friendly communications resources while the G-2 (S-2) is the CEWO's primary resource to gain electronic threat characteristics.

ELECTRONIC PROTECTION CONSIDERATIONS

7-5. EP includes physical security, COMSEC measures, system technical capabilities, such as frequency hopping, shielding of electronics, electromagnetic spectrum management, and emission control procedures. EP is an EMS-dependent system's use of electromagnetic energy and/or physical properties to preserve itself from direct or environmental effects of friendly and adversary EW, thereby allowing the system to continue operating (JP 3-13.1). The CEWO considers the following for EP—

- Vulnerability analysis and assessment of friendly communications assets.
- EP monitoring techniques and feedback procedures.
- EP effects on friendly capabilities.

Vulnerability Analysis and Assessment

7-6. Vulnerability analysis and assessment form the basis for developing EP plans. The CEWO reviews the unit EP techniques and procedures to determine weaknesses and develops plans for improvement. The G-6 (S-6), United States Cyber Command, and the Defense Information Systems Agency provide a variety of cybersecurity services, including vulnerability analysis and assessments.

7-7. The National Security Agency monitors COMSEC and provides security posture feedback to units. Its programs focus on telecommunications systems using wire and electronic communications. Their programs can support and remediate the command's COMSEC procedures.

Electronic Protection Effects on Friendly Capabilities

7-8. The CEWO and the G-6 (S-6) consider effects on friendly communications when developing an EP plan. A plan that maximizes EP can overly restrict the friendly use of communications assets. The CEWO maintains a balance regarding the unit's ability to communicate with the planned level of EP. EP effects on friendly communications are included in the CEWO's risk assessment. The CEWO and G-6 (S-6) present the risk assessment to the commander during the MDMP. The commander decides what level of risk is acceptable. For more information regarding EP during the MDMP refer to FM 3-12.

7-9. For EP planning, the CEWO and G-6 (S-6) consider the following—

- Electromagnetic hardening.
- Electronic masking.
- Emission control.
- Electromagnetic spectrum management.
- Wartime reserve modes.
- Electromagnetic compatibility.

ELECTROMAGNETIC HARDENING

7-10. The CEWO and G-6 (S-6) mutually develop SOPs and inspect the configuration of unit equipment such as the proper grounding of communications assemblages, serviceability of cable shielding and adequate cable connectivity. These actions protect friendly communications and noncommunications resources from threat identification, lethal and nonlethal attack and exploitation. *Electromagnetic hardening* is action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-13.1).

ELECTRONIC MASKING

7-11. Obstructions, such as hills, mountaintops, or buildings present ideal conditions for maximum radio transmission coverage. Transmitters placed on the top of a hill, mountaintop, or building are vulnerable to threat visual identification, DF techniques, and jamming. Known transmitter locations allow an adversary to jam the receivers, listen to transmissions and collect information such as friendly battle rhythm and duration of friendly transmissions, or to attack using lethal means. To mitigate these vulnerabilities, CEWOs use electronic masking techniques by placing antennas on the side of the mountain, hill or building in a manner that allows the optimal friendly use of the antenna while preventing threat detection and exploitation. *Electronic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-13.1).

7-12. Figure 7-1 illustrates the adversary's use of terrain masking. In this example, the adversary is avoiding detection by friendly DF sensors. This technique applies to any type of emitter to include radars and directional antennas focusing on placing the emitters where they are least likely detectable.

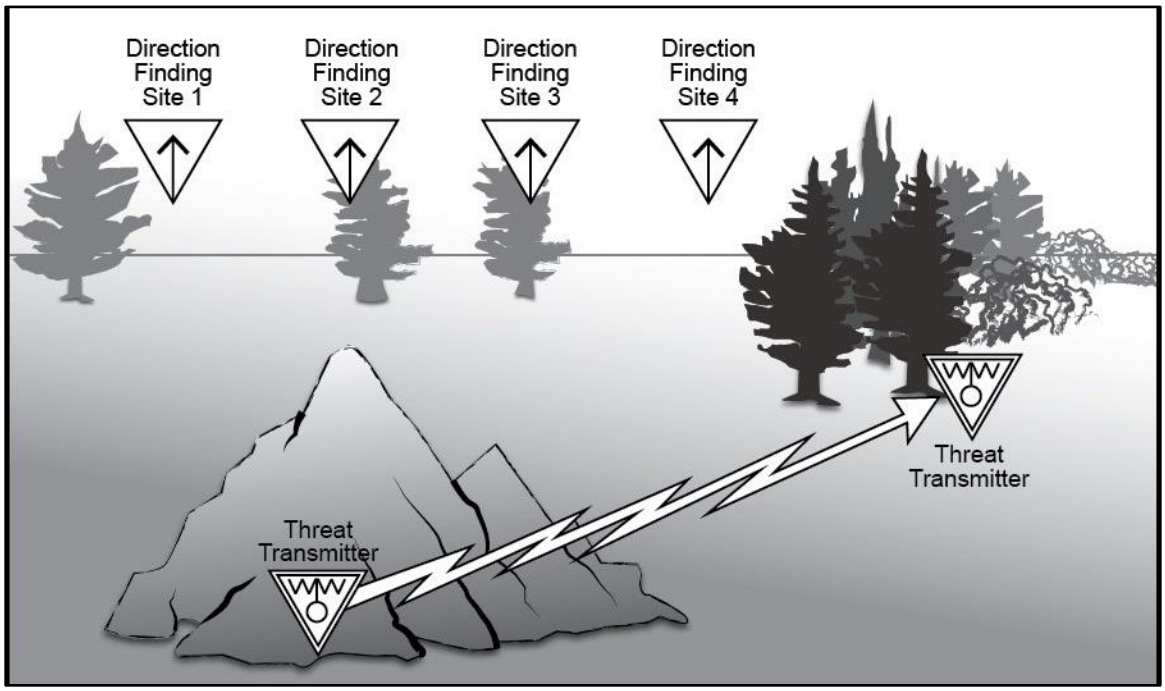

Figure 7-1. Threat use of terrain masking

EMISSION CONTROL

7-13. EP is only effective when everyone in an organization understands its importance and can readily identify opportunities to implement protection activities. Emission control prevents the threat of discovering and attacking the locations of friendly forces with EW. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan (JP 3-13.1). To establish emission control best practices, the CEWO and the G-6 (S-6) consider—

- Transmit power settings.
- Designating user time slots for transmissions.

Minimum Transmit Power

7-14. The most basic protection from enemy EW is radio discipline. This can take the form of limiting transmissions, antenna masking, and use of low power. The use of minimum transmit power is a technique that prevents signals from traveling beyond the intended receiving station and thereby limits threat ability to find and fix friendly forces. Some transmitters include adjustable transmit power settings. A technique to establish minimum transmission power is, begin with a low transmitting power setting and gradually increase the output power until the intended recipient can validate the successful reception of the transmitted signal. Table 7-1 on page 7-4 includes techniques to minimize transmit power levels.

Table 7-1. Techniques for minimizing transmissions and transmission times

Technique	*Description*
Ensure all transmissions are necessary	Analysis of U.S. tactical communications indicates that most communication used in training exercises is explanatory and not directive. Units use tactical radio communications to convey orders and critical information rapidly. Execution of the operation must be inherent in training, planning, ingenuity, teamwork, and established and practiced standing operating procedures. The high volume of radio communications that usually precedes a tactical operation makes the friendly force vulnerable to enemy interception, direction finding, jamming, and deception.
Note. Even when communications are secure, the amount of radio transmissions can betray an operation, and the enemy can still disrupt the ability of the U.S. forces to communicate.	
Preplan messages before transmitting them	The radio operator should know what to say before beginning a transmission. When the situation and time permit, write out the message before beginning the transmission. This minimizes the number of pauses in the transmission and decreases transmission time. It also ensures the conciseness of the message.
Transmit quickly and precisely	This is critical when the quality of communications is poor. This reduces the need to repeat a radio transmission. Unnecessary repetition increases transmission time and the enemy's opportunity to intercept U.S. transmissions and gain valuable information. When a transmission is necessary, the radio operator should speak in a clear, well-modulated voice, and use proper radiotelephone procedures.
Use equipment capable of data burst transmission	This is one of the most significant advantages of tactical satellite communications systems. Soldiers use limited time for encoded messages on a digital entry device for transmission over satellite systems.
Use an alternate means of communications	Soldiers use alternate means of communications, such as cable, wire, or messages to convey necessary directives and information.
Use brevity codes	A brevity code is a code which provides no security, but which has as its sole purpose the shortening of messages rather than the concealment of their content. (Refer to ATP 1-02.1 for more information on brevity codes.)

Radio Placement

7-15. The placement of transmitters and distant receivers in close proximity limits the threat's ability to jam the intended signal. Additionally, the CEWO and G-6 (S-6) staff ensure that antennas are more than twice the distance of their height from infrastructure such as power lines. For safety, units avoid placing antennas near sleep areas, tents, and vehicle parking areas.

7-16. The G-6 (S-6) staff is responsible for the management of friendly use of EMS resources. The G-6 (S-6) staff, with assistance from the spectrum manager, provides the CEMA section spectrum manager with a database of all assigned friendly frequencies. The G-6 (S-6) staff recommends the location of the tactical operations center to the G-3 (S-3) staff. Variables for site selection include feasibility for DOD information network connectivity to higher, lower, and lateral command posts. Site selection includes EP considerations such as—

- Available terrain for electronic masking.
- Distance between transmitters and receivers.

ELECTROMAGNETIC SPECTRUM MANAGEMENT

7-17. *Electromagnetic spectrum management* is planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 6-01). Electromagnetic spectrum management affects a unit's ability to conduct EP. The G-6 (S-6) spectrum manager prepares and maintains a list of friendly frequencies and coordinates with the G-2 (S-2) who maintains the list of threat frequencies in use. Knowing the purpose of EMS resources and their characteristics allows the spectrum manager to assist the CEWO when preparing the EP portion of an operation or mission.

7-18. Electromagnetic spectrum management also involves knowing the types and quantity of friendly transmitters in the area of operations. When units use frequencies employed by other friendly forces in the same area of operations, it may cause undesirable EMI.

7-19. Units choose the optimal frequency to communicate based on the frequency characteristics. For example, high frequency (HF) frequencies are desirable when communicating over land for thousands of miles. Very high frequencies, in contrast to HF frequencies, usually are ineffective at distances over 30 kilometers. The spectrum manager analyzes RF characteristics using modeling software that calculates the intended and unintended effects a transmitter will have on a receiver and the distance the radio wave travels. The database includes frequencies used for mission command and EA.

WARTIME RESERVE MODES

7-20. Potential adversaries search for information that reveals friendly EW vulnerabilities in the information environment such as technical articles, magazines, news programs and web pages that are available on the Internet. The Army prevents public access to wartime reserve modes. *Wartime reserve modes* are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance (JP 3-13.1).

ELECTROMAGNETIC COMPATIBILITY

7-21. Some units rely on operational needs statements for the procurement of EW equipment. Before units acquire EW equipment, units conduct electromagnetic compatibility analysis. *Electromagnetic compatibility* is the ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response (JP 3-13.1).

ELECTROMAGNETIC INTERFERENCE

7-22. EMI prevents successful transmissions. Units must recognize and mitigate EMI to create the conditions required to use the EMS to communicate. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment (JP 3-13.1).

RECOGNIZING ELECTROMAGNETIC JAMMING

7-23. Radio operations require that radio operators can recognize electromagnetic jamming. Recognizing electromagnetic jamming is not always an easy task; the cause of EMI can be internal and external. If the EMI remains after grounding or disconnecting the antenna, the disturbance is most likely internal and caused by a malfunction of the radio. Contact maintenance personnel for repairs or replace the faulty equipment. Eliminate or substantially reduce the EMI or suspected jamming by grounding the radio equipment or disconnecting the receiver antenna. If measures to eliminate the radio as the source of the disturbance are unsuccessful, it is most likely external to the radio. Check external EMI further for threat jamming or unintentional EMI.

7-24. Sources, other than jamming, cause EMI. Unintentional EMI is caused by—

- Friendly and threat use of the same frequencies.
- Other electronic or electric and electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.

7-25. Unintentional EMI normally travels a short distance; a search of the immediate area may reveal its source. Moving the receiving antenna short distances may cause noticeable variations in the strength of the

interfering signal. Conversely, little or no variation normally indicates threat jamming. Regardless of the source, take appropriate actions to reduce the effect of EMI on friendly communications.

Obvious Jamming

7-26. Obvious jamming usually is simple to detect. When experiencing jamming, it is important to recognize and overcome the incident. Table 7-2 lists some common jamming signals.

Table 7-2. Common jamming signals

Signal	*Description*
Random Noise	It is indiscriminate in amplitude and frequency. It is similar to normal background noise. Random noise degrades all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate electronic protection actions.
Stepped Tones	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Single-channel amplitude modulation or frequency modulation use stepped tones for voice circuits.
Spark	Spark is one of the most effective jamming signals. Spark uses short intensity and high intensity; they repeat at a rapid rate. This signal is effective in disrupting all types of radio communications.
Gulls	Generated by a quick rise and slow fall of a variable radio frequency and are similar to the cry of a seagull. It produces a nuisance effect and is very effective against voice radio communications.
Random Pulse	Pulses of varying amplitude, duration, and rate are generated and transmitted. They disrupt teletypewriter, radar, and all types of data transmission systems.
Wobbler	A single frequency modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.
Recorded Sounds	Any audible sound, especially of a variable nature, distracts radio operators and disrupts communications. Music, screams, applause, whistles, machinery noise, and laughter are examples of recorded sounds.
Preamble Jamming	A broadcasted tone over the operating frequency of secure radio nets resembles the synchronization preamble of the speech security equipment. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio networks using speech security devices.

Subtle Jamming

7-27. The adversary can use powerful, unmodulated or noise modulated jamming signals. Modulation is the process of adding information to an RF signal or carrier by varying its amplitude, frequency, or phase. A lack of noise characterizes unmodulated jamming signals. Noise modulated jamming signals are characterized by noticeable EMI noise. Subtle jamming is ambiguous when there is no sound heard from the receivers. Although everything appears normal to the radio operator, the receiver cannot receive an incoming, friendly signal. Users assume their radios are malfunctioning, instead of recognizing the subtle jamming.

Reporting Jamming

7-28. Units report suspected threat jamming and any unidentified or unintentional EMI that disrupts the ability of U.S. forces to communicate. Units report any suspected jamming or EMI even if the radio operator can overcome the effects of the jamming or EMI. Units use the information in the joint spectrum interference resolution (JSIR) report to locate, mitigate, or destroy the threat jamming equipment or take other action to the benefit of U.S. forces.

Note. Army units use the JSIR format to describe and report EMI for intentional and unintentional interference to friendly communications. Refer to CJCSM 3320.02D for additional information regarding the JSIR Program.

OVERCOMING JAMMING

7-29. The adversary uses diverse forms of jamming. Radio operators require awareness to the possibility of jamming. Training and field experience are invaluable opportunities for operators' ability to distinguish jamming from unintentional EMI. Adversarial jamming requires friendly action. The following paragraphs address the actions to take for detected threat jamming. Users continue normal operations after overcoming jamming or jamming ceases and submit or update the JSIR. The unit submits a JSIR regardless of overcoming the jamming or EMI interference. For more information about the JSIR, see appendix D.

Continue to Operate

7-30. Threat EA usually involves jamming followed by a brief listening period. Operator activity during the listening period indicates how effective the jamming to alleviate the threat has been. If the friendly operation continues to operate in a normal manner, the adversary assumes the jamming is not effective. However, if the adversary senses the radio traffic stops, the adversary assumes the jamming is effective. Because the adversary is monitoring friendly operation in this manner, friendly operators continue to use the communications equipment to prevent the adversary's assessment of the desired effect, so normal operations continue.

Improve the Signal to Jamming Ratio

7-31. The signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. Signal refers to the signal received. Jamming refers to the hostile transmission received. It is best to have a signal-to-jamming ratio in which the desired signal is stronger than the jamming. In this situation, the jamming signal cannot significantly degrade the desired signal. Improving the signal to jamming ration facilitates successful communications. To improve the signal-to-jamming ratio operators and signal leaders consider the following courses of action—

- Increase the transmitter power output.
- Adjust, change, or relocate the antenna.
- Establish a retransmission station.
- Use an alternate route for communications.
- Change frequencies.

Increase the Transmitter Power Output

7-32. When the adversary successfully jams, operators use the available reserve power on the distant transmitter to overpower the adversary's jamming. The operator then submits a JSIR report.

Adjust Change or Relocate the Antenna

7-33. When jamming occurs, the radio operator ensures optimal adjustment of the antenna to receive the desired incoming signal. Methods that apply to a specific radio set are in the appropriate operator's technical manual. Depending on the antenna, adjustment methods include reorientation of the antenna, changing the antenna polarization and installing a different antenna with a longer range.

> ***Note***. Distant and local stations require the same antenna polarization. Operators polarize antennas in the horizontal or vertical planes. See appendix A.

Establish a Retransmission Station

7-34. A retransmission station reduces the length between transmitters and intended receivers. This technique improves the signal-to-jamming ratio.

Use an Alternate Route for Communications

7-35. 7-35.Threat jamming seeks to prevent friendly forces from communicating with another radio station. When degraded radio communications occur between two radio stations, operators implement the PACE plan and use another frequency or communication method. An example of an alternate communication method is changing from a terrestrial based LOS transmission path to satellite communications.

7-36. Units provide maps and network diagrams that illustrate friendly radio stations, alternate routes for communications and the associated terrain. Radio operators use this information to make route adjustments to improve communications.

Change Frequencies

7-37. Commanders direct units to change to an alternate frequency to overcome threat jamming. If a prescribed frequency change does not occur smoothly, the adversary may discover what is happening, and try to disrupt or degrade communications on the new frequency. All radio operators require knowledge of when they are to switch to an alternate frequency. Procedures that describe the conditions and plans to change frequencies are included in the operations order, SOI or SOPs.

7-38. Through CEMA, units have an opportunity to develop deception plans before changing frequencies. Preplanned and well-coordinated actions are required for dummy stations to continue to operate on the frequency being jammed, to mask the change to an alternate frequency.

7-39. EP is a preventive measure or countermeasure used to mitigate intentional and nonintentional EMI. EMI is a concern during planning and execution. A lack of consideration of EP actions creates vulnerabilities to friendly use of the EMS. Electromagnetic interference does not always require action.

7-40. Electromagnetic interference requires action when it negatively affects operations by prohibiting the friendly use of the EMS. Units incorporate effective techniques to minimize, reduce, or eliminate prohibitive electromagnetic interference (JP 3-13.1). Techniques to resolve EMI include—

- Changing friendly frequencies as prescribed in the SOI or operations order.
- Implementing terrain-masking techniques.
- Using directional antennas.
- Relocating transmitters and receivers.

ELECTROMAGNETIC INTERFERENCE BATTLE DRILL

7-41. Some prohibitive EMI has a measurable, operational impact. Units execute battle drills to address prohibitive EMI. An EMI battle drill helps isolate the cause of interference and dispel erroneous assumptions about its cause. For example, knowing that CREW devices are jammers may lead to a hasty assumption that a CREW device impairs the use of combat net radios when operator error or faulty equipment is the cause of the EMI. The uninformed assumption that CREW systems are the problem leads to an unnecessary loss of confidence in EW equipment. Lack of confidence in equipment can lead to reluctance to prosecute EW and can have a negative impact on operations. Proper analysis uses sensors and indicators that identify interfering frequencies, the levels of transmission power and receiver strength.

Note. Watts express the radio transmission output levels, while decibels (dB) express radio receive signal strength. For more information about decibels, refer to ATP 2-22.6-2.

7-42. The lowest element or individual experiencing the EMI should report the interference via the Joint Spectrum Interference Resolution Website. If unable to access the website, contact someone to input the information into the website at the earliest convenient time. On a staff, normally the G-6 (S-6) staff submits JSIR reports to resolve interference. When appropriate, the staff disseminates the mitigating steps to subordinate units as lessons learned and best practices to avoid future interference. A well-constructed EMI battle drill, guides units to respond to JSIR reports in a consistent, methodical manner. See table 7-3 on page 7-9 for an example of an EMI troubleshooting battle drill.

