

FM 3-36

ELECTRONIC WARFARE IN OPERATIONS

February 2009

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

Headquarters, Department of the Army

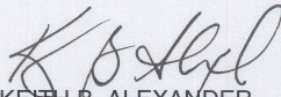
FOREWORD

This electronic warfare (EW) doctrine is a key element in the Army's ongoing effort to rebuild and modernize its EW capability. This publication, FM 3-36, the first Army EW doctrine to be issued in nearly a decade, is as timely as it is essential. In addition to directly supporting traditional EW operations, FM 3-36 is moving the Army's EW strategy into cyberspace and the electromagnetic environment and is a great start in providing guidance to commanders and ultimately our national decision makers. It provides commanders clear concepts and doctrine that maximize operational effectiveness across the electromagnetic spectrum in both traditional and evolving technologies.

The global proliferation of electronics and wireless transmissions has evolved into a significant technological advantage for our nation while simultaneously creating a greater dependence on technology. This dependence also presents challenges, as our adversaries are constantly developing the means to use these same wireless networks, electronics, computer networks, and electronic warfare capabilities to launch attacks against us. To meet these challenges, the Army is implementing and integrating network and electronic warfare capabilities to counter the hostile use of cyberspace, space, and the electromagnetic spectrum.

FM 3-36 provides Army commanders and their staff guidance on how the electromagnetic spectrum can impact their operations and how friendly EW operations can be used to gain an advantage. This manual describes the application of EW in support of full spectrum operations and provides a baseline for ensuring a common understanding and operational consistency. Although new equipment, tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remains constant. So, as new strategies and tactics are devised to meet the cyberspace environment of the 21st century, electronic warfare remains a critical component of our national defense.

This updated doctrine and other modifications to the Army's operational strategies are testimony to the innovation and vision on which our nation relies in this era of the Cyber Revolution.



KEITH B. ALEXANDER
Lieutenant General, U.S. Army
Director, National Security Agency

Electronic Warfare in Operations

Contents

	PREFACE	iv
Chapter 1	ELECTRONIC WARFARE OVERVIEW	1-1
	Operational Environments	1-1
	Information and the Electromagnetic Spectrum	1-1
	Divisions of Electronic Warfare	1-4
	Activities and Terminology	1-7
	Summary	1-12
Chapter 2	ELECTRONIC WARFARE IN FULL SPECTRUM OPERATIONS	2-1
	The Role of Electronic Warfare	2-1
	The Application of Electronic Warfare	2-3
	Summary	2-7
Chapter 3	ELECTRONIC WARFARE ORGANIZATION.....	3-1
	Organizing Electronic Warfare Operations.....	3-1
	Planning and Coordinating Electronic Warfare Activities.....	3-4
	Summary	3-6
Chapter 4	ELECTRONIC WARFARE AND THE OPERATIONS PROCESS.....	4-1
	Section I — Electronic Warfare Planning.....	4-1
	The Military Decisionmaking Process	4-2
	Decisionmaking in a Time-Constrained Environment.....	4-9
	The Integrating Processes and Continuing Activities.....	4-10
	Employment Considerations	4-15
	Section II — Electronic Warfare Preparation.....	4-19
	Section III — Electronic Warfare Execution.....	4-19
	Section IV — Electronic Warfare Assessment	4-20
	Summary	4-21
Chapter 5	COORDINATION, DECONFLICTION, AND SYNCHRONIZATION	5-1
	Coordination and Deconfliction	5-1
	Synchronization	5-5
	Summary	5-5

Contents

Chapter 6	INTEGRATION WITH JOINT AND MULTINATIONAL OPERATIONS.....	6-1
	Joint Electronic Warfare Operations	6-1
	Multinational Electronic Warfare Operations	6-4
	Summary	6-6
Chapter 7	ELECTRONIC WARFARE CAPABILITIES	7-1
	Service Electronic Warfare Capabilities.....	7-1
	External Support Agencies and Activities	7-1
	Summary	7-3
Appendix A	THE ELECTROMAGNETIC ENVIRONMENT.....	A-1
Appendix B	ELECTRONIC WARFARE INPUT TO OPERATION PLANS AND ORDERS. B-1	
Appendix C	ELECTRONIC WARFARE RUNNING ESTIMATE.....	C-1
Appendix D	ELECTRONIC WARFARE-RELATED REPORTS AND MESSAGES.....	D-1
Appendix E	ARMY AND JOINT ELECTRONIC WARFARE CAPABILITIES.....	E-1
Appendix F	TOOLS AND RESOURCES RELATED TO ELECTRONIC WARFARE.....	F-1
	GLOSSARY	Glossary-1
	REFERENCES.....	References-1
	INDEX	Index-1

Figures

Figure 1-1. The electromagnetic spectrum	1-2
Figure 1-2. Electromagnetic spectrum targets.....	1-3
Figure 1-3. The three subdivisions of electronic warfare	1-4
Figure 1-4. Means versus effects	1-12
Figure 2-1. Electronic warfare weight of effort during operations	2-2
Figure 3-1. Electronic warfare coordination organizational framework	3-2
Figure 4-1. The operations process	4-1
Figure 4-2. Example of analysis for an enemy center of gravity.....	4-3
Figure 4-3. Course of action development.....	4-5
Figure 4-4. Course of action comparison.....	4-8
Figure 4-5. Integrating processes and continuing activities.....	4-10
Figure 4-6. Electronic warfare support to intelligence preparation of the battlefield	4-11
Figure 4-7. Electronic warfare in the targeting process	4-13
Figure 5-1. Spectrum deconfliction procedures	5-3
Figure 6-1. Joint frequency management coordination	6-3
Figure 6-2. Electronic warfare support request coordination.....	6-4
Figure A-1. The electromagnetic spectrum.....	A-2
Figure B-1. Appendix 4 (Electronic Warfare) to annex P (Information Operations) instructions	B-2
Figure C-1. Example of an electronic warfare running estimate	C-2

Figure C-2. Sample update information to the electronic warfare running estimate.....	C-3
Figure E-1. Guardrail common sensor	E-2
Figure E-2. Aerial common sensor (concept).....	E-2
Figure E-3. Prophet (vehicle-mounted).....	E-3
Figure E-4. AN/MLQ-36A mobile electronic warfare support system	E-5
Figure E-5. EA-6B Prowler	E-6
Figure E-6. EC-130H Compass Call	E-8
Figure E-7. RC-135V/W Rivet Joint.....	E-9
Figure E-8. Navy EA-6B Prowler.....	E-10
Figure E-9. EA-18 Growler	E-11

Tables

Table 2-1. Two Army information tasks: command and control warfare and information protection	2-4
Table 2-2. Electronic warfare support to two Army information tasks.....	2-5
Table 3-1. Functions of electronic warfare working groups	3-3
Table 4-1. Sample input to