Table 7-3. Electromagnetic interference troubleshooting battle drill

Signal	*Description*
1	Follow equipment troubleshooting (verify frequency, cable and antenna connections, communications security). If EMI continues, then follow remaining steps.
2	Determine start and stop times or duration of EMI.
3	Identify EMI effect (interfering voice, noise, static).
4	Identify other emitters in area of operations.
5	Check adjacent and nearby units for similar problems.
6	Prepare and submit a joint spectrum interference resolution report to S-6.
LEGEND	
EMI	electromagnetic interference
S-6	battalion or brigade signal staff officer

REMEDIAL ELECTRONIC PROTECTION TECHNIQUES

7-43. Remedial EP techniques that help reduce the effectiveness of threat jamming efforts are the—

- Identification of threat jamming signals.
- Determination of the EMI as being obvious or subtle jamming.
- Recognition of jamming causing EMI by—
  - Determining whether the EMI is internal or external to the radio.
  - Determining whether the EMI is deliberate or unintentional.
- Reporting of jamming and other EMI incidents.
- Overcoming of jamming and EMI by adhering to the following techniques—
  - Continue to operate.
  - Diagnose the root cause of EMI.
  - Improve the signal-to-jamming ratio.
  - Adjust the receiver settings.
  - Increase the transmitter power output.
  - Adjust or change the antenna.
  - Establish a retransmission station.
  - Relocate the antenna.
  - Use an alternate route for communications.
  - Change the frequencies.
  - Acquire another satellite or retransmission station.
  - Installation of firmware and update software.
  - Use enhancements to tactical radio ancillary communications electronics equipment and COMSEC devices.

CONCEALMENT

7-44. EP plans include provisions to conceal communications personnel and equipment. Though physical concealment is ineffective in changing the EMS signature, obscuring the physical attributes may prevent positive identification of the equipment as a communications system. Units use camouflage material to cover communications assemblages and their power generators. It is difficult to conceal most communications systems. However, installing antennas as low as possible on the backside of terrain features, and behind manufactured obstacles help conceal communications equipment while still facilitating effective communications.

THREAT ELECTRONIC ATTACK ON FRIENDLY COMMAND NODES

7-45. Adversaries attack or exploit friendly command nodes that support operations. They have developed and equipment and techniques to contest the friendly use of the EMS. Friendly units use EP measures to counter threat EW and exploitation actions against friendly communications nodes.

7-46. Adversary attack on friendly command nodes can disrupt or destroy information, intelligence gathering efforts, and communications that support weapons systems. Threat forces expend considerable resources gathering intelligence about U.S. forces. Goals or effects may include—

- Jam friendly communications.
- Enter friendly radio networks.
- Collect information and intelligence about friendly forces.

STAFF ELECTRONIC PROTECTION RESPONSIBILITIES

7-47. The staff implements the EP plan for the commander. Staff responsibilities are—

- Planning, coordinating, and supporting the execution of EP activities (CEMA working group).
- Advising the commander of threat EMS related capabilities [G-2 (S-2) staff].
- Supervising the CEMA section and include EP scenarios in command post, field training exercises, and evaluates employed EP techniques [G-3 (S-3) staff].
- Work with the CEWO to prepare and conduct the unit EP training program. Ensure there are PACE means of communications to support mission command. Distribute COMSEC. Perform friendly frequency management duties and issues the SOI. Review the JRFL and prepares which includes a restricted frequency list of taboo, protected and guarded frequencies [G-6 (S-6) staff].

Note. The PACE plan compliments EP as it provides multiple means of communications and designates the order in which an element will move through available communications methods until contact can be established with the desired recipient.

7-48. Preventive EP techniques include all measures taken to avoid threat detection and threat EA. EP seeks to mitigate threat information collection and intelligence gathering efforts. Electronic communications equipment has built-in features used to mitigate threat EA, ES and SIGINT actions. CEWOs advise the use of built-in features and user tactics, techniques, and procedures for countermeasures against threat actions.

EQUIPMENT AND COMMUNICATIONS ENHANCEMENTS

7-49. Some communications equipment has embedded capabilities used to prevent jamming, locating and listening by threat forces. Operators use the embedded capabilities when supporting operations.

FREQUENCY-HOPPING MODE

7-50. Some peer and near-peer adversaries with advanced EW equipment can jam radios that use frequency-hopping techniques. Single channel transmissions are vulnerable to jamming by unsophisticated transmitters, so units use frequency-hopping mode but remain vulnerable to threat EA and DF efforts. Frequency hopping is useful in mitigating the effects of threat jamming, and in keeping friendly position location data from threat forces.

ADAPTIVE ANTENNA TECHNIQUES

7-51. Adaptive antenna techniques result in more survivable communications. These techniques typically link with spread spectrum waveforms to combine frequency hopping with pseudo-noise coding. Pseudo-noise coding is a technique to make spread spectrum waveforms and frequency-hopping mode appear to be unintelligible noise to an unintended receiver. Spread spectrum is a form of wireless communication in which the frequency of the transmitted signal varies deliberately. This uses more bandwidth than the signal would have otherwise, making it less susceptible to interference.

FREQUENCY HOP MULTIPLEXER

7-52. The frequency hop multiplexer (FHMUX) and vehicular whip antennas that support FHMUX are available for use to enhance very high frequency (VHF) communications. The FHMUX is an antenna multiplexer used with single channel ground and airborne radio system in stationary and mobile operations. This FHMUX allows multiple radios to transmit and receive through one VHF antenna while operating in the frequency-hopping mode, single channel mode, or a combination of both. Using one antenna reduces visual and electronic profiles of command posts and reduces emplacement and displacement times.

This page intentionally left blank.

Appendix A

The Electromagnetic Spectrum

Electronic warfare professionals must understand the electromagnetic spectrum and the electromagnetic environment to achieve desired effects. Appendix A describes the fundamentals of the electromagnetic spectrum and radio wave propagation.

RADIO WAVE BANDS AND CHARACTERISTICS

A-1. Frequency is an essential consideration in radio wave propagation. The following summaries indicate the principal effects associated with the various frequency bands, starting with the lowest and progressing to the highest usable frequency, as shown in table A-1.

Table A-1. Radio wave bands and frequencies

Radio Wave Band	*Frequency*	*Frequency in megahertz*
Extremely low frequency (ELF)	3–30 hertz	Only a small portion of the band is useful for communications.
Very low frequency (VLF)	3–300 kHz	Below .03 MHz
Low frequency (LF)	30–300 kHz	.03–.3 MHz
Medium frequency (MF)	300 kilohertz–3 MHz	.3–3 MHz
High frequency (HF)	3–30 MHz	3–30 MHz
Very high frequency (VHF)	30–300 MHz	30–300 MHz
Ultrahigh frequency	300 MHz –3 GHz	300–3,000 MHz
Super high frequency (SHF)	3–30 GHz	3,000–30,000 MHz
Extremely high frequency (EHF)	30–300 GHz	30,000–300,000 MHz

Legend:

EHF	extremely high frequency	kHz	kilohertz
ELF	extremely low frequency	MF	medium frequency
HF	high frequency	MHz	megahertz
LF	low frequency	VHF	very high frequency
GHz	gigahertz	SHF	super high frequency

EXTREMELY LOW FREQUENCY

A-2. Generally, extremely low frequency waves occur accidentally or naturally. This frequency is the white noise and electrical hum encountered in almost all circuits, or it results from the interaction of solar wind and atmospheric charges.

VERY LOW FREQUENCY

A-3. The VLF signals are compatible with the Earth-ionosphere waveguide and achieve great distances, low attenuation, and excellent stability. Earth-ionosphere waveguide is a phenomenon that allows some radio waves to propagate in the space between the ground and the boundary of the ionosphere. During magnetic storms, very low frequency signals may constitute the only source of radio communications over great distances. Operators do not use VLF for great distances over land because of the long wavelength and requirement for large antennas. Magnetic storms have little effect on these transmissions because of the

efficiency of the Earth-ionosphere waveguide. However, interferences from atmospheric noise are troublesome. Submarines have radios under the surface of the sea that use VLF signals.

LOW FREQUENCY

A-4. As frequency increases to the LF band and diffraction decreases, there is greater attenuation with distance, and the range for a given power output rapidly drops. Using more efficient antennas for transmitting offsets the drop in power and increases range. LF signals are most stable within ground wave distance of the transmitter. A wider bandwidth permits pulsed signals at 100 kilohertz. The pulsed signals allow separation of the stable ground wave pulse from the variable skywave pulse up to 1,500 kilometers (932 miles), and up to 2,000 kilometers (1,243 miles) for overwater paths. The frequency for long-range navigation is in the LF band, which is useful for radio DF.

MEDIUM FREQUENCY

A-5. Medium frequency ground waves provide dependable service, but the long-distance communications require increases in transmit power. This range varies from about 645 kilometers (400 miles) at the lower portion of the band to about 24 kilometers (15 miles) at the upper end for a transmitted signal of 1 kilowatt. Achievable distance depends on—

- The amount of transmitting power.
- The efficiency of the antenna.
- The nature of the terrain between the transmitting and receiving stations.

A-6. Elevating the antenna to obtain direct waves may improve the quality of the transmission. At the band's lower frequencies, skywaves are available both day and night. As the frequency increases, ionospheric absorption increases to a maximum at about 1,400 kilohertz. At higher frequencies, the absorption decreases, permitting increased use of skywaves. Since the ionosphere changes with the hour, season, and sunspot cycle, the reliability of skywave signals is variable. By careful selection of frequency, ranges of as much as 12,875 kilometers (8,000 miles) with 1 kilowatt of transmitted power are possible, using multi-hop signals. However, the frequency selection is critical. If it is too high, the signals penetrate the ionosphere and are lost in space; if it is too low, signals are too weak. In general, skywave reception is equally good by day or night. Lower frequencies are best for the night.

HIGH FREQUENCY

A-7. The ground wave range of HF signals is limited to about 5 kilometers (3 miles), but the elevation of the antenna may increase the direct-wave distance of transmission. Additionally, the height of the antenna has an important effect on skywave transmissions. By day, this may be 10–30 megahertz; at night, it may drop to the 8–10 megahertz range. This band is widely used for ship-to-ship and ship-to-shore communications.

VERY HIGH FREQUENCY

A-8. Communication uses the direct wave, or direct wave plus a ground reflected wave. Although some wave interference between direct and ground-reflected waves is present, elevating the antenna to increase the distance at which direct waves can be used results in increased reception distances. Diffraction is much less than with lower frequencies, but most evident when signals cross sharp mountain peaks or ridges. Under suitable conditions, ionospheric reflections are sufficiently strong to be useful, but generally, they are unavailable. There is little interference from atmospheric noise in this band. Reasonably efficient directional antennas are possible with VHF. Operators mainly use this band for communications.

ULTRAHIGH FREQUENCY

A-9. Skywaves are absent in the ultrahigh frequency band since the ionosphere lacks enough density to refract the waves, which instead pass through the ionosphere into space. Ground waves and ground-reflected waves are usable, although there is some wave interference. Diffraction is negligible, but the radio horizon extends about 15 percent beyond the visible horizon, due to refraction. Reception of ultrahigh frequency

(UHF) signals is virtually free from fading and interference by atmospheric noise. This band is widely used for ship-to-ship and ship-to-shore communication.

SUPER-HIGH FREQUENCY

A-10. In the super-high frequency band, known as the microwave or as the centimeter wave band, skywaves are absent. Transmission is entirely by direct and ground-reflected waves. Diffraction and interference by atmospheric noise are virtually nonexistent. Transmission in the super-high frequency band is similar to that of ultrahigh frequency, but the effects of using shorter waves is greater. Reflection by clouds, water droplets, and dust particles increases, causing greater scattering, increasing wave interference, and fading. The super-high frequency band is for marine navigational radar use.

REGULATION OF FREQUENCY USE

A-11. While the characteristics of various frequencies are important to the selection of the most suitable one for any given purpose, there are additional considerations. Confusion and extensive interference would result if every user had complete freedom of selection. The allocation of various frequency bands to particular uses is a matter of international agreement. Within the United States, the Federal Communications Commission authorizes the use of specific frequencies. Figure A-1 on page A-4 displays the frequencies supporting DOD capabilities, federal controlled frequencies, and shared spectrum.

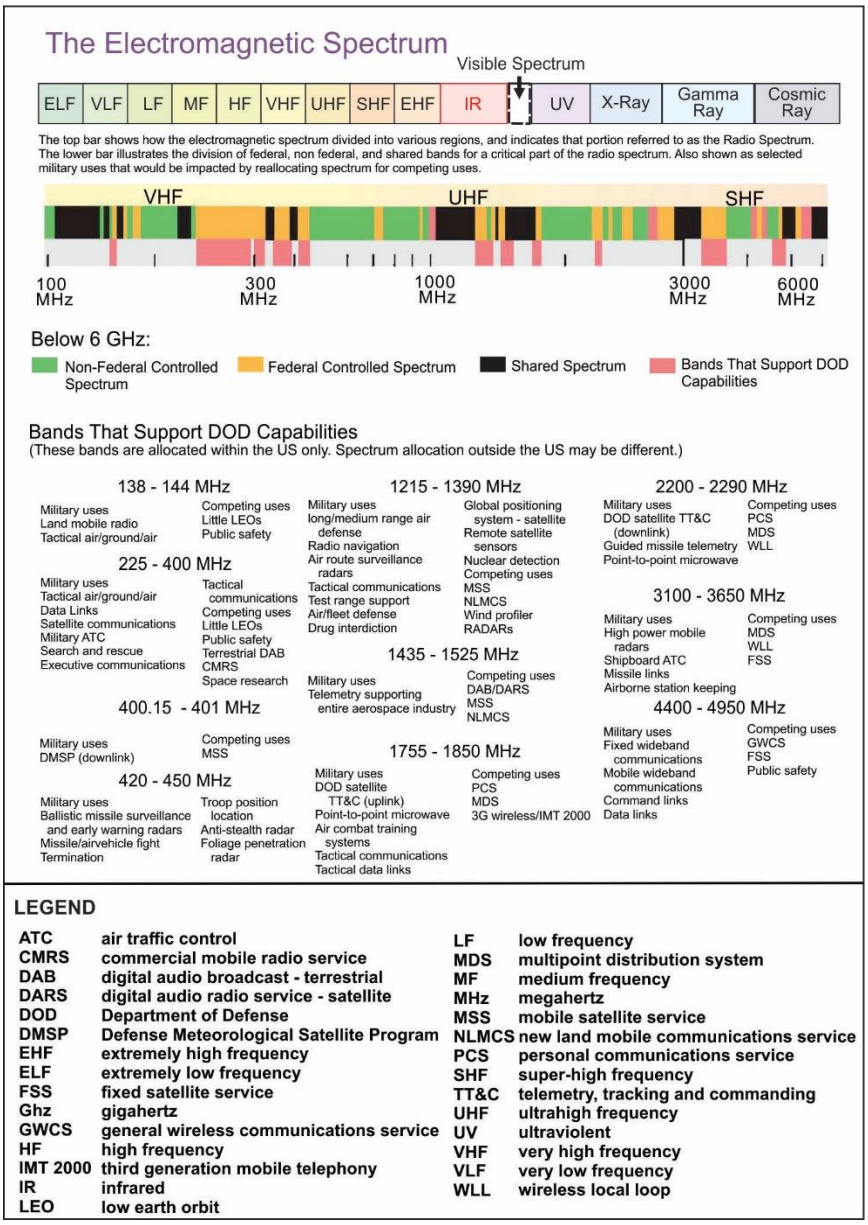

Figure A-1. Department of Defense use of the electromagnetic spectrum

EARTH'S ATMOSPHERE

A-12. The Earth's atmosphere comprises numerous layers, of which three are key to this discussion: the troposphere, the stratosphere, and the ionosphere, which can play a crucial role in long-range radio communications. Table A-2 on page A-5 summarizes the features of the three layers, beginning with the troposphere, the lowest layer.

Table A-2. Atmosphere layers, features, and their effects on radio waves

Atmospheric Region	*Elevation in Kilometers(km) and Miles (mi)*	*Features*	*Effects on Radio Frequencies*
Ionosphere	50–600 km 31–373 mi	Electrically charged set of layers with large amounts of free electrons.	• Excellent refraction of medium frequency and high frequency signals. • Primary medium for skywaves.
Stratosphere	15–50 km 9–31 mi	The only isothermal region of the atmosphere.	No effect.
Troposphere	10–15 km 6–9 mi	• Sustains life. • Lowest region of the atmosphere. • Temperatures decreases with increasing altitude.	• Primarily acts to absorb radio waves. • Small amounts of refraction possible, but unpredictable.
Legend: km kilometers mi miles			

TROPOSPHERE

A-13. The troposphere is that portion of the Earth's atmosphere extending from the surface of the Earth to an elevation of approximately 10–15 kilometers (6–9 miles). This region of the atmosphere greatly influences electromagnetic emissions—a direct result of the ever-changing conditions, such as temperature and moisture content, within this layer. This region is where most weather activities occur; it also contains the mixture of life-sustaining gasses.

STRATOSPHERE

A-14. The stratosphere is located between the troposphere and the ionosphere about 15–50 kilometers (9–31 miles) above the Earth's surface. The stratosphere and the isothermal region are synonymous. The isothermal region maintains a nearly constant temperature. Isothermal means same or constant temperature. The stratosphere has little, if any, effect on radio waves, which travel through this layer to reach the ionosphere.

IONOSPHERE

A-15. The ionosphere is a region of numerous positive and negative ions and unattached electrons. The extent of ionization depends upon the kinds of atoms present in the atmosphere, the density of the atmosphere, the position relative to the Sun (time of day and season), as well as solar flares, magnetic storms, and nuclear detonations, which affect ionization. After sunset, ions and electrons recombine faster than they are separated, decreasing the ionization of the atmosphere. Table A-3 on page A-6 illustrates the differences in the three major regions of the Earth's atmosphere.

Table A-3. Ionosphere layers and effects on radio waves

Ionosphere Layer	*Elevation*	*Features*	*Effects on Radio Frequencies*
F	145–400 km 90–249 mi (F2: 145–200 km) (F2: 90–124 mi) (F1: 240–400 km) (F1: 149–249 mi)	• Very positively ionized with large amounts of free electrons. • During the day, separates into the F1 and F2 layers. • At night, F layer decreases in ionization and increases in altitude.	• Primary means of refracting medium frequency and high frequency signals in skywave propagation. • At night, slightly erratic behavior, but much greater communications distances.
E	100–200 km 62–124 mi	• Positively ionized with varying amounts of free electrons. • Condition changes with temperature, angle of the sun, magnetic fields, and time of day.	• Erratic behavior. • Sometimes refracts radio waves in the medium frequency, high frequency, and very high frequency bands.
D	50–100 km 31–62 mi	• Layer closest to the Earth. • Negatively ionized with relatively little free electrons. • Exists only during the day.	• Primarily acts to absorb HF radio waves. • Layer may refract low frequency and very low frequency, but unpredictable.
Legend: HF high frequency km kilometers mi miles			

A-16. In the outermost regions of the atmosphere, air density is so low that oxygen exists mainly as separate atoms, rather than as combined oxygen molecules, as it does nearer to the Earth's surface. The F layer is where the energy level is low, and ionization from solar radiation is intense. Above this level, the ionization decreases because of the lack of atoms to be ionized. Below this level, it decreases because the ionizing agent of the appropriate energy is already absorbed. During daylight, two levels of maximum ionization are present: the F2 layer, at about 200 kilometers (125 miles) above the Earth's surface, and the F1 layer, at about 145 kilometers (90 miles). At night, these combine to form a single F layer. See figure A-2 on page A-7.

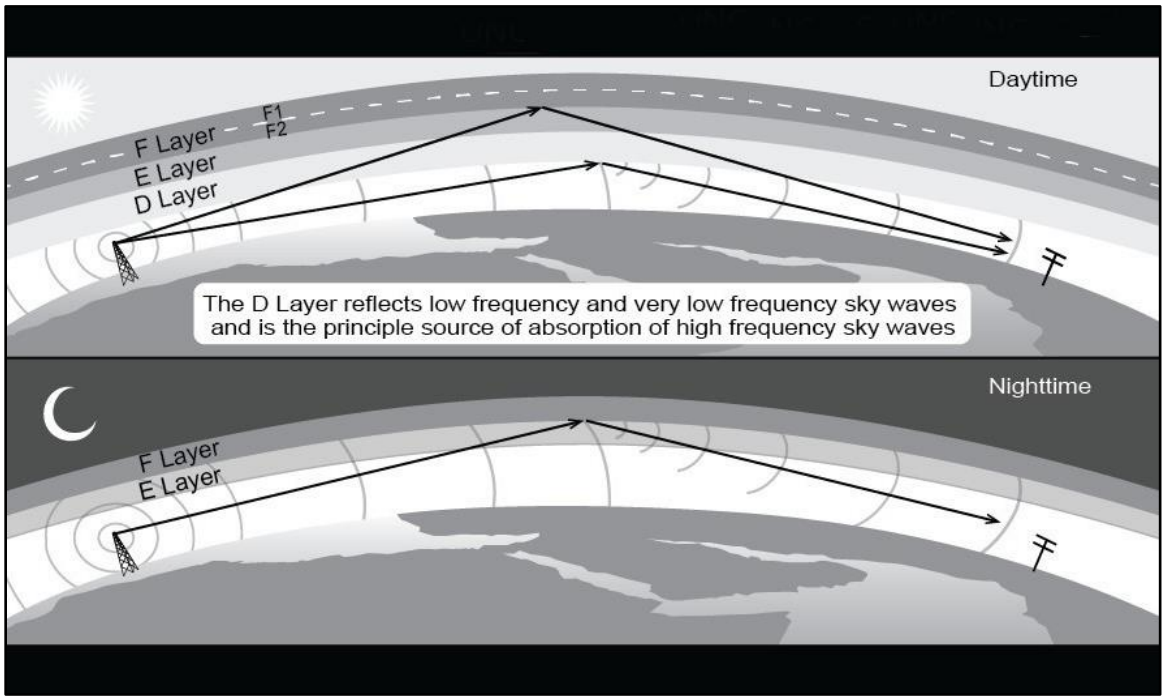

Figure A-2. The ionosphere—daytime and nighttime composition

A-17. The ion—a key characteristic of the atmosphere—affects radio waves. Since an atom normally has an equal number of negatively charged electrons and positively charged protons, it is electrically neutral. An ion is an atom or group of atoms that becomes electrically charged, either positively or negatively, by the loss or gain of one or more electrons.

A-18. Loss of electrons may occur in a variety of ways. In the atmosphere, ions form due to the collision of atoms with rapidly moving particles, or by effects of cosmic rays or ultraviolet light. In the lower atmosphere, recombination soon occurs, leaving a small percentage of ions. However, in the thin atmosphere, far above the Earth's surface, atoms are widely separated, and many ions may be present.

BANDS OF THE ELECTROMAGNETIC SPECTRUM

A-19. The EMS refers to the entire range of electromagnetic radiation frequencies. The frequency range suitable for radio transmission extends from 10 kilohertz–300,000 megahertz. This portion of the EMS has several bands, as shown in figure A-2. Below the RF spectrum, and overlapping it, is the audio frequency band, extending from 20–20,000 Hertz. Above the RF spectrum are infrared, the optical (visible) spectrum (light in its various colors), ultra-violet rays, x-rays, and gamma rays. Within the RF range, from 1–40 gigahertz (1,000–40,000 megahertz), between the ultrahigh frequency and extremely high frequency are additional bands, defined as—

- L band: 1–2 gigahertz.
- S band: 2–4 gigahertz.
- C band: 4–8 gigahertz.
- Ku band: 12–18 gigahertz.
- K band: 18–27 gigahertz.
- Ka band: 27–40 gigahertz.

A-20. Maritime radar systems commonly operate in the S and X bands. Satellite positioning, navigation, and timing signals are in the L band. Figure A-3 on page A-8 illustrates the EMS and communication bands.

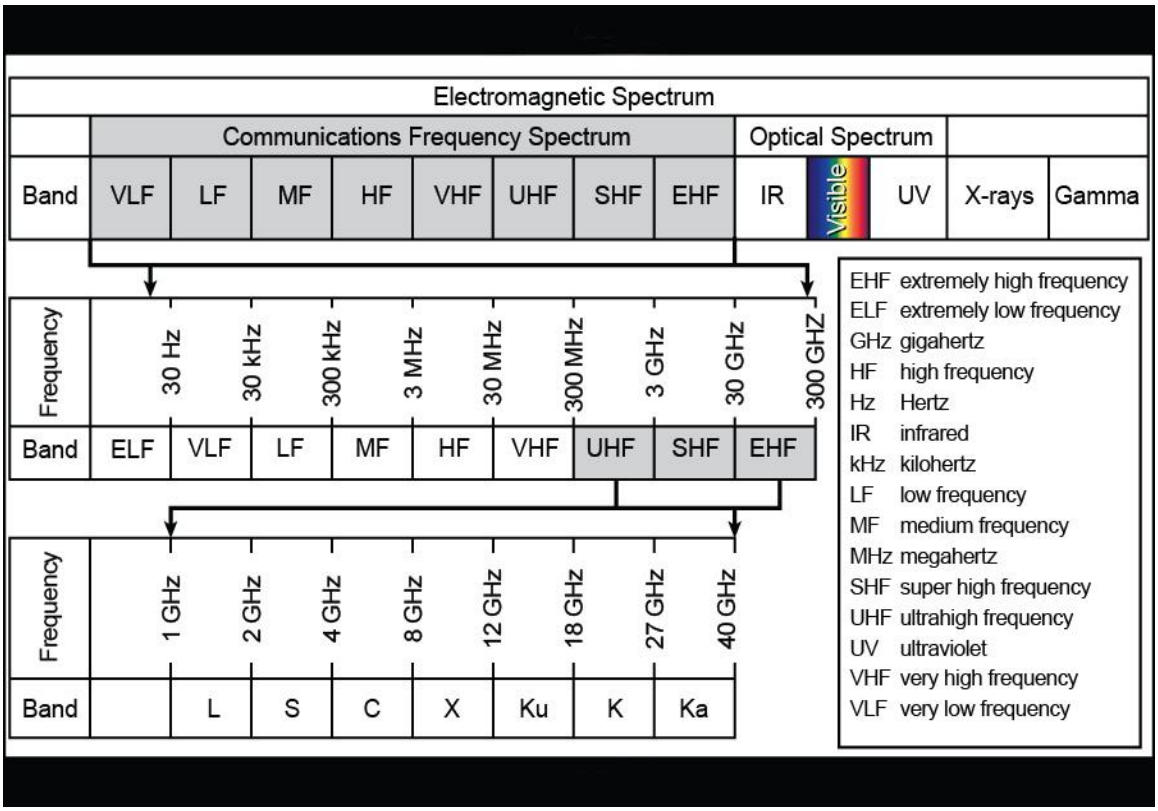

Figure A-3. The electromagnetic spectrum and communication bands

A-21. Modern communications systems use frequencies between the extremely low frequency and extremely high frequency. Typical frequency ranges for modern communications include—

- Voice (push-to-talk radios) HF through ultrahigh frequency range.
- Cordless telephones use VHF range.
- Broadcast television (Channels 2 through 13) use VHF range.
- Frequency modulation (FM) broadcast-VHF range.
- Broadcast television (Channels 14 through 69) use ultrahigh frequency range.
- Cellular phones use L and S bands.
- Satellite communications use C, X, Ku, and Ka bands between ultrahigh frequency and extremely high frequency ranges.

RADIO WAVE

A-22. A radio wave is an electromagnetic transmission and consists of an electric field (E field) and a magnetic field (H field). An electric current is a flow of electrons along a conductor between points of differing potential. A direct current flows continuously in the same direction. Direct current occurs when the polarity of the electromotive force causing the electron flow is constant, such as the case with a battery. If the relative motion between a conductor and a magnetic field induces the current, for example, a rotating machine called a generator, then the resulting current changes direction in the conductor as the polarity of the electromotive force changes with the rotation of the generator's rotor. Reversing the direction of the current is alternating current.

A-23. The energy of the current flowing through the conductor either dissipates as heat (an energy loss proportional to both the current flowing through the conductor and the conductor's resistance) or is stored in an electromagnetic field oriented symmetrically about the conductor. The orientation of this field is a function

of the polarity of the source producing the current. An electromagnetic field collapses back into a wire when the current stops.

A-24. What will occur if the polarity of the current source supplying the wire reverses at a rate that exceeds the finite amount of time required for the electromagnetic field to collapse back upon the wire? In this case, another magnetic field, proportional in strength but exactly opposite in magnetic orientation to the initial field, will form on the wire. The initial magnetic field, its current source absent, cannot collapse back upon the wire because of the existence of this second electromagnetic field. Instead, it propagates out into space. This phenomenon is the basic principle of a radio antenna, which transmits a wave at a frequency proportional to the rate of pole reversal and speed equal to the speed of light.

RADIO WAVE TERMINOLOGY

A-25. The magnetic field strength near a conductor is directly proportional to the magnitude of the current flowing through the conductor (see paragraph A-12 for the discussion of alternating current). A rotating generator produces current in the form of a sine wave. That is, the magnitude of the current varies as a function of the relative position of the rotating conductor and the stationary magnetic field used to induce the current. The current starts at zero and increases to a maximum as the rotor completes one-quarter of its revolution and falls to zero when the rotor completes one half of its revolution. Sine functions represent a current that approaches a negative maximum; then it once again returns to zero.

A-26. Figure A-4 illustrates the relationship between current and the magnetic field strength induced in the conductor through which the current flows. Field strength is proportional to the magnitude of the current; therefore, if the current is represented by a sine wave function, then so too will be the magnetic field strength resulting from that current. The characteristic shape of the field strength curve led to the term wave when referring to electromagnetic propagation. The maximum displacement of a crest from zero is the amplitude.

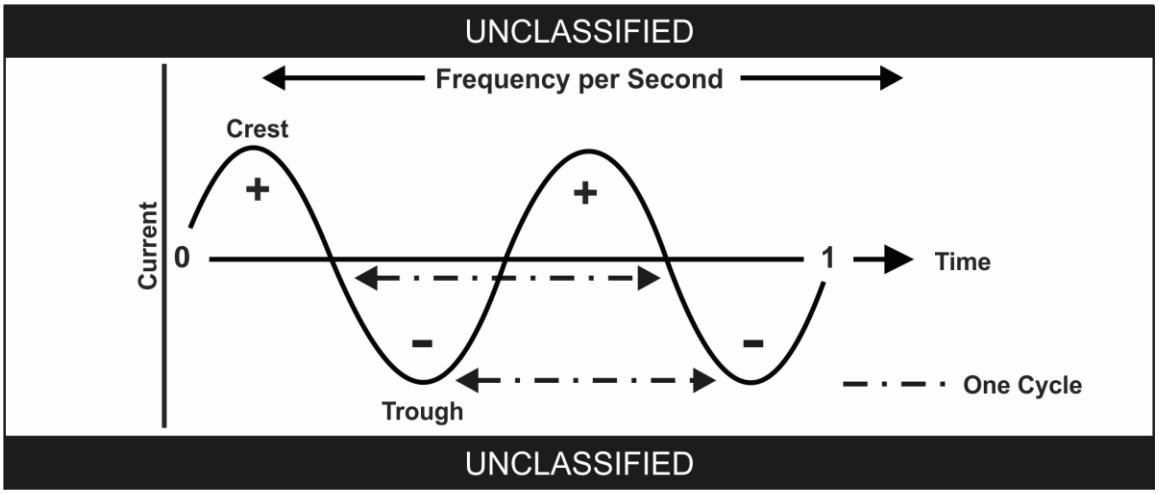

Figure A-4. Relationship between magnetic field strength and current

A-27. The square of the wave amplitude is directly proportional to the energy transported by a wave. Doubling the amplitude of a wave is indicative of quadrupling the energy transported by the wave. Tripling the amplitude of a wave is indicative of a nine-fold increase in the energy transported by the wave. Table A-4 shows the amplitude-energy relationship.

Table A-4. The proportional relationship between amplitude and energy

Amplitude	1 unit	2 units	3 units	4 units	5 units
Energy	2 units	8 units	18 units	32 units	50 units

A-28. One cycle is a complete sequence of values, as from wave crest to wave crest or from zero amplitude to zero amplitude. The distance traveled by the energy during one cycle is the wavelength, usually expressed in metric units (such as meters or centimeters). The number of cycles repeated during unit time (usually one

second) is the frequency in Hertz (cycles per second). One kilohertz is 1,000 cycles per second. One megahertz is 1,000,000 cycles per second. Wavelength and frequency are inversely proportional.

A-29. The phase of a wave is the amount the cycle progresses from a specified origin. For most purposes, it is in circular measure; 360 degrees is considered a complete cycle. Generally, the origin is not important; the principal interest being the phase relative to that of some other wave. Thus, two waves with crests a quarter of a cycle apart are 90 degrees out of phase. If the crest of one wave (+) occurs at the trough (-) of another, the two are 180 degrees out of phase.

RADIO TRANSMISSION TYPES

A-30. A continuous wave refers to a series of waves transmitted at a constant frequency and amplitude. One only hears continuous waves at the very lowest RFs, when they may produce an audible high-pitched hum in a receiver. One uses a modified continuous wave directly, as in radio DF, in some manner. The modified continuous wave is modulation. When this occurs, the continuous wave serves as a carrier wave for information. Any of several types of modulation may be used.

A-31. In amplitude modulation, the amplitude of the carrier wave alters according to the amplitude of a modulating wave, usually of audio frequency, as shown in figure A-4. The receiver demodulates the signal by removing the modulating wave and converting it to its original form. This form of modulation is widely used in voice radio, as in the standard broadcast band of commercial broadcasting.

A-32. FM occurs when the frequency changes in accordance with the amplitude of the impressed signal, as shown in figure A-5. Commercial FM broadcasts use altered frequency for FM radio broadcasts and the sound portion of television broadcasts.

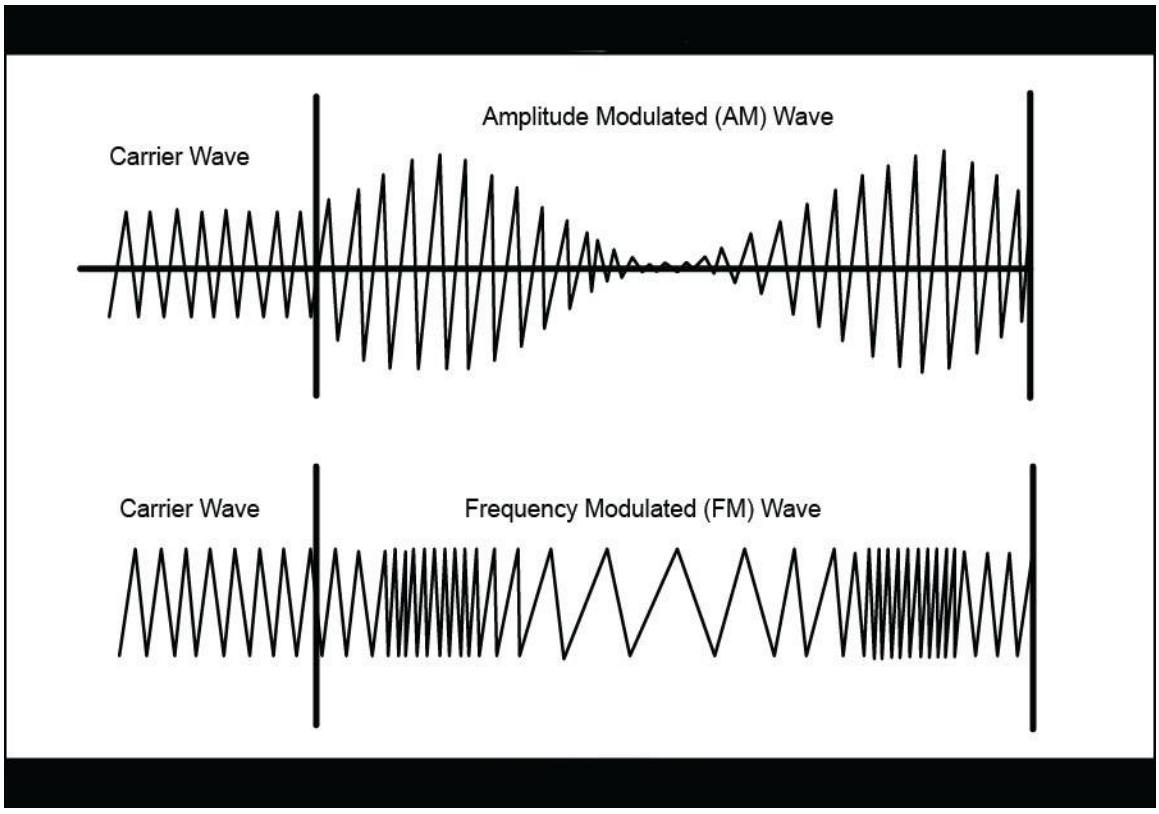

Figure A-5. Amplitude modulation and frequency modulation

A-33. Pulse modulation is somewhat different. There is no impressed modulating wave. In this form of transmission, the transmitter uses short bursts of the carrier wave, separated by relatively long periods of

silence, during which there is no transmission. Some radio navigation aids use this transmission type (see figure A-6) including radar and long-range navigation such as LORAN-C.

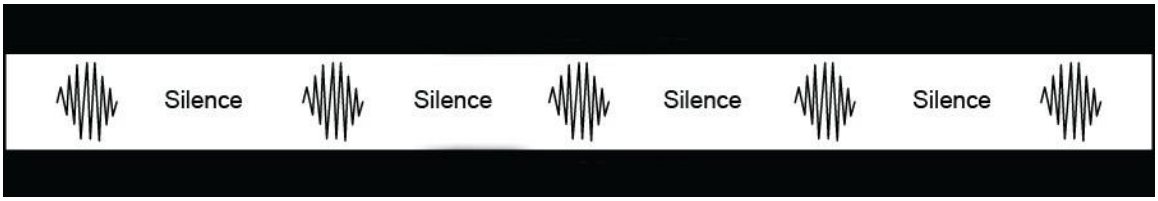

Figure A-6. Pulse modulation

RADIO WAVE PROPAGATION

A-34. Radio waves travel through space at the same speed as light. They travel approximately 300,000,000 meters per second (186,000 miles per second). The following is a conversion formula for wavelength and frequency. If the measurement in hertz is known and a conversion to wavelength is desired, apply—

$$\text{Wavelength (meters)} = \frac{300{,}000{,}000}{\text{frequency (hertz)}}$$

A-35. If wavelength (in meters) is known and a conversion to frequency (hertz) is desired, apply—

$$\text{Frequency (hertz)} = \frac{300{,}000{,}000}{\text{wavelength (meters)}}$$

A-36. Radio wave propagation extends or transmits electromagnetic energy through space. Wavelength, frequency, and polarization are essential elements of the actual wave and affect radio wave propagation. The simplest form of propagation is through the space wave. The wave radiates from the transmitter and continues through space until it reaches the receiver. The Earth's curved surface, while appearing to be flat over a short distance, limits the effective LOS range.

A-37. Users determine the total limiting distance by assuming an earth with a radius four-thirds times its proper radius. Such an earth would have a larger circumference and, hence, a longer distance to the horizon. Increasing the height extends the distance of either the transmitting or the receiving antenna, effectively extending the horizon. Given the height of two antennas (in feet), the LOS distance can be calculated by identifying the square root of the known height, then multiplying the result by 1.41, and adding the sums together to obtain the LOS distance in miles. The following formula can also be applied using kilometers and meters—

$$\text{LOS distance (miles)} = 1.41 \times \sqrt{(\text{height 1 [feet]})} + 1.41 \times \sqrt{(\text{height 2 [feet]})}$$

A-38. This LOS distance formula does not include terrain or address free-space path loss, which involves the loss of signal strength along with an unobstructed LOS path (see paragraph A-64).

A-39. Figure A-7 on page A-12 gives an approximation of the LOS transmission range without any mathematical calculations. Use a straightedge on the chart, aligned with the elevations of the transmitting antenna to the receiving antenna to determine the transmission range.

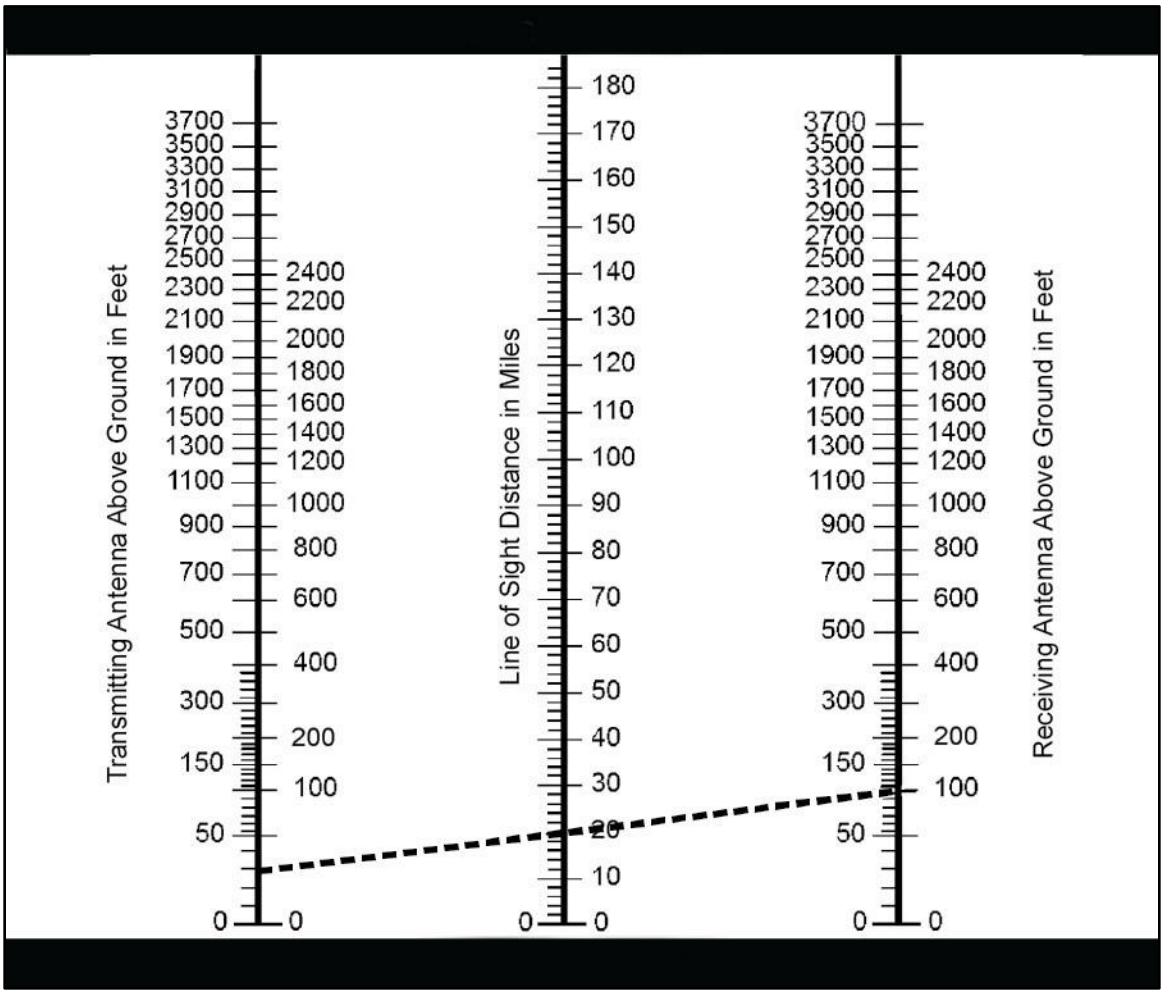

Figure A-7. Antenna heights and line of sight distances

A-40. Radio waves tend to travel in straight lines unless acted upon by some force. A sharply defined object reflects radio waves off the surface of any sharply defined object. A refracted wave bounces off the ionosphere at the same angle at which it arrives, meaning the angle of incidence is equal to the angle of arrival. Radio waves can also encounter other obstructions or objects that will scatter, diffract, or reflect the signal. Substantial losses of energy limit the distance of travel when the Earth reflects the waves. This loss is due to substantial losses of energy in the form of heat dissipated into the Earth's crust. Factors that affect radio wave propagation include—

- Wavelength.
- Polarization.
- Physical obstructions
- Space, land, air, and water.
- Weather.

POLARIZATION

A-41. Radio waves produce both an electric field and magnetic field, which are always perpendicular. The direction of the electrical component (electric field) of a radio wave, relative to the ground, determines the polarization of the wave (see figure A-8 on page A-13). Polarization can be linear (vertical or horizontal) or nonlinear (circular or elliptical). Thus, if the electrical component is vertical, the wave is vertically polarized, and if horizontal, it is horizontally polarized.

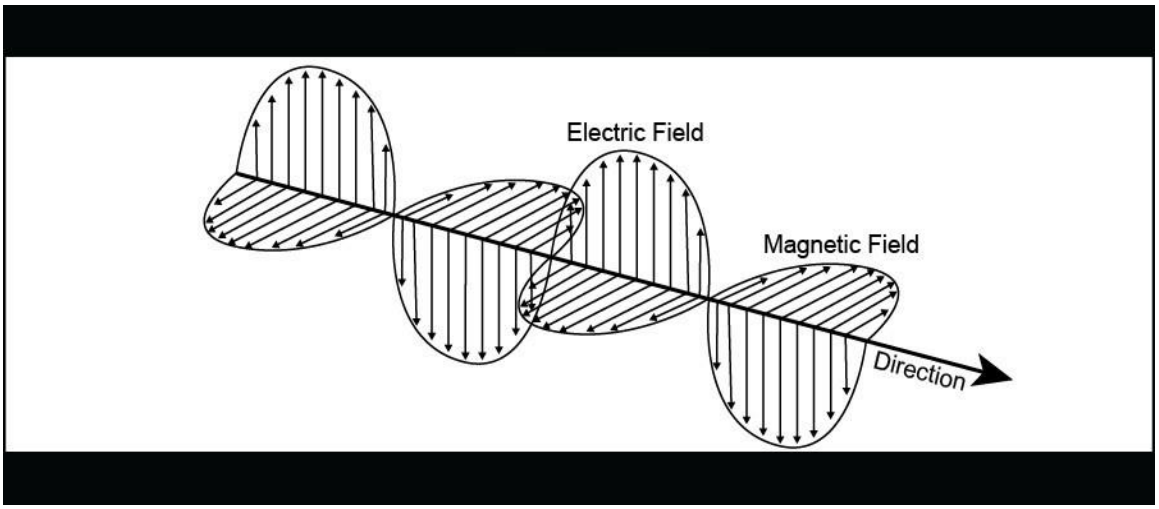

Figure A-8. Electric and magnetic fields of a radio wave

A-42. To illustrate vertical wave polarization, imagine rope lying reasonably straight on the ground. If one raises and lowers the loose end of the rope with a violent up and down motion, a series of undulating waves will travel along the rope. The movement of the waves will be vertical to the Earth, or vertically polarized. If the same rope had a similar movement applied horizontally, the waves would be in a horizontal plane or horizontally polarized.

A-43. If one uses a whip or other vertical type-transmitting antenna to propagate radio waves, the transmitted wave is vertically polarized. Vertically polarized waves travel along the surface of the Earth. The waves travel vertically because the Earth short-circuits any horizontal component. If the transmitting antenna is horizontal, relative to the Earth's surface, the transmitted wave is horizontally polarized. Circular and elliptical polarization adopts characteristics of vertical and horizontal polarization, resulting in a circular or a hybrid waveform. Figure A-9 shows waves traveling in space polarize in any desired direction.

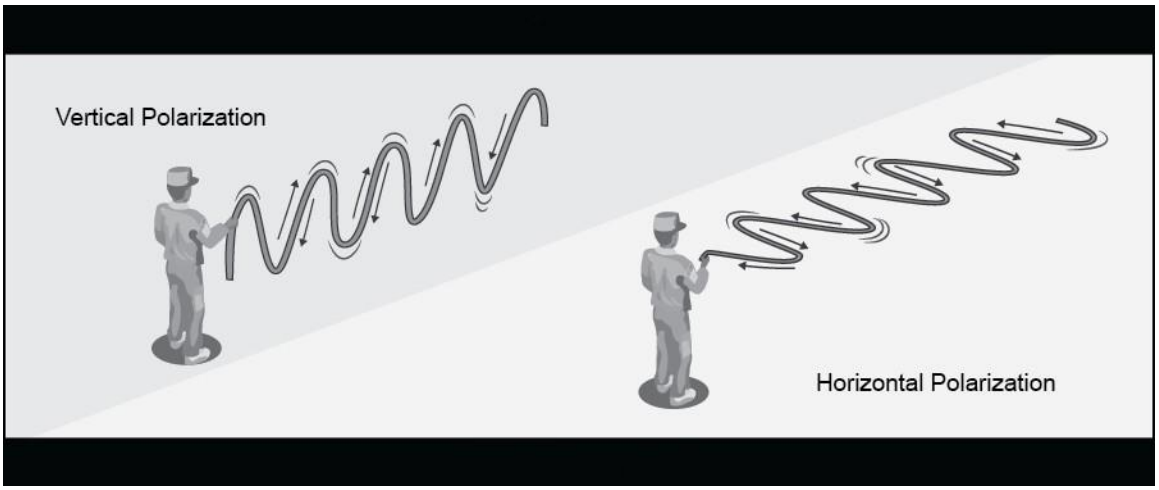

Figure A-9. Vertical and horizontal polarization

A-44. Some antennas also apply a circular polarization in which the electric field rotates at the RF circularly, either to the right or to left of the axis of propagation. Instead of transmitting in just one plane, a circularly polarized antenna transmits in both planes at once, with a 90-degree phase shift between the two planes. The signal, in this case, would look like a corkscrew as opposed to a wave. Circular polarization occurs in two variations as well, right-hand (clockwise) or left-hand (counterclockwise) polarization. Circular polarization

reduces the probability of multipath interference. If the two plane waves have different amplitudes or the phase difference is other than 90 degrees, then the polarization is elliptical (see figure A-10).

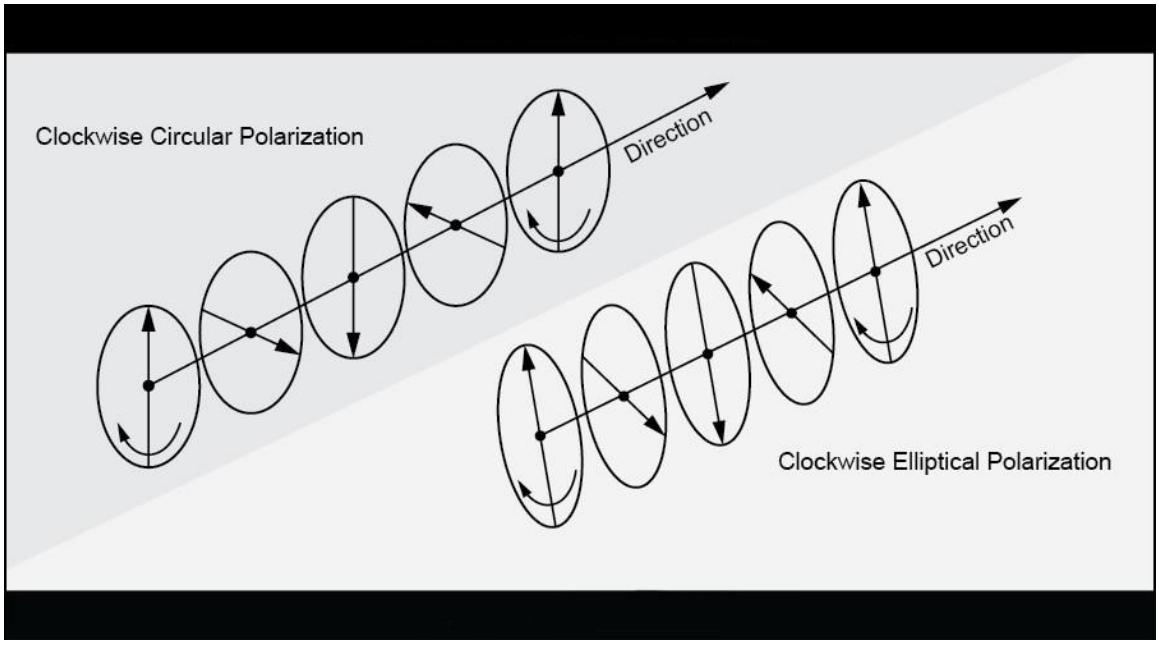

Figure A-10. Circular and elliptical polarization

A-45. Polarization is sometimes predictable based on an antenna's geometry. An antenna's linear polarization is generally along the direction (as viewed from the receiving location) of the antenna's currents. For instance, a vertically oriented whip antenna will transmit and receive vertically polarized waves. Antennas with horizontal elements, such as the old rooftop television antennas, are horizontally polarized (broadcast television usually uses horizontal polarization). Even when the antenna system is vertically orientated, such as an array of horizontal dipole antennas, the polarization is in the horizontal direction, corresponding to the current flow. It is best for a receiving antenna to match the polarization of the transmitted wave for optimum reception.

A-46. When a vertically polarized antenna tries to communicate with a horizontally polarized antenna (called cross-polarization), and vice versa, there can be as much as a 30-decibel loss in signal strength. A horizontally aligned signal will not align with a vertically aligned antenna, so a considerable amount of the transmitted wave will simply bypass the receiving station.

REFLECTION

A-47. Reflection involves a change in the direction of waves when a wave bounces off a barrier. When radio waves strike a surface, the surface reflects them in the same manner as light waves. The Earth's surface reflects all radio waves. The strength of the reflected wave depends on the angle of incidence (the angle between the incident ray and the horizontal surface), type of polarization, frequency, reflecting properties of the surface, and divergence of the reflected ray. Lower frequencies penetrate the Earth's surface more than higher ones. At very low frequencies, radios receive signals below the surface of the sea. The wavefront of a radio wave is an expanding spherical surface, all the points of which are in the same phase. A phase change occurs when a wave reflects from the surface of the Earth. The amount of the change varies with the conductivity of the Earth (such as soil composition and moisture content) and the polarization of the wave, reaching a maximum of 180 degrees for a horizontally polarized wave reflected from seawater (considered to have infinite conductivity).

A-48. Figure A-11 on page A-15 shows a planar wavefront reflected from a smooth surface. As in the reflection of light, the angle of incidence equals the angle of reflection. However, the incident wavefront, A–A1, is reversed by the reflecting surface and appears at B–B1—180 degrees out of phase. The reversal in

reflection occurs because point X of the incident wave reaches the reflecting surface before point Y and reflects to point X1 during the time it takes for point Y, on the wavefront, to move to the point of reflection, which is Y1.

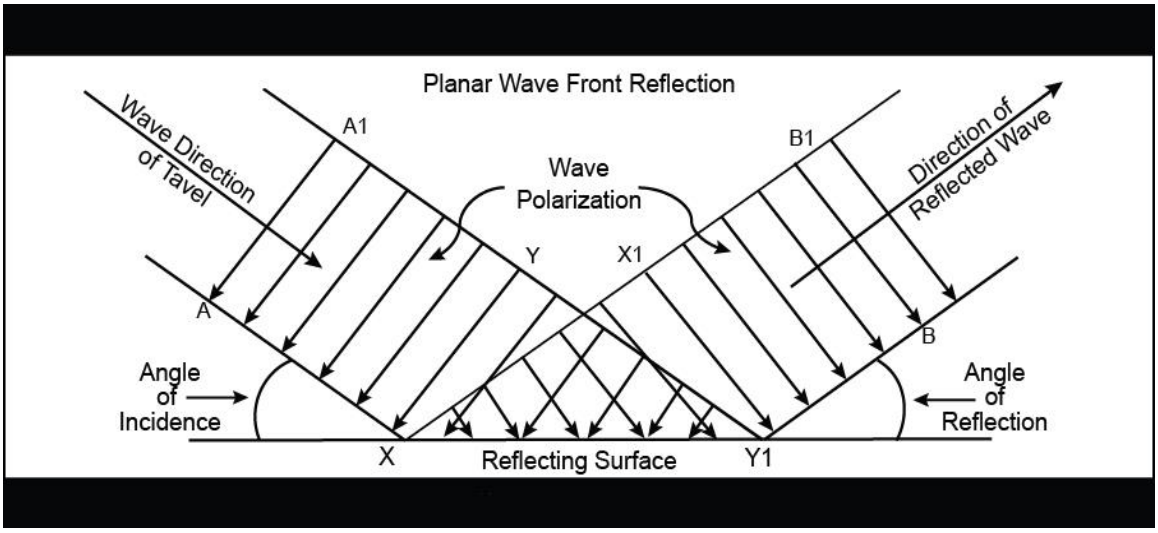

Figure A-11. Planar wavefront reflection

A-49. When a reflected wave and a direct wave arrive at a receiver, the total signal is the vector sum of the two. If the signals are in phase, they reinforce each other, producing a stronger signal. If there is a phase difference, the signals tend to cancel each other, the cancellation being complete if the phase difference is 180 degrees and the two signals have the same amplitude. This interaction of waves is wave interference.

A-50. At lower frequencies, there is no practical solution to counter interference caused in this way. For frequencies in the VHF band (30–300 megahertz) and higher, the operator improves the condition by elevating the antenna, if the wave is vertically polarized. Operators reduce interference at higher frequencies by using directional antennas to avoid reflection.

A-51. Various reflecting surfaces occur in the atmosphere. At high frequencies, reflections occur from the rain. At still higher frequencies, reflections are possible from clouds, particularly rain clouds. Reflections may even occur at a sharply defined boundary surface between air masses, as when warm, moist air flows over cold, dry air. When such a surface is roughly parallel to the surface of the Earth, radio waves may travel for greater distances than normal. The principal source of reflection in the atmosphere is the ionosphere (see paragraphs A-90 through A-98).

REFRACTION

A-52. Refraction involves a change in the direction of waves as a wave passes from one medium to another. Refraction of radio waves is like that of light waves. The direction of travel changes as a signal passes from air of one density to that of a different density. The principal cause of refraction in the atmosphere is the difference in temperature and pressure occurring at various elevations and within different air masses.

A-53. Although refraction occurs at all frequencies, below 30 megahertz, the effect is small in comparison with ionospheric effects, diffraction, and absorption. At higher frequencies, refraction in the lower layer of the atmosphere extends the radio horizon to a distance about 15 percent greater than the visible horizon. The effect is the same as if the radius of the Earth was about one-third greater than it is and there was no refraction.

A-54. Sometimes the lower portion of the atmosphere becomes stratified. This stratification results in nonstandard temperature and moisture changes with height. If there is a marked temperature inversion or a sharp decrease in water vapor content with increased height, a horizontal radio duct form. Super-refraction is when HF radio waves travel horizontally within the duct and refract to the extent that they remain within the duct, following the curvature of the Earth for phenomenal distances (see figure A-12 on page A-16).

Operators achieve maximum results when both transmitting and receiving antennas are within the duct. The lower limit to the frequency affected by ducts varies from about 200 megahertz to more than 1,000 megahertz.

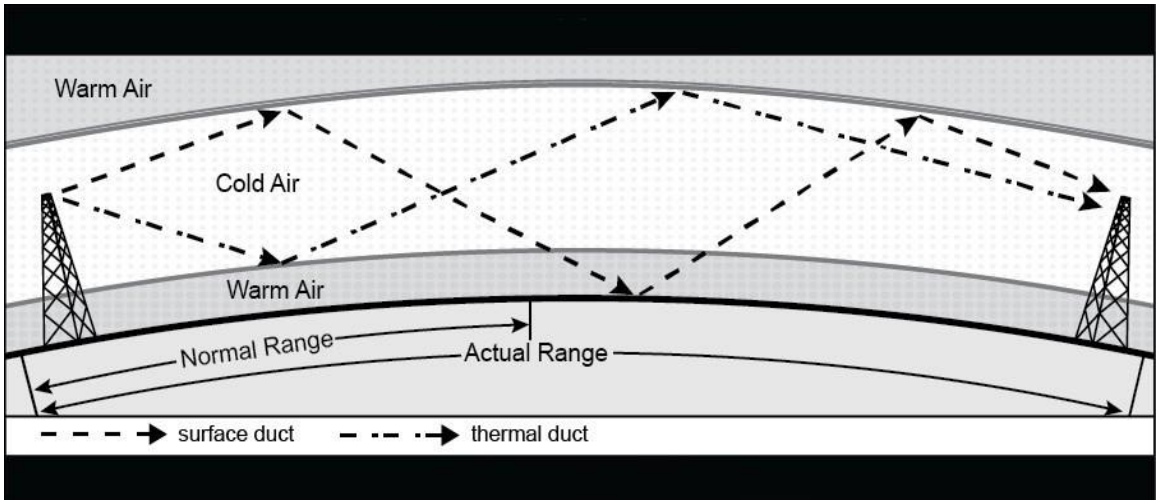

Figure A-12. Super-refraction ducts

A-55. At night, surface ducts may occur over land due to cooling of the surface. At sea, surface ducts about 15 meters (50 feet) thick may occur at any time in the trade wind belt—easterly surface winds found in the tropics near the equator. Surface ducts of 30 meters (100 feet) or more in thickness may extend from land out to sea when warm air from the land flows over the cooler ocean surface. Elevated ducts from about a meter (a few feet) to more than 300 meters (1,000 feet) in thickness may occur at elevations between 300 meters (1,000 feet) to about 457 meters (5,000 feet) because of the settling of a large air mass. Large air masses frequently occur in Southern California and certain areas of the Pacific Ocean.

A-56. Bending in the horizontal plane occurs when a ground wave crosses a coast at an oblique angle because of a marked difference in the conducting and reflecting properties of the land and water over which the wave travels. The effect is the coastal refraction or land effect.

DIFFRACTION

A-57. Radio wave diffraction refers to distortion when a wave encounters an obstacle. Diffraction causes a wave to change direction as it passes around a barrier or through an opening. When a radio wave encounters an obstacle, its energy reflects or absorbs, causing a shadow beyond the obstacle; however, some energy does enter the shadow area because of diffraction. Huygens' Principle states that every point on the surface of a wavefront is a source of radiation transmitting energy in all directions ahead of the wave. No noticeable effect of this principle occurs until the wavefront encounters an obstacle, which intercepts a portion of the wave.

A-58. From the edge of the obstacle, energy radiates into the shadow area and outside of the area. The latter interacts with energy from other parts of the wavefront, producing alternate bands in which the secondary emission reinforces, or tends to cancel, the energy of the primary emission. The practical effect of an obstacle is significantly reduced signal strength in the shadow area, and a disturbed pattern for a short distance outside the shadow area, as illustrated in figure A-13 on page A-17.

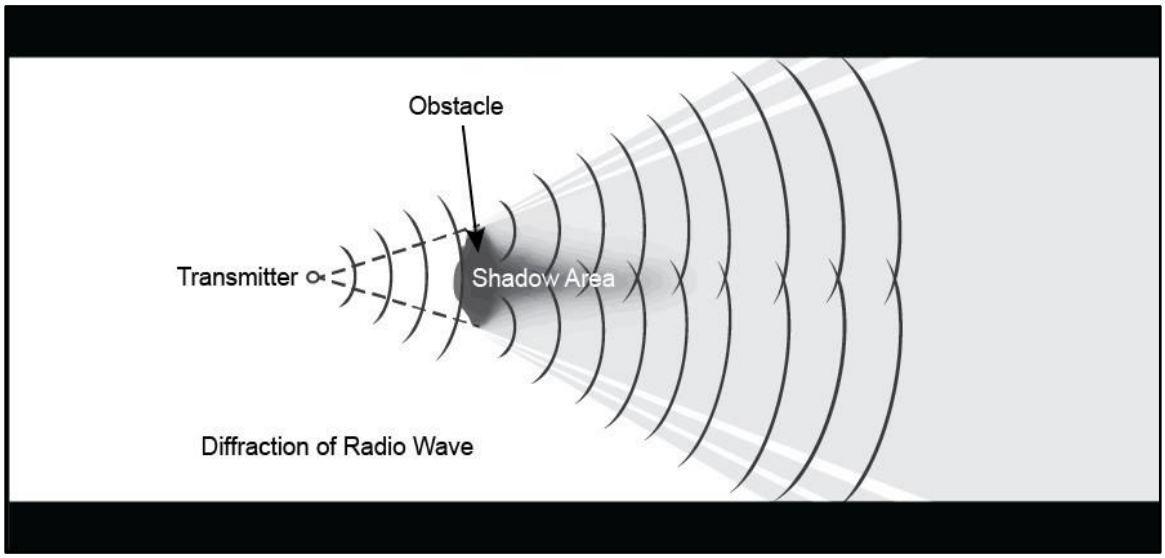

Figure A-13. Diffraction of radio waves around a solid object

A-59. The amount of diffraction is inversely proportional to the frequency, being greatest at very low frequencies. The lower the frequency, or the longer the wavelength, the greater the diffraction. Thus, radio waves diffract more than light or sound waves. Figure A-14 illustrates the why distant station receive radio waves of the proper frequency on the far side of a hill or other natural obstruction.

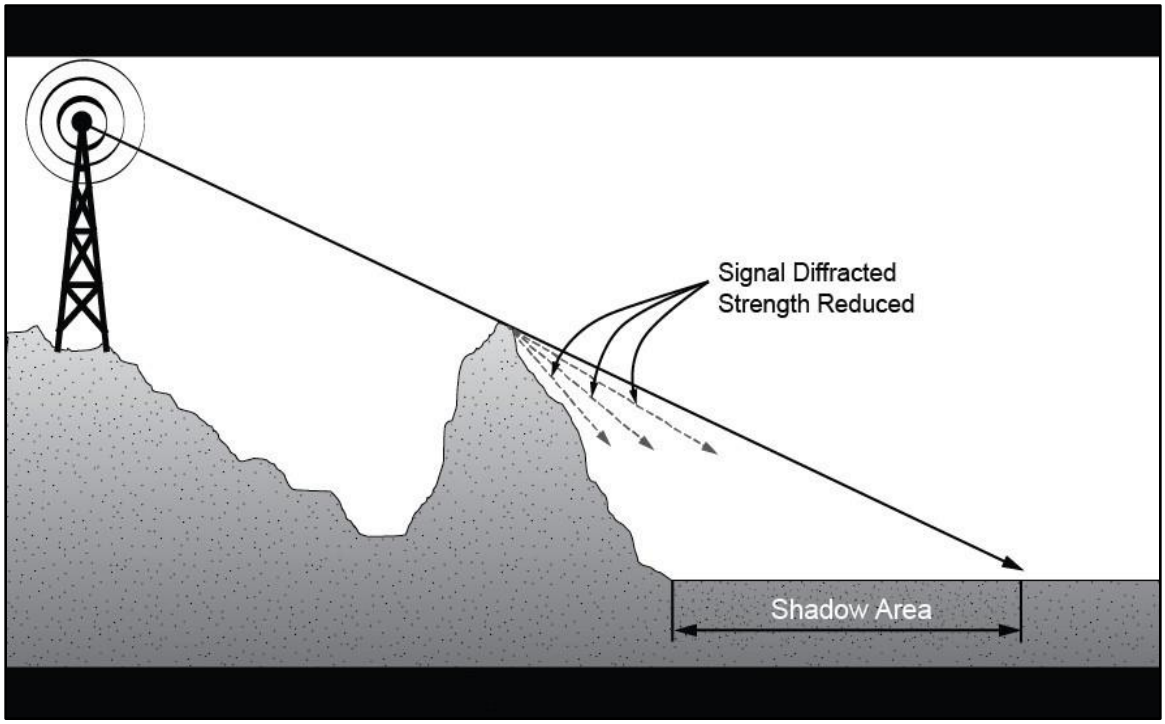

Figure A-14. Diffraction of radio waves around a hillside

ABSORPTION AND SCATTERING

A-60. The amplitude of a radio wave expanding outward through space varies inversely with distance, weakening with increased distance. The decrease of strength with the distance of a radio wave is attenuation.

A-61. A wave traveling along the Earth's surface loses a certain amount of energy as the wave diffracts. Because of this absorption, the remainder of the wavefront tilts downward, resulting in further absorption. Attenuation is greater over a surface that is a poor conductor. Relatively little absorption occurs over seawater, which is an excellent conductor at low frequencies. As a result, low frequency ground waves travel great distances over water.

A-62. Weather also affects the absorption rates of radio waves. Heavy rainfall can cause excessive absorption and may reduce the transmitting and receiving range of frequencies at VHF and above. Attenuation due to fog is determined by the quantity of water per unit volume and by the size of droplets. Fog is of minor importance for frequencies below 2 gigahertz, but can cause serious attenuation at frequencies above 2 gigahertz. Extreme cold will cause radio signals to fade or even cease. Vegetation, such as a jungle environment, also increases absorption and shortens the range of transmitters.

A-63. A skywave (see paragraph A-70) suffers an attenuation loss in its encounter with the ionosphere. The amount depends upon the height and composition of the ionosphere as well as the frequency of the radio wave. Maximum ionospheric absorption occurs at about 1,400 kilohertz.

A-64. In general, atmospheric absorption increases with frequency. It is a problem only in the super-high frequency and extremely high frequency ranges. At these frequencies, attenuation increases by scattering due to reflection by oxygen, water vapor, water droplets, and rain in the atmosphere.

NOISE

A-65. Unwanted signals in a receiver are interference. The intentional production of such interference to obstruct communication is jamming. Unintentional interference is noise.

A-66. Noise may originate within the receiver. A humming sound is usually the result of induction from neighboring circuits carrying alternating current. Poor contacts or faulty components within the receiver cause irregular crackling or sizzling sounds. Stray currents in normal components cause some noise which sets the ultimate limit of sensitivity that used by a receiver. It is the same at any frequency.

A-67. Noise originating outside the receiver may be either fabricated or natural. Fabricated noises originate in electrical appliances, motor and generator brushes, ignition systems, and other sources of sparks that transmit electromagnetic signals picked up by the receiving antenna.

A-68. Atmospheric noise, atmospherics, or static are the discharge of static electricity in the atmosphere and cause natural noise. A thunderstorm is an example of a cause for natural noise. An exposed surface may acquire a more substantial charge of static electricity. Friction from water or solid particles that blow against a surface causes static. Water droplets striking a surface cause positive and negative charge—one part of the droplet requires a positive charge and the other a negative charge. These charges transfer to the surface of the water.

A-69. The charge tends to gather at points and ridges of the conducting surface. When it accumulates enough to overcome the insulating properties of the atmosphere, it discharges into the atmosphere. Under suitable conditions, this becomes visible and is Saint Elmo's fire. Atmospheric noise occurs to some extent at all frequencies but decreases with higher frequencies. Above about 30 megahertz, it is not generally a problem.

FREE-SPACE PATH LOSS

A-70. Usually, the major loss of energy is due to the spreading of a wavefront as it travels away from the transmitter. As the distance increases, the wavefront spreads, like the beam of a flashlight. The amount of energy contained within any area of the wavefront decreases as the distance increases. The free-space path loss calculation excludes environmental effects.

A-71. Decibels is the amount of energy lost between a transmitter and a receiver. The following are typical calculation rules—

- Distance multiplied by 10 results in the loss of 20 decibels.
- Distance doubled results in the loss of 6 decibels.

MULTIPATH INTERFERENCE

A-72. Multipath interference is a phenomenon whereby a wave from a single source travels to a receiver by two or more paths and, provided the wave remains coherent, two (or more) components of the wave interfere with each other. The waves travel along a different path length and arrive at the receiver out of phase with each other, as shown in figure A-15. Multipath fading interferes with the desired signal in amplitude, as well as phase.

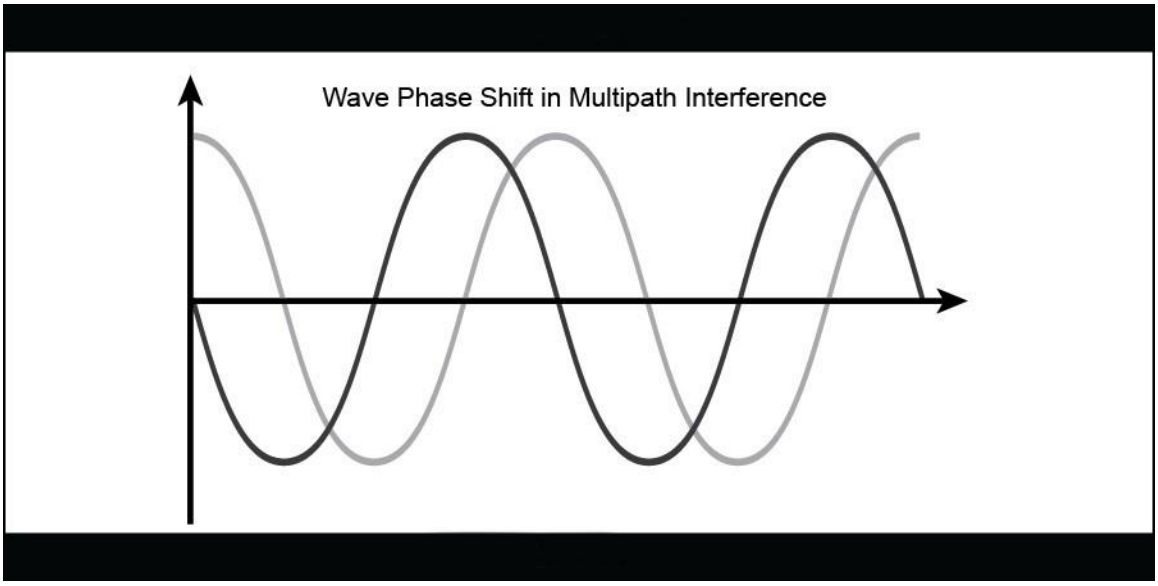

Figure A-15. Phase shift in multipath interference

GROUND WAVE

A-73. The wave that travels along the surface of the Earth is a ground wave. Ground wave propagation is the result of electrical characteristics of the Earth and by the amount of diffraction of the waves along the curvature of the Earth. The strength of the ground wave at the receiver depends on the power output and frequency of the transmitter, the shape and conductivity of Earth along the transmission path, and the local weather conditions.

A-74. A direct wave is a radio wave that travels directly from the transmitting antenna to the receiving antenna, as depicted in figure A-16 on page A-20. This part of the wave is limited to LOS distance between the transmitting and receiving antennas, plus the small distance added by atmospheric refraction and diffraction of the wave along the Earth's curvature. Operators extend this distance by increasing the height of either the transmitting or the receiving antenna, or both.

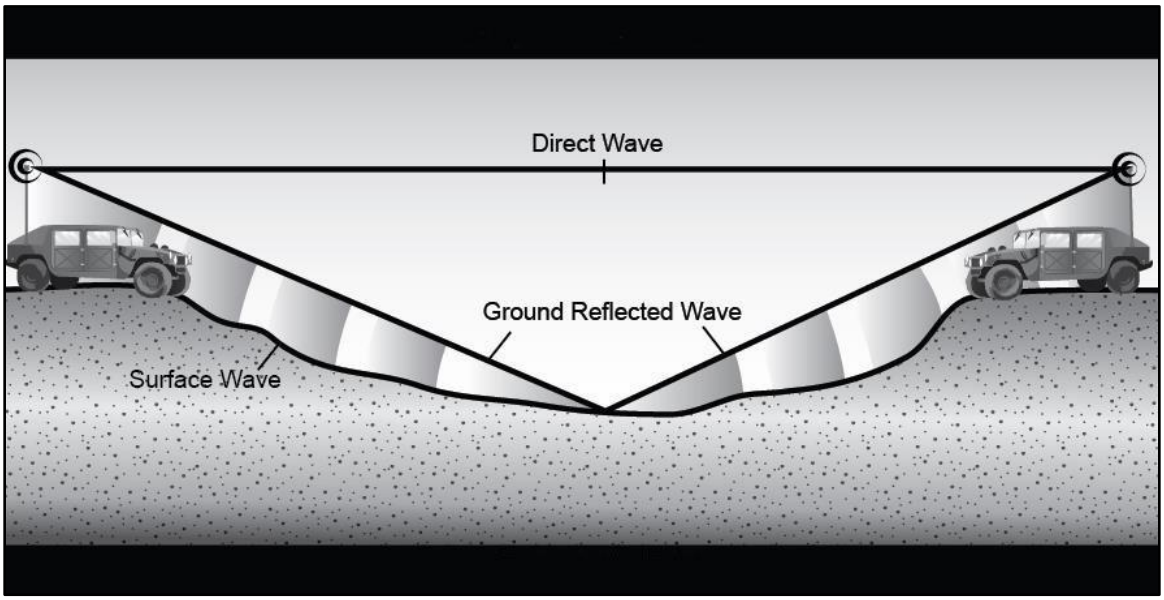

Figure A-16. Possible routes for ground waves

A-75. A ground reflected wave is a radio wave that reaches the receiving antenna after reflecting from Earth's surface. Cancellation of the radio signal can occur when the ground reflected component, and the direct wave component arrive at the receiving antenna simultaneously and are 180 degrees out of phase with each other.

A-76. The conductivity and dielectric constant of the Earth affect the component of a ground wave, which is a surface wave. When both the transmitting and receiving antennas are on, or close to the ground, the direct and ground-reflected components of the wave tend to cancel out, and the resulting field intensity is principally that of the surface wave. However, the surface wave component also affects waves above the Earth's surface. The effect extends to considerable heights, diminishing in field strength with increased height. Because the ground absorbs part of its energy, the electric intensity of the surface wave attenuates at a greater rate. This attenuation depends on the relative conductivity of the surface over which the wave travels (see table A-5).

Table A-5. Propagation characteristics of terrain

Surface Type	*Relative Conductivity*	*Dielectric Constant*
Seawater	Good	80
Large bodies of fresh water	Fair	80
Wet soil	Fair	30
Flat, loamy soil	Fair	15
Dry, rocky terrain	Poor	7
Desert	Poor	4
Jungle	Unusable	Unusable

SKYWAVE

A-77. A skywave is a wave reaching a receiver by way of the ionosphere. When a radio wave encounters a particle with an electric charge, the particle vibrates. The vibrating particle absorbs electromagnetic energy from the radio wave, which it then radiates. The net effect is a change of polarization and an alteration of the path of the wave.

A-78. The higher the frequency, the greater the ionization density required to refract radio waves back to the Earth's surface. The F layer of the ionosphere refracts the higher frequencies because it is the most highly ionized. The E layer's varying ionization creates erratic behavior, refracting medium frequency, HF, and the

lower radio waves. The D layer of the ionosphere, which is the least ionized, primarily absorbs radio waves, though small amounts of refraction are possible but unpredictable.

A-79. At any given time and for each ionized region, there is an upper-frequency limit at which radio waves transmitted vertically are refract back to Earth. This limit is the critical frequency. Radio waves directed vertically, at frequencies higher than the critical frequency, pass through the ionized layer out into space (see Ray 1 in figure A-17). Generally, operators direct radio waves used in communications toward the ionosphere, at an oblique angle called the angle of incidence.

A-80. Radio waves at frequencies above the critical frequency refract back to Earth if transmitted at angles of incidence smaller than a certain angle that is the critical angle. At the critical angle, and at all angles larger than the critical angle, if the frequency is higher than the critical frequency, the radio waves will pass through the ionosphere. At frequencies greater than about 30 megahertz, virtually all the energy penetrates through the ionosphere. As the frequency increases, the required angle decreases.

A-81. Figure A-17 shows Ray 1 entering the ionosphere at an angle that alters the wave and allows it to pass into space. As the horizontal angle decreases, Ray 2 refracts back toward the Earth. As the angle decreases further, such as with Ray 3, the wave returns to Earth at a greater distance from the transmitter.

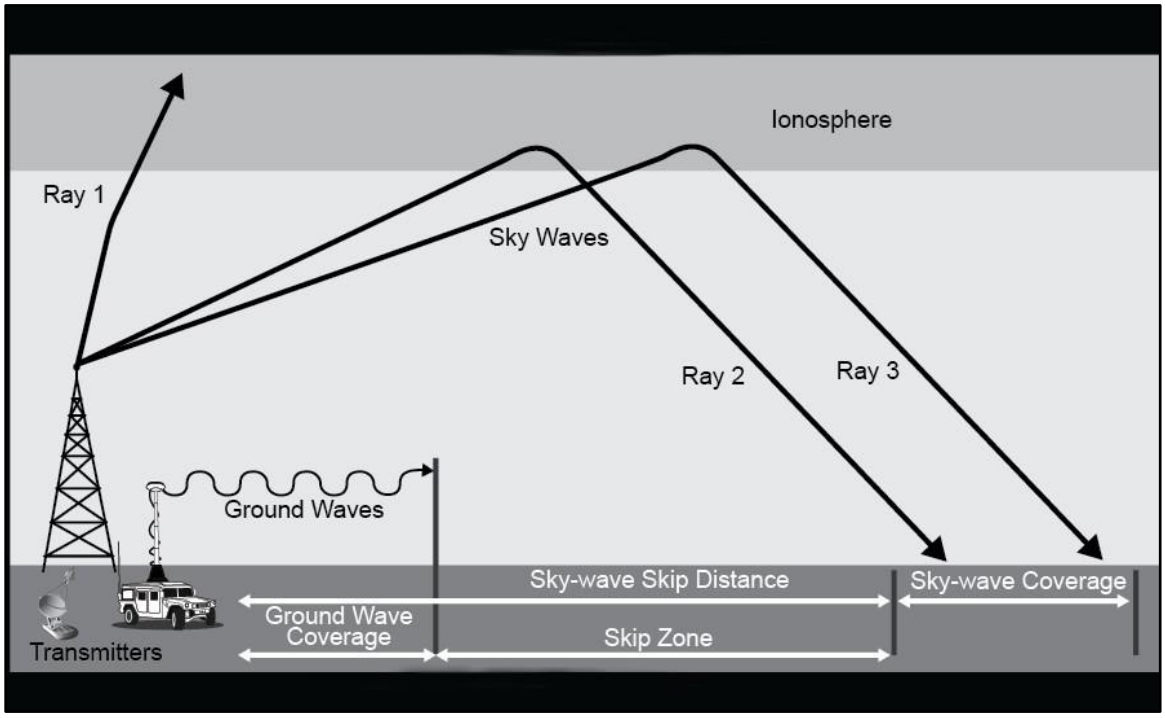

Figure A-17. Relationship between skip zone, skip distance, and ground wave

A-82. At angles greater than the critical angle, the wave passes through the ionosphere, continuing into space. The skip distance is the minimum distance from the transmitter and receiver. See figure A-17. The area where the ground wave extends out for less distance that the skywave is a skip zone.

A-83. A near-vertical transmission path is a near-vertical incidence skywave. A near-vertical incidence skywave usually uses frequencies less than 10 megahertz and can operate on the lower sideband or the upper sideband for voice and data communications. This skywave provides reliable communication, ranging from 50–400 kilometers (30–250 miles), by directing energy at 60–90 degrees, which—provided the frequency or power is not too high—refracts back toward the Earth's surface. This near-vertical angle of transmission reduces the skip zone and can overcome terrain features hampering short distance and beyond LOS communications.

A-84. The antenna height, in relation to the operating frequency, affects the angle at which transmitted radio waves strike the ionosphere. Operators control this angle of incidence to obtain the desired area of coverage.

Lowering the antenna height will increase the angle of transmission and provide a broad and even signal pattern within a region the size of a typical corps' area of operations. Raising the antenna height lowers the angle of incidence. Lowering the angle of incidence produces a skip zone (see figure A-17). In a corps-sized area of operations, the skip zone is not a desirable condition. However, low angles of incidence make long distance communications possible.

A-85. At any given receiver, there is a maximum usable frequency for skywave communication. Acceptable reception occurs between the maximum usable and minimum usable frequencies. The minimum usable frequency is the between the lowest usable frequency and low, unusable frequencies. Within the band of usable frequency, the operator can use the optimum frequency for best reception results. It cannot be too near the maximum usable frequency because this frequency fluctuates with changes of intensity within the ionosphere. During magnetic storms, the ionosphere density decreases. The maximum usable frequency decreases, and the lower usable frequency increases. Radio blackout is when there are no usable frequencies.

A-86. Skywave signals reaching a given receiver may arrive by any of several paths, as shown in figure A-18. A signal that undergoes a single reflection is called a one-hop signal. A signal that undergoes two reflections with a ground reflection between is called a two hop signal, and so forth. A multi-hop signal undergoes several reflections. The layers at which the reflections occur are one hop E, two hop F, and so forth.

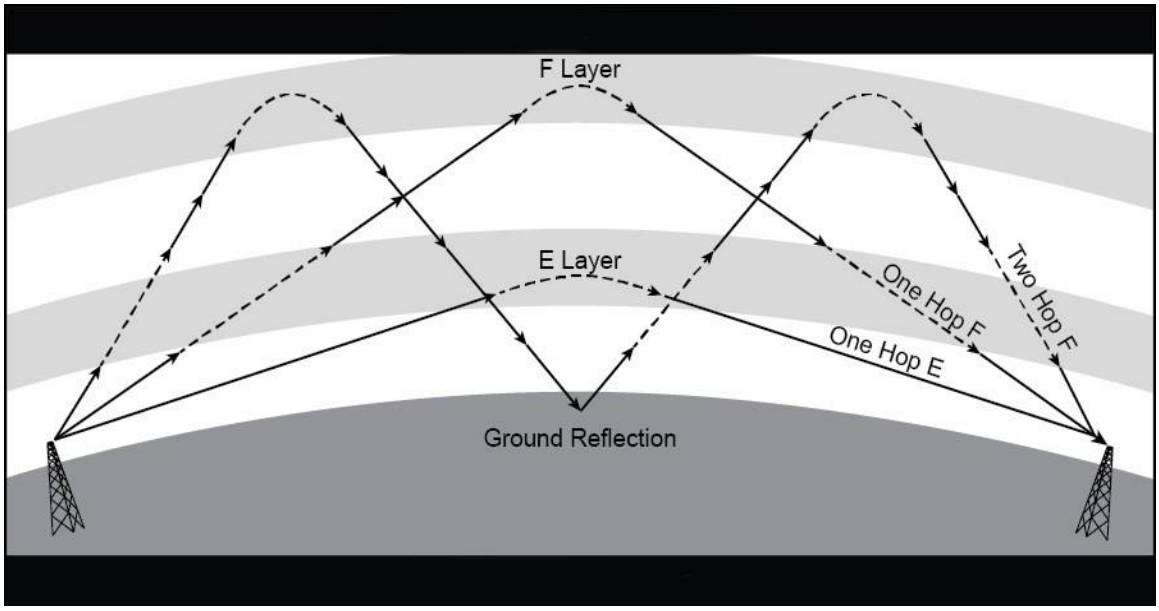

Figure A-18. Skywave paths

A-87. Because of the different paths and phase changes occurring at each reflection, the various signals arriving at a receiver have different phase relationships. Since the density of the ionosphere is continually fluctuating, the strength and phase relationships of the various signals may undergo an almost continuous change. The various signals may reinforce each other at one moment and cancel each other at the next, resulting in fluctuations in the strength of the total signal received known as fading. This phenomenon is a result of the interaction of components within a single reflected wave or reduced strength due to changes in the reflecting surface. Ionospheric changes are associated with fluctuations in the radiation received from the Sun since this is the principal cause of ionization. Signals from the F layer are particularly erratic because of the rapidly fluctuating conditions within the layer itself.

A-88. The maximum distance for a usable, one hop E signal during the daytime is about 2,400 kilometers (1,500 miles). At this distance, the signal leaves the transmitter in approximately a horizontal direction. At night, the E layer decreases and becomes relatively useless for radio transmission. A one-hop F signal is received out to about 4,000 kilometers (2,500 miles). At low frequencies, ground waves extend out for great distances.

A-89. Polarization error occurs when skywave polarization changes during reflection from the ionosphere, accompanied by an alteration in the direction of travel of the wave. Night effect occurs near sunrise and sunset, when rapid changes are occurring in the ionosphere, reception becomes erratic and polarization error a maximum.

A-90. During the daylight hours, the ionosphere is subject to the maximum ultraviolet output from the Sun, bringing the D, E, F1, and F2 layers to their highest reflection potential for higher frequencies.

A-91. At night, the composition of the ionosphere layers change, the D layer disappears, the E layer decreases in strength and the F1 and F2 layers combine. The higher RFs are more likely to penetrate the ionosphere, so operators use lower communications during the night.

A-92. The one exception to the rule concerns operations conducted during the summer. Due to the proximity of the Sun to the Earth and the more prolonged exposure of the ionosphere during this season, operators can use higher frequencies during the day and night. However, one must remember that the actual number of layers, their heights above the Earth, and the relative intensity of ionization present will vary.

MAXIMUM USABLE FREQUENCY

A-93. The maximum usable frequency is the highest frequency at which a radio wave will return to Earth at a given distance when using a given ionized layer and a transmitting antenna with a fixed angle of radiation. The maximum usable frequency is always higher than the critical frequency because the angle of incidence is less than 90 degrees. If the distance between the transmitter and receiver increases, the maximum usable frequency will also increase. At certain frequencies, radio waves lose some energy through absorption by the D layer and a portion of the E layer.

A-94. The total frequency absorption is less, and communication becomes more satisfactory, as operators use higher frequencies—up to the maximum usable frequency level. The absorption rate is greatest for frequencies ranging from 500 kilohertz–2 megahertz during the day. At night, the absorption rate decreases for all frequencies. Table A-6 outlines the general guidance on transmission angles (in degrees) for day and night communications.

Table A-6. Transmission angle and distance

Transmit Angle (degrees)	*Distance to F Layer*			
	Daytime		*Nighttime*	
	Kilometers	*Miles*	*Kilometers*	*Miles*
0	3,220	2,000	4,508	2,800
5	2,415	1,500	3,703	2,300
10	1,932	1,200	2,898	1,800
15	1,450	900	2,254	1,400
20	1,127	700	1,771	1,100
25	966	600	1,610	1,000
30	725	450	1,328	825
70	153	95	290	180
80	80	50	145	90
90	0	0	0	0

LOWEST USABLE FREQUENCY

A-95. As the frequency of transmission over any skywave path decreases, atmospheric noise becomes greater and results in an unacceptable signal-to-noise ratio. The frequency above the point that has too much noise for use is the lowest usable frequency. Frequencies lower than the lowest usable frequencies are too weak for beneficial communications. The lowest usable frequency also depends on the power output of the transmitter as well as the transmission distance. When operators decrease transmission power, the rate of refraction increases. Waves below the lowest usable frequency refract back to the Earth at a shorter distance, as

indicated in figure A-19. When the lowest usable frequency is greater than the maximum usable frequency, skywave communications are not possible.

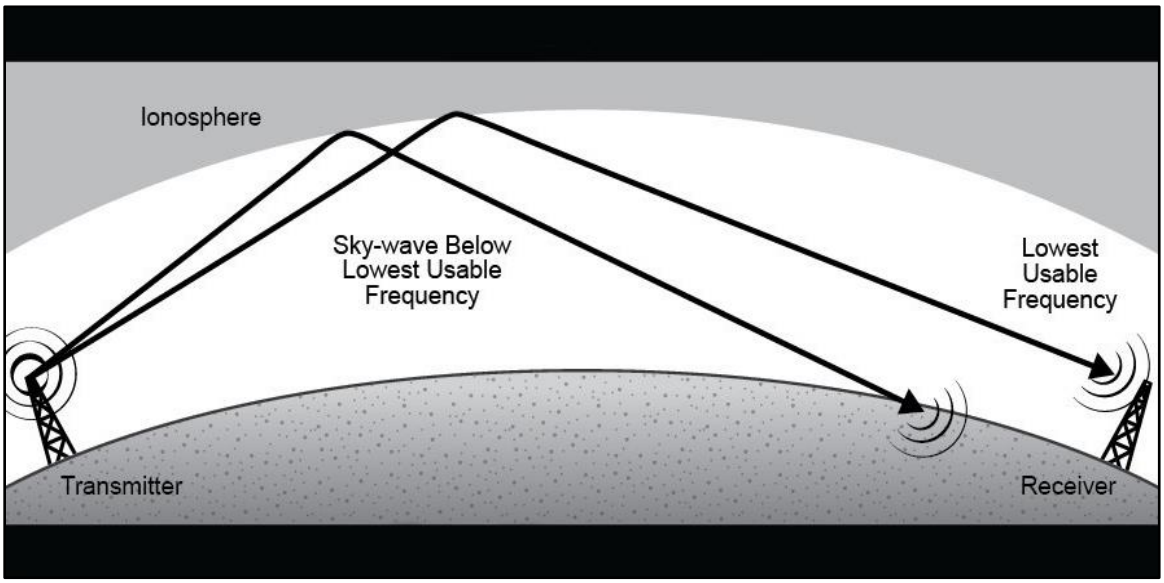

Figure A-19. Refraction of frequency below the lowest usable frequency

REGULAR IONOSPHERE ACTIVITY

A-96. When planning a communications structure, there are regular and irregular ionosphere activities for consideration. Some variations affect or degrade communications and cannot be mitigated. Regular ionosphere activities include—

- Diurnal variations.
- Seasonal.
- Eleven-year sunspot cycle.
- Twenty-seven-day sunspot cycle.

Diurnal Variations

A-97. Daily daytime and nighttime changes occur in the composition and number of ionospheric layers. Skip distance varies and absorption increases during the day; therefore—

- During the day, operators use higher frequencies when ion density of the F2 layer is greater, and frequencies suffer less absorption while passing through the D layer.
- At night, operators use lower frequencies when the D layer disappears.

Seasonal

A-98. As the position of the Sun moves from one hemisphere to the other with corresponding changes in the season, the maximum ion density in the D, E, and F1 layers shift accordingly. Each change is relatively greater during the summer, raising the virtual height of the ionosphere's F2 layer considerably in summer. During winter, the ion density decreases (peaking at noon) and the virtual height of the F2 layer decreases.

Twenty-Seven Day Sunspot Cycle

A-99. This cycle is another sunspot variation resulting from the rotation of the sun on its axis. As the number of sunspots changes from day to day, with solar rotation or the formation of new spots or the disappearance of old ones on the visible part of the sun, absorption by the D layer also changes. Similar changes occur in the E-layer critical frequency. These variations exhibit wide geographic ranges. Although fluctuations in F2

layer critical frequencies from day to day are higher than for any other layer, these fluctuations are not generally of a worldwide character. Because of the variability of the F2 layer, precise predictions of its critical frequencies are not possible for individual days. However, long-term trends and geographical distribution occur in advance.

IRREGULAR IONOSPHERE ACTIVITY

A-100. Irregular ionospheric activity is not accurately predictable. Irregular ionosphere activities include sporadic E, sudden ionospheric disturbance or Dellinger fade, and ionospheric storms.

Sporadic E

A-101. An excessively ionized E layer obscures reflections returning from the higher layers. This phenomenon causes unexpected propagation of a signal hundreds of miles beyond the normal range. This effect, called Sporadic E, frequently occurs during the day and night. However, there is a seasonal pattern, peaking during the summer in both hemispheres with a much smaller peak in winter. An occurrence of Sporadic E is not usually simultaneous at all stations. Operators use lower frequencies to achieve short-hop communications during these conditions.

Ionospheric Storms

A-102. Ionospheric storms usually accompany magnetic disturbances about 18 hours after a sudden ionospheric disturbance; can last for several hours, up to a couple of days; and may extend over a large portion of the Earth. The critical frequencies are much lower than normal because of a decrease in ion density and the virtual heights of the layers much greater so that the maximum usable frequencies are much lower than normal. It is often necessary to lower the working frequency to maintain communications during one of these storms. There is also increased absorption of radio waves during storms. Ionosphere storms are most severe at higher latitudes and decrease in intensity toward the equator.

This page intentionally left blank.

Appendix B

Jamming Calculations

This appendix discusses jamming formula symbols, the minimum jammer power output, and the maximum jammer distance.

FORMULA SYMBOLS

B-1. Electronic warfare professionals use jamming formulas to determine the jamming power output and jammer distance to a target. This information enables the electronic warfare personnel to understand the technical aspects of jamming and establishes the basis for advising the commander on jamming mission characteristics and effects. Mathematical formulas use the symbols in table B-1. Each symbol identifies a unit of measurement used for accurate calculations.

Table B-1. Formula symbols

Symbol	*Use of*
Pj	Minimum amount of jammer power output required in watts (read on power output meter of the jammer).
Pt	Power output of the enemy transmitter in watts.
Hj	Elevation of the jammer location above sea level in feet (does not include antenna height or length).
Ht	Elevation of the enemy transmitter location above the sea level.
Dj	Jammer location-to-target receiver location distance in kilometers.
Dt	Enemy transmitter location-to-target receiver location distance in kilometers.
K	Frequency modulation jammer tuning accuracy factor.
N	Terrain and ground factors: 5 = Very rugged terrain (rocky, mountainous or desert) with poor ground conductivity. 4 = Moderately rugged terrain (rolling to high hills, forests) with fair to good ground conductivity. 3 = Rolling hills (farmland type terrain) with good ground conductivity. 2 = Level terrain (over water, sea, lakes, and ponds) with good ground conductivity.

B-2. Technical intelligence publications and manuals contain the specifications for friendly equipment and threat systems. The G-2 (S-2) provides electronic threat characteristics on threat systems. It is necessary to estimate electronic threat characteristics when no information is available.

FORMULA 1—MINIMUM JAMMER POWER OUTPUT

$$Pj = Pt \times K \times \left(\frac{Ht}{Hj}\right)^2 \times \left(\frac{Dj}{Dt}\right)^n$$

B-3. When the difference between Ht and Hj is less than 10 meters, they are considered the same elevation. When dividing Dj by Dt, include the second decimal place and do not round off. Also, note that this is for a jammer using a whip antenna; divide the result by 2 for a log periodic array antenna. Figure B-1 on page B-2 illustrates a sample calculation.

Calculate the minimum power needed to jam an enemy receiver. The enemy receiver is 17 kilometers from the friendly jammer. The enemy transmitter is rated at 5 watts power output and is located 9 kilometers from its intended receiver location. The enemy transmitter is 385 meters above sea level and the friendly jammer is

Dt = Enemy transmitter to target receiver distance = 9 kilometers
Pj = Maximum power output of friendly jammer = 1500 watts
Pt = Power output of enemy transmitter = 5 watts
Ht = Elevation of enemy transmitter = 385 meters
Hj = Elevation of friendly jammer = 388 meters
K = FM jammer tuning accuracy factor = 2
n = Terrain and ground conductivity factor = 4

$$Pj = \text{Pt x K x} \left(\frac{\text{Ht}}{\text{Hj}}\right)^2 \text{x} \left(\frac{\text{Dj}}{\text{Dt}}\right)^n$$

$$Pj = 5 \text{ x } 2 \text{ x } \left(\frac{385}{388}\right)^2 \text{x} \left(\frac{17}{9}\right)^4$$

$$Pj = 10 \text{ x } (1)^2 \text{ x } (1.88)^4$$

$$Pj = 10 \text{ x } 12.46$$

$$Pj = 124.60 \text{ or } 125 \text{ watts}$$

Therefore, the minimum power output for the friendly jammer must be at least 125 watts with a whip antenna and 62.5 watts with an LPA antenna. Less jammer power output will produce ineffective jamming results.

LEGEND
FM frequency modulation
LPA log periodic array

Figure B-1. Example minimum jammer power output calculations

FORMULA 2—MAXIMUM JAMMER POWER OUTPUT

B-4. This formula is for the determination for the maximum distance of jamming using a whip antenna from the target receiver. For the log periodic array antenna, double the Pj factor. Figure B-2 on page B-3 shows the maximum jammer power output calculation.

Calculate the maximum distance a friendly jammer may be from an enemy receiver. Using the same tactical situation as in figure B-1, the enemy transmitter is rated at 5 watts power output and is located 9 kilometers from its intended receiver location. The enemy transmitter is 385 meters above sea level and the friendly jammer is 388 meters above sea level. The friendly jammer has a maximum power rating of 1500 watts. The terrain is moderately rugged with rolling high hills and forests. Formula data is—

Dt = Enemy transmitter to target receiver distance = 9 kilometers
Pj = Maximum power output of friendly jammer = 1500 watts
Pt = Power output of enemy transmitter = 5 watts
Ht = Elevation of enemy transmitter = 385 meters
Hj = Elevation of friendly jammer = 388 meters
K = FM jammer tuning accuracy factor = 2
n = Terrain and ground conductivity factor = 4

$$Dj = \mathrm{Dt} \times \sqrt[n]{\frac{Pj}{Pt \times K \times \left(\frac{Ht}{Hj}\right)^2}}$$

$$Dj = 9 \times \sqrt[4]{\frac{1500}{5 \times 2 \times \left(\frac{385}{388}\right)^2}}$$

$$Dj = 9 \times \sqrt[4]{\frac{1500}{10 \times (1)^2}}$$

$$Dj = 9 \times \sqrt[4]{\frac{1500}{10}}$$

$$Dj = 9 \times \sqrt[4]{150}$$

$$Dj = 9 \times 3.5 = 31.5 \text{ km}$$

Therefore, the jammer using a whip antenna may be located a maximum of 31.5 kilometers from the enemy receiver. For a jammer using the LPA antenna, use 3000 watts for Pj and the result is 37.44 kilometers.

LEGEND

FM frequency modulation
LPA log periodic array

Figure B-2. Example maximum jammer power output calculation

This page intentionally left blank.

Appendix C

Electronic Warfare Equipment and Systems

Due to the complex nature of combat, successful unified land operations require action in all domains. Units use available joint electronic warfare resources to support the commander's intent. This appendix includes characteristics of Army and joint equipment that is useful in electronic warfare planning.

ARMY

C-1. The Army is currently increasing its EW capabilities. It maintains several EW systems in its inventory. When requested, the Army provides these capabilities to corps and below.

ELECTRONIC WARFARE PLANNING AND MANAGEMENT TOOL

C-2. The CEWO uses the Electronic Warfare Planning and Management Tool (EWPMT) to visualize and simulate the behavior of EMS in the area of operations resources before executing an EW mission. The CEWO also shares the view of the EME with the staff. The CEWO uses EWPMT to analyze the likely threat EW course of action and electronic threat characteristics provided by the G-2 (S-2) staff. The EWPMT provides an automated platform that enables the CEWO to provide the following—

- Provide input to the common operational picture.
- Display sensor information from deployed EW and SIGINT assets including—
  - Detected emitters.
  - Plot lines of bearing.
  - Analysis of circular error probable ellipse.
- Conduct mission planning and rehearsals.
- Manage EW assets.
- Model and visualize how the EME responds to friendly and enemy EW activities.

C-3. The CEMA section loads and configures the required data on the EWPMT prior to operations and connects to services for updates and provide information to the rest of the staff. The CEMA section coordinates with the network management technician assigned to the G-6 (S-6) staff for network configurations such as the specified Internet protocol address and computer name. The network management technician also ensures that the EWPMT has connectivity with the data distribution service. The data distribution service facilitates near, real-time data sharing for information systems. The connectivity to the data distribution service allows EWPMT to integrate with other mission command information systems to publish and subscribe to the organization's common operational picture products and assist in achieving a higher level of situational understanding. The map data for EWPMT is available from the National Geospatial-Intelligence Agency.

COUNTER RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICE ELECTRONIC WARFARE SYSTEMS

C-4. CREW systems form a family of EA systems. Although the Army has the largest inventory, all U.S. ground forces use these systems to prevent improvised explosive device detonation by RF energy. These forces maintain a mounted, dismounted, and fixed-site CREW capability to protect personnel and equipment. As technology improves, the capabilities of some systems have progressed beyond mere jamming to providing information collection and DF. The systems currently in use by U.S. forces and multinational partners include—

- Mounted—
  - AN/VLQ-12 Duke V2/V3 (Army).
  - Symphony (coalition).
  - EGON Active/Reactive Counter-IED System (special operations forces).
- Dismounted—
  - AN/PLQ-9 Thor III (joint).
  - AN/PLT-5 Thor II (explosive ordnance disposal).
  - Baldr.
  - Guardian H3 (North Atlantic Treaty Organization)
  - Modi (conventional and non-conventional).
- Other—AN/GLM-11 (V)1, Universal Test Set.

C-5. Jammers may function in an active or reactive mode. Active means the jammer continuously emits a signal to block a preprogrammed frequency. It is effective against multiple low-power signals but is vulnerable to threat DF equipment and may not be effective against high-power signals. Reactive jammers search for specific signals and then emit the jamming signal. Reactive jammers are less vulnerable to DF equipment and are excellent against high-power signals.

AIRCRAFT SURVIVABILITY EQUIPMENT

C-6. Aircraft survivability equipment aims to reduce aircraft vulnerability, thus allowing aircrews to accomplish their immediate mission and survive. Army aviation maintains a suite of aircraft survivability equipment that provides EP against threat weapon systems within the EMS for detection, tracking, and targeting. This protection can include RF warning and countermeasures systems, a common missile warning system, information requirement countermeasures systems, and laser detection and countermeasure systems.

INTELLIGENCE SYSTEMS

C-7. The intelligence community operates and maintains systems capable of providing ES information. Usually, the information is collected, consolidated as data, and becomes SIGINT, but the additional capability can also provide the limited information for ES purposes. The systems and operators must use the correct authority and procedures when operating for either SIGINT or ES, without confusing classifications or missions.

Guardrail Common Sensor

C-8. The Guardrail Common Sensor is a corps-level, airborne SIGINT collection and locating system. It provides tactical commanders with near real-time targeting information. Key features include the following—

- Integrated communications intelligence and electronic intelligence reporting.
- Enhanced signal classification and recognition.
- Near real-time DF.

C-9. The Guardrail common sensor shares technology with the ground-based common sensor, airborne reconnaissance-low, and other joint systems.

Prophet Enhanced

C-10. Prophet Enhanced is a ground-based tactical SIGINT system. This system contributes to force protection and situational awareness through intelligence support to units.

Spectrum Tools

C-11. Host nations have EMS usage plans that assist in the management of frequencies. The spectrum manager in the G-6 (S-6) assists the CEMA section in frequency use authorization for EW activities. The G-6 (S-6) spectrum manager requests frequency resources through Spectrum XXI or by liaising with the Combatant Command or the Host Nation.

C-12. The End-to-End Supportability System (E2ESS) is a web application that facilitates warfighter deployment and communications by providing worldwide visibility of host supportability of spectrum dependent devices (SDD). The E2ESS automates the distribution of host nation coordination requests allowing combatant command submission for host nation supportability, reducing time requirements for managing the host nation spectrum authorization process. The design of the database provides informed decision making concerning frequency bands. E2ESS is a database of automates the distribution host nation coordination requests and combatant command submission of host nation supportability comments. It enables managers to determine the historical EMS supportability of similar systems.

AIR FORCE

C-13. The Air Force has two primary platforms that provide EW capabilities—

- EC-130H Compass Call.
- RC-135V/W Rivet Joint.

EC-130H COMPASS CALL

C-14. The EC-130H Compass Call is an airborne tactical weapon system. The EC-130H provides degrade and disrupt effects of threat communications systems and radars used to support threat ground, air, or maritime operations; and many modern commercial communication signals that a threat might employ.

RC-135V/W RIVET JOINT

C-15. The RC-135V/W Rivet Joint is a combatant-command-level surveillance asset that responds to strategic tasks. The RC-135V/W Rivet Joint is equipped with information gathering equipment that enables monitoring of threat electronic activity. The aircraft has secure communications using HF, VHF and UHF spectrum resources as well as satellite communications.

MARINE CORPS

C-16. The Marine Corps uses a variety of EW systems and supporting systems to execute their tactical EW missions. Like the other Services, equipment and techniques change based on threat and technology.

AN/ULQ-19(V)2 ELECTRONIC ATTACK SET

C-17. The AN/ULQ-19(V)2 electronic attack set allows operators to conduct spot or sweep jamming of single-channel voice or data signals operating in the standard military frequency range of 20–79.975 megahertz from selected mobile platforms—for example, high mobility multipurpose wheeled vehicles, mobile electronic warfare support system (MEWSS), helicopters. When employed as a tactical, general purpose, low-VHF jamming system, the AN/ULQ-19(V)2 has a 250-watt RF linear amplifier that produces a nominal 200 watts of effective radiated power using a standard omnidirectional whip antenna. To provide jamming, the system must operate with an unobstructed signal LOS to the target enemy's communications transceiver.

AN/MLQ-36 MOBILE ELECTRONIC WARFARE SUPPORT SYSTEM

C-18. The AN/MLQ-36 MEWSS provides a multifunctional capability that provides limited armor protection for SIGINT and EW operators. This equipment can provide SIGINT and EW support to highly mobile mechanized and military operations in urban terrain where maneuver and/or armor protection is critical. MEWSS consists of a signals intercept system, a radio DF system, an EA system, a secure communications system, and an intercom system installed in a logistic variant of the light armored vehicle. The AN/MLQ-36A MEWSS product improvement program (PIP) is an advanced SIGINT and EW system integrated into a light armored vehicle.

C-19. The MEWSS PIP provides a total replacement of the EW mission equipment now fielded in the AN/MLQ-36 MEWSS. The MEWSS PIP provides the ability to detect and evaluate enemy communications emissions, detect, and categorize enemy noncommunications emissions, determine lines of bearing, and degrade enemy tactical radio communications during expeditionary operations. When mission-configured and working cooperatively with other MEWSS PIP platforms, the common suite of equipment can also provide precision location of battlefield emitters. The system has an automated tasking and reporting data link available to other Marine air-ground task force assets such as the AN/TSQ-130 technical control and analysis center PIP. The MEWSS PIP and its future enhancements will provide the capability to exploit new and sophisticated enemy electronic emissions and conduct electronic attack in support of existing and planned national, theater, fleet, and Marine air-ground task force SIGINT and EW operations.

NAVY

C-20. The Navy's primary airborne EW platform is the E/A-18G Growler. The Navy also maintains both surface and subsurface EW shipboard systems for offensive and defensive missions to support the fleet. For further information on Navy missions and equipment, refer to Navy Warfare Publication 3-13.

C-21. The E/A-18G Growler is the Navy's replacement aircraft for the EA-6B Prowler. The E/A-18G Growler's general capabilities include—

- Suppression of threat air defenses. The EA-18G Growler counters threat air defenses using both reactive and preemptive jamming techniques.
- Standoff and escort jamming.
- Integrated air and ground airborne EA.
- Self-protect and time-critical strike support. With its active electronically scanned array radar, digital data links, and air-to-air missiles, the EA-18G Growler can protect itself and effectively identify and prosecute targets.

C-22. The E/A-18G Growler's airborne EA capabilities are—

- Effectiveness against any surface-to-air threat.
- Sense and locate threats.
- Uninterrupted communications during jamming operations.

Appendix D
Forms, Reports, and Messages

Electronic warfare professionals use several different forms, reports, and messages in the performance of their duties. The common, prescribed forms are included in this appendix.

ELECTRONIC ATTACK REQUEST FORMAT

D-1. The CEWO requests effects using the EARF to (see table D-1).

Table D-1. Electronic attack request format instructions

<table>
<tr><td colspan="2">Requesting Major Support Command:</td></tr>
<tr><td colspan="2">Requesting Unit:</td></tr>
<tr><td colspan="2">Contact information: This person will be responsible to verify approved request before the mission starts and to relay the information to the executing unit.</td></tr>
<tr><td colspan="2">Joint Tactical Air Strike Request Number: Enter the joint tactical air strike request number for submission with the electronic attack request format.</td></tr>
<tr><td colspan="2">Concept of Operations: Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to specific objectives for the integrated tasking order.</td></tr>
<tr><td colspan="2">Electronic Attack Concept of Operations: Define the desired effect(s) and timeline.</td></tr>
<tr><td colspan="2">CEASE BUZZER Procedures: This will be in accordance with theater special instructions. Provide frequency to communicate between the jamming control authority and electronic attack asset. VHF and UHF are the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be internet relay chat capable.</td></tr>
<tr><td colspan="2">Friendly Frequency Use for Operation:</td></tr>
<tr><td>Target Communication System(s) to be Jammed or Denied:</td><td>Target requested—list the type and frequency, if known.
Intelligence assessment (required—do not copy and paste frequencies from one day to the next without intelligence validation assessment).
Target Location in latitude and longitude or military grid reference system.</td></tr>
<tr><td colspan="2">Jamming date-time group(s): From and to, in Zulu Time (preferred):</td></tr>
<tr><td colspan="2">Type of Electronic Attack Requested: Preplanned and scheduled on-call:</td></tr>
<tr><td colspan="2">Legend:
VHF very high frequency
UHF ultrahigh frequency</td></tr>
</table>

JOINT TACTICAL AIR STRIKE REQUEST

D-2. CEWOs use DD Form 1972, *Joint Tactical Air Strike Request*, to request an airborne EA support. The JTASR specifies the effects desired using air and space power (see figure D-1). The CEWO's completion of the JTASR is critical to helping air planners in the combat air operations center to select the aircraft and payload to support the JTASR. To ensure the air component achieves the effects desired by the ground component, the JTASR must describe clear and detailed effects. Most organizations require the submission of a JTASR and an EARF together. The JTASR and EARF must complement each other. JP 3-09.3 contains the line-by-line instructions for completing both forms. Once filled with operational information, the DD Form 1972 becomes classified SECRET. This sample is not classified.

JOINT TACTICAL AIR STRIKE REQUEST — See Joint Pub 3-09.3 for preparation instructions.

SECTION I - MISSION REQUEST

1. UNIT CALLED: Chieftan | THIS IS: Gator 01 | REQUEST NUMBER: IA9501-A | DATE SENT: TIME 1615 BY MAJ Smith

2. PREPLANNED: A PRECEDENCE 4 B PRIORITY II | IMMEDIATE: C PRIORITY | RECEIVED: TIME 1615 BY SrA Ford

3. TARGET IS/NUMBER OF
A PERS IN OPEN 20-30 | B PERS DUG IN | C WPNS/MG/RR/AT | D MORTARS, ARTY
E AAA ADA | F RKTS MISSILE | G ARMOR 3xBTR in a line | H VEHICLES 4 Stationary
I BLDGS 2 | J BRIDGES | K PILLBOX, BUNKERS | L SUPPLIES, EQUIP
M CENTER (CP, COM) | N AREA | O ROUTE | P MOVING N E S W
Q REMARKS

4. TARGET LOCATION IS — CHECKED BY: SSgt INTEL
A 11SUG8005 (COORDINATES) | B (COORDINATES) | C (COORDINATES) | D (COORDINATES)
E TGT ELEV 10 | F SHEET NO. 2857 II | G SERIES V795S | H CHART NO.

5. TARGET TIME/DATE
A ASAP | B NLT 1600 | C AT | D TO

6. DESIRED ORD RESULTS — A ORDNANCE LGB/Guns
B DESTROY | C NEUTRALIZE X | D HARASS INTERDICT

7. FINAL CONTROL
A FAC/RABFAC II | B CALL SIGN GATOR 20 | C FREQ ORANGE 17
D CONT PT JACKS

8. REMARKS

SECTION II - COORDINATION

9. NOFS: 4XTLAM FLA 1 SS | 10. ARTY | 11. AIO/G-2/G-3

12. REQUEST: [X] APPROVED [ ] DISAPPROVED | 13. BY: MAJ Hughes | 14. REASON FOR DISAPPROVAL

15. RESTRICTIVE FIRE/AIR PLAN: A IS NOT IN EFFECT | B NUMBER | 16. IS IN EFFECT: A (FROM TIME) | B (TO TIME)

17. LOCATION: A (FROM COORDINATES) | B (TO COORDINATES) | 18. WIDTH (METERS) | 19. ALTITUDE/VERTEX: A (MAXIMUM/VERTEX) | B (MINIMUM)

SECTION III - MISSION DATA

20. MISSION NUMBER	21. CALL SIGN	22. NO. AND TYPE AIRCRAFT	23. ORDNANCE
3021/3022	Razor 51/52 Venom 16/17	(2) AV-8B (2) AH-1Z	SCL 1/3
24. EST/ACT TAKEOFF	**25. EST TOT**	**26. CONT PT (COORDS)**	**27. INITIAL CONTACT**
1424	1438	Breaker	
28. FAC/FAC(A)/TAC(A) CALL SIGN/ FREQ	**29. AIRSPACE COORDINATION AREA**	**30. TGT DESCRIPTION**	***31. TGT COORD/ELEV**

32. BATTLE DAMAGE ASSESSMENT (BDA) REPORT (USMTF INFLTREP)
LINE 1/CALL SIGN Razor 51/52 | LINE 4/LOCATION 18SUG8005
LINE 2/MSN NUMBER 3021/3022 | LINE 5/TOT 1454
LINE 3/REQ NUMBER 1A9501-A | LINE 6/RESULTS Neutralize/Destroy
REMARKS | *TRANSMIT AS APPROPRIATE

DD FORM 1972, MAY 2019 — PREVIOUS EDITION MAY BE USED. — Adobe Professional 7.0

SAMPLE

Figure D-1. Sample joint tactical air strike request

JOINT SPECTRUM INTERFERENCE RESOLUTION REPORT

D-3. Sharing information contained in the completed JSIR helps the unit build situational understanding of the threat and aids in the development of mitigation procedures. The report preparer provides a copy of the completed form to the CEWO, spectrum manager, and G-6 (S-6) staff.

D-4. Operators encountering EMI use the JSIR-Online. The JSIR-Online portal is located on the SECRET Internet Protocol Router Network. Unit SOPs may also require JSIR approval from the chain of command using the JSIR format in figure D-2. The report preparer provides a copy of the completed form to the CEWO, spectrum manager, and G-6 (S-6) staff.

Format for Manually Prepared
Joint Spectrum Interference Resolution Report.

Date of Report: When the report was prepared; not when interference occurred.

1. Originator/Report Preparer Information: Identify the person preparing this report to assist with follow-up actions or questions. Include title, name, organization, location, telephone number, and e-mail address in enough detail to allow anyone reading the report to identify the preparer of this report.
2. Organization Experiencing the Interference Information: Identify the organization by name and location; provide a point of contact with first-hand knowledge of the interference. If the report originator or preparer is the same as the unit point of contact, then state "POC same as originator" or words to that effect.
3. Where and when interference occurred:
   a) Date(s): (include entire date range if more than one day).
   b) Time period: (use precise hour and minute of start and end time, if known).
   c) State/country: (provide geographic name).
   d) Location: (briefly describe the location such as, "on a road through a mountain valley…")
   e) Coordinates: (military grid or latitude and longitude).
4. Description of the type of interference: (meaconing, intrusion, jamming, or interference).
5. Description of the system and radio frequency disrupted or degraded: (nomenclature and frequency/frequencies).
6. Impact of interference to the mission: (describe how the interference is affecting the unit's ability to accomplish the mission).
7. Report all local actions and troubleshooting that have been taken to resolve the problem: (attach additional pictures or documents to report troubleshooting) (Identify the steps taken and whether those efforts had any effect on the interference).
8. Type of assistance required: (indicate specific actions the affected unit would like to occur to mitigate the interference).
9. Cause of interference (if known): (identify what caused the interference and how this determination was made).
10. Recommendation for improving resolution techniques or new frequency allocation: (only filled out by the spectrum investigating unit or frequency manager).

Figure D-2. Joint spectrum interference resolution report instructions

STOP JAMMING MESSAGE

D-5. To stop jamming, the CEWO submits a stop jamming message (see figure D-3 on page D-4).

STOP JAMMING MESSAGE

GENERAL INSTRUCTIONS: Use to terminate a jamming task conducted by an electronic attack (EA) asset.

LINE 1 – DATE & TIME: (Date-time group of when jamming should be terminated).

LINE 2 – UNIT: (Unit supported by jamming mission and is requesting termination).

LINE 3 – FREQUENCY: (Enter the radio frequency being jammed or enter "ALL" if jamming is to stop on all jammed frequencies).

LINE 4 – NARRATIVE: (Any additional information required for clarification).

LINE 5 – AUTHENTICATION: (Message authentication if unit standard operating procedures require authentication).

Figure D-3. Stop jamming message instructions

ELECTRONIC WARFARE FREQUENCY DECONFLICTION MESSAGE

D-6. The CEWO completes an electronic warfare frequency deconfliction message to stop jamming activities (see figure D-4).

ELECTRONIC WARFARE FREQUENCY DECONFLICTION MESSAGE (EWDECONFLICT)

REPORT NUMBER: E005 {USMTF #F402}

GENERAL INSTRUCTIONS: Use to promulgate a list of protected, guarded, and taboo frequencies to ensure friendly force use of the frequency spectrum without adverse impact from friendly electronic attack.

Reference: ATP 3-12.3

LINE 1: DATE AND TIME _____	(DTG)
LINE 2: UNIT _____	(Unit making report)
LINE 3: TYPE _____	(Taboo, protect, or guard)
LINE 4: STATUS _____	(Restricted status of frequency: new, change, cancel, or renew)
LINE 5: FREQUENCY _____	(Frequency/frequencies)
LINE 6: ON TIME _____	(Start DTG of frequency restriction)
LINE 7: OFF TIME _____	(End DTG of frequency restriction)
LINE 8: LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid zone designator)

** Repeat lines 3 through 8 as a group to accommodate multiple reports. Assign sequential line numbers to succeeding iterations; for example, first iteration 3 through 8; second iteration 3a through 8a; and so on.

LINE 9: NARRATIVE _____	(Free text for additional information required for clarification of report)
LINE 10: AUTHENTICATION _____	(Report authentication

Legend:

DTG	date-time group
MGRS	military grid reference system
UTM	universal transverse mercator

Figure D-4. Electronic warfare frequency deconfliction message instructions

ELECTRONIC WARFARE MISSION SUMMARY

D-7. The CEWO maintains a record of EW missions. The record is the EW mission summary (see figure D-5 on pages D-5 and D-6).

Electronic Warfare Mission Summary [EWMSNSUM]

REPORT NUMBER: E010 {USMTF #G424}
GENERAL INSTRUCTIONS: Use to summarize significant EW missions and the status of offensive EW assets.
Reference: ATP 3-12.3

LINE 1: DATE AND TIME _____	(DTG)
LINE 2: UNIT _____	(Unit making report)
LINE 3: FROM _____	(Beginning DTG [zulu] of period summarized)
LINE 4: THROUGH _____	(Ending DTG [zulu] of period summarized)
LINE 5: COUNTRY _____	(Nationality of the target emitter of concern)
LINE 6: LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid zone designator.
LINE 7: EMITTER _____	(Emitter call sign and name or nomenclature)
LINE 8: FUNCTION _____	(Primary function of target)
LINE 9: NOTATION _____	(Notation or sorting code)
LINE 10: SIGNAL _____	(Type of signal or target emitter)
LINE 11: ON TIME _____	(DTG that planned EA activity initiated)
LINE 12: OFF TIME _____	(DTG that planned EA activity terminated)
LINE 13: PRIORITY _____	(Relative importance of EA mission)
LINE 14: TYPE _____	(Type of EA used against the emitter)
LINE 15: PRIMARY FREQUENCY _____	(Primary frequency of EA target signal)
LINE 16: SECONDARY FREQUENCY _____	(Secondary frequency of EA target signal)
LINE 17: LOW FREQUENCY _____	(Lower frequency limit of target equipment class)
LINE 18: HIGH FREQUENCY _____	(Upper frequency limit of target equipment class)
LINE 19: BANDWIDTH _____	(Target frequency bandwidth in MHz)
LINE 20: PULSE REPETITION _____	(Pulse repetition interval or frequency)
LINE 21: SYSTEM USED _____	(Nomenclature of EW asset used)
LINE 22: OPERATIONAL _____	(Number of units that can perform primary EW mission)
LINE 23: NONOPERATIONAL _____	(Number of units that cannot perform primary EW mission)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electronic attack	MHz	megahertz
EW	electronic warfare	UTM	universal transverse mercator

Figure D-5. Electronic warfare mission summary instructions

LINE 24: DESTROYED _____	(Number of units that were destroyed in combat)
LINE 25: CHAFF _____	(Type of chaff)
LINE 26: LOWER FREQUENCY _____	(Lower frequency of a range blanked by chaff or lower EA frequency)
LINE 27: UPPER FREQUENCY _____	(Upper frequency of a range blanked by chaff or lower EA frequency)
LINE 28: LOW LEVEL _____	(Lower altitude in hundreds of feet of airspace blanked by chaff)
LINE 29: UPPER LEVEL _____	(Upper altitude in hundreds of feet of airspace blanked by chaff)
LINE 30: TECHNIQUE _____	(EA technique employed)
LINE 31: COUNTRY _____	(Country in which chaff was employed)
LINE 32: ON TIME _____	(DTG the chaff drop was initiated)
LINE 33: OFF TIME _____	(DTG the chaff drop was terminated)
LINE 34: START LOCATION _____	(Start location of chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 35: STOP LOCATION _____	(Stop location of chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 36: NARRATIVE _____	(Free test for additional clarifying information)
LINE 37: AUTHENTICATION _____	(Report authentication)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electronic attack	UTM	universal transverse mercator

Figure D-5. Electronic warfare mission summary instructions (continued)

ELECTRONIC WARFARE TASKING MESSAGE

D-8. The CEWO uses the electronic warfare tasking message format to task an EW asset to provide a requested effect (see figure D-6 on page D-7 through D-8).

Electronic Warfare Tasking Message [EWTM]

REPORT NUMBER: E010 {USMTF #A426}
GENERAL INSTRUCTIONS: Use to (1) task component commanders to perform EW operations to support the overall EW plan; (2) support component EW operations; or (3) request EW support from sources outside the command.
Reference: ATP 3-12.3

LINE 1: DATE AND TIME _____	(DTG)
LINE 2: UNIT _____	(Unit making report)
LINE 3: EA _____	(Electronic attack activity requested)
LINE 4: TASKED _____	(Designator of tasked unit if the JOC is tasking the unit)
LINE 5: COUNTRY _____	(Nationality of the target emitter of concern)
LINE 6: LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid zone designator.
LINE 7: EMITTER _____	(Emitter call sign and name or nomenclature)
LINE 8: FUNCTION _____	(Primary function of target)
LINE 9: NOTATION _____	(Notation or sorting code)
LINE 10: SIGNAL _____	(Type of signal or target emitter)
LINE 11: ON TIME _____	(DTG that planned EA activity initiated)
LINE 12: OFF TIME _____	(DTG that planned EA activity terminated)
LINE 13: PRIORITY _____	(Relative importance of EA mission)
LINE 14: TYPE _____	(Type of EA used against the emitter)
LINE 15: PRIMARY FREQUENCY _____	(Primary frequency of EA target signal)
LINE 16: SECONDARY FREQUENCY _____	(Secondary frequency of EA target signal)
LINE 17: LOW FREQUENCY _____	(Lower frequency limit of target class)
LINE 18: HIGH FREQUENCY _____	(Upper frequency limit of target class)
LINE 19: BANDWIDTH _____	(Target frequency bandwidth in MHz)
LINE 20: PULSE REPETITION _____	(Pulse repetition interval or frequency)
LINE 21: ES _____	(Electronic warfare support activity requested)
LINE 22: COUNTRY _____	(Nationality of the target emitter of concern)
LINE 23: LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid zone designator.
LINE 24: EMITTER _____	(Emitter call sign and name or nomenclature)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electronic attack	MHz	megahertz
EW	electronic warfare	UTM	universal transverse mercator
JOC	joint operations center		

Figure D-6. Electronic warfare tasking message instructions

LINE 25: FUNCTION	(Primary function of target)
LINE 26: NOTATION	(Notation or sorting code)
LINE 27: SIGNAL	(Type of signal of target emitter)
LINE 28: PRIMARY FREQUENCY	(Primary frequency of ES target signal)
LINE 29: SECONDARY FREQUENCY	(Secondary frequency of ES target signal)
LINE 30: LOW FREQUENCY	(Lower frequency limit of target class)
LINE 31: HIGH FREQUENCY	(Upper frequency limit of target class)
LINE 32: BANDWIDTH	(Target frequency bandwidth in MHz)
LINE 33: PULSE REPETITION	(Pulse repetition interval or frequency)
LINE 34: START LOCATION	(Start location of chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 35: STOP LOCATION	(Stop location of chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 36: ESSENTIAL	(EEI category indicator)
LINE 37: PRIORITY	(Relative importance of ES mission)
LINE 38: CHAFF	(Type of Chaff)
LINE 39: LOWER FREQUENCY	(Lower frequency of a range blanked by chaff or lower EA frequency)
LINE 40: UPPER FREQUENCY	(Upper frequency of a range blanked by chaff or lower EA frequency)
LINE 41: LOW LEVEL	(Lower altitude in hundreds of feet of airspace blanked by chaff)
LINE 42: UPPER LEVEL	(Upper altitude in hundreds of feet of airspace blanked by chaff)
LINE 43: TECHNIQUE	(EA technique employed)
LINE 44: COUNTRY	(Country in which chaff was employed)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electronic attack	MHz	megahertz
EEI	essential element of information	UTM	universal transverse mercator

Figure D-6. Electronic warfare tasking message instructions (continued)

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. ATP 3-12.3 is not the proponent for any Army terms. The proponent publication for joint and Army terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
ATO	air tasking order
CAS	close air support
CEMA	cyberspace electromagnetic activities
CEWO	cyber electronic warfare officer
CJCSM	Chairman of the Joint Chiefs of Staff manual
COMSEC	communications security
CREW	counter radio-controlled improvised explosive device electronic warfare
DF	direction finding
DODI	Department of Defense instruction
E2ESS	Host Nation Spectrum Worldwide Database Online
EA	electronic attack
EARF	electronic attack request format
EME	electromagnetic environment
EMI	electromagnetic interference
EMS	electromagnetic spectrum
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWPMT	Electronic Warfare Planning and Management Tool
FHMUX	frequency hop multiplexer
FM	frequency modulation
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
HF	high frequency
HPTL	high-payoff target list
IPB	intelligence preparation of the battlefield
JP	joint publication
JRFL	joint restricted frequency list

JSIR	joint spectrum interference resolution
JTAC	joint terminal attack controller
JTASR	joint tactical air strike request
LOB	line of bearing
LOS	line of sight
MDMP	military decision-making process
MEWSS	mobile electronic warfare support system
PACE	primary, alternate, contingency, and emergency
PIP	product improvement program
RCIED	radio-controlled improvised explosive device
RF	radio frequency
ROE	rules of engagement
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
SIGINT	signals intelligence
SJA	staff judge advocate
SOI	signal operating instructions
SOP	standard operating procedure
UHF	ultrahigh frequency
VHF	very high frequency

SECTION II – TERMS

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. (JP 3-13.1)

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. Also called **CEMA**. (ADRP 3-0)

directed energy

An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. (JP 3-13.1)

electromagnetic compatibility

The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (JP 3-13.1)

electromagnetic environment

The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. Also called **EME**. (JP 3-13.1)

electromagnetic hardening

Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (JP 3-13.1)

electromagnetic interference

Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the efectiveness performance of electronics and electrical equipment. Also called **EMI**. (JP 3-13.1)

electromagnetic intrusion

The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (JP 3-13.1)

electromagnetic jamming

The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-13.1)

electromagnetic pulse

The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 3-13.1)

electromagnetic spectrum

The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. See also **electronic warfare**. Also called **EMS**. (JP 3-13.1)

electromagnetic spectrum management

Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (JP 6-01)

electronic attack

Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called **EA**. (JP 3-13.1)

electronic masking

The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly sytems. (JP 3-13.1)

electronic protection

Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. (JP 3-13.1)

electronic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 3-13.1)

electronics security

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 3-13.1)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (JP 3-13.1)

electronic warfare reprogramming

The deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. (JP 3-13.1)

electronic warfare support

A division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called **ES**. (JP 3-13.1)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. (JP 3-13.1)

frequency deconfliction

A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management. (JP 3-13.1)

high-payoff target

A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. (JP 3-60)

line of sight

The unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another. (ATP 2-01.3)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

wartime reserve modes

Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. (JP 3-13.1)

References

All URLs accessed on 18 June 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. June 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/doctrine.

CJCSM 3320.02D. *Joint Spectrum Interference Resolution (JSIR) Procedures*. 3 June 2013.

DODI 6055.11. *Protecting Personnel from Electromagnetic Fields*. 19 August 2009.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-09.3. *Close Air Support*. 10 June 2019.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.

JP 3-14. *Space Operations*. 10 April 2018.

JP 3-60. *Joint Targeting*. 28 September 2018.

JP 6-01. *Joint Electromagnetic Spectrum Management Operations*. 20 March 2012.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 2-0. *Intelligence*. 4 September 2018.

ADP 3-0. *Operations*. 6 October 2017.

ADP 5-0. *The Operations Process*. 17 May 2012.

ADP 6-0. *Mission Command*. 17 May 2012.

ADRP 1. *The Army Profession*. 14 June 2015.

ADRP 3-0. *Operations*. 6 October 2017.

ATP 1-02.1. *Brevity - Multi-Service Tactics, Techniques, and Procedures for Multi-Service Brevity Codes*. 20 June 2018.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 1 March 2019.

ATP 2-22.6-2. *Signals Intelligence Volume II Reference Guide*. 20 June 2017.

ATP 3-09.32. *JFIRE Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*. 21 January 2016.

ATP 3-60. *Targeting*. 7 May 2015.

ATP 5-19. *Risk Management*. 14 April 2014.

ATP 6-02.70. *Techniques for Spectrum Management Operations.* 31 December 2015.

FM 1-04. *Legal Support to the Operational Army*. 18 March 2013.

FM 2-0. *Intelligence*. 6 July 2018.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017

FM 3-13. *Information Operations*. 6 December 2016.

FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

OTHER PUBLICATIONS

Most Navy doctrinal publications are available online: https://www.nwdc.navy.mil/site/doctrine.html (Requires DOD-approved certificate login and user account registration.)

Navy Warfare Publication 3-13. *Navy Information Operations.* February 2014.

RECOMMENDED READINGS

CSCSI 3320.02F. *Joint Spectrum Interference Resolution*. 08 March 2013.

CJCSM 3320.01C. *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*. 14 December 2012.

PRESCRIBED FORMS

None

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

Unless otherwise indicated, Department of Defense forms are available online: https://www.esd.whs.mil/Directives/forms/.

DD Form 1494. *Application for Equipment Frequency Allocation*.

DD Form 1972. *Joint Tactical Air Strike Request.*

WEBSITES

End-to-End Supportability System:

https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/host-nation-spectrum-worldwide-database-online-hnswdo (Requires DOD-approved certificate login and user account registration.)

Index

Entries are by paragraph number.

A

absorption, A-60

B

battle drills, 7-41

C

circular error probability, 5-21

close air support, 6-29

continuing to operate, 7-30

counter radio-controlled improvised explosive device electronic warfare, 2-9, 6-57

countermeasures, 6-11

CREW specialists, 2-10

cuts, 5-10

cyber and electronic warfare officer, 2-5, 3-46, 7-8

cyberspace electromagnetic activities section, 2-1, 2-4, 3-25, 4-3, 5-5, 6-2, 7-16, C-3

D

defensive electronic attack, 6-55

diffraction, A-57

direction finding, 5-10

E

electromagnetic compatibility, 7-21

electromagnetic deception, 6-12

electromagnetic environment, 1-8

electromagnetic environment survey, 5-8

electromagnetic hardening, 7-10

electromagnetic interference, 7-22

electromagnetic intrusion, 6-54

electromagnetic jamming, 6-45, 7-23

formulas, B-1

electromagnetic pulse, 6-10

electromagnetic spectrum
atmospheric effects, A-12
radio bands, A-1

electromagnetic spectrum management, 7-17

electronic attack
airborne, 6-31
considerations, 6-6
executing, 6-28
planning, 6-1
preparing, 6-21

electronic attack request format, 6-22, D-1

electronic masking, 7-11

electronic protection
planning, 7-3
remedial, 7-43
responsibilities, 7-1, 7-47

electronic reconnaissance, 5-2

electronic warfare
airborne, 3-7, 3-33
assessment, 3-60
configurations, 3-28
control authority, 2-11
divisions, 1-5
execution, 3-67
fixed-site, 3-32
manpack, 3-30
mission summary, D-7
overview, 1-1
personnel, 2-1
planning, 3-5, 3-36
preparation, 4-1
reprogramming, 3-24
tasking message, D-8
vehicle-mounted, 3-31
visualization, 3-25

electronic warfare equipment
Air Force, C-13
Army, C-1
Marine Corps, C-16
Navy, C-20

electronic warfare noncommissioned officer, 2-7

electronic warfare support, 5-1
execution, 5-7
preparing, 5-5

electronic warfare technician, 2-6

emission control, 7-13

F

fixes, 5-11

frequency deconfliction message, D-6

G

G-2 (S-2) responsibilities, 2-13, 3-37

G-3 (S-3) responsibilities, 2-14

G-6 (S-6) responsibilities, 2-15, 3-40

ground wave, A-73

guarded, 3-43

H

End-to-End Supportability System, C-12

I

information operations officer responsibilities, 2-16

J

joint restricted frequency list, 2-8

joint spectrum interference resolution, D-3

joint tactical air strike request, D-2

L

line of bearing, 5-11

lowest usable frequency, A-95

M

maximum usable frequency, A-93

measures of effectiveness, 3-62

Entries are by page number.

measures of performance, 3-62
military decision-making process, 3-1
minimum power output, 6-25
multipath interference, A-72

P

path loss, A-70
polarization, A-41
protected, 3-42

R

radio frequency noise, A-65
reflection, 5-29, A-47
refraction, 5-28, A-52
risk management, 3-11
running estimate, 3-17

S

scattering, A-60
signals intelligence
  integration, 4-10
  sensors, 4-12
signal-to-jamming ratio, 7-31
skywave, A-77
spectrum manager, 2-8
staff judge advocate, 2-17
  responsibilities, 3-44
stop jamming message, D-5
sunspot cycles, A-99

T

taboo, 3-41
targeting, 3-55
targeting working group, 3-52

V

vulnerability assessment, 7-6

W

wartime reserve modes, 7-20
wave propagation, A-34

ATP 3-12-3

16 July 2019

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1919308

DISTRIBUTION:
Distributed in electronic media only(EMO).

PIN: 205422-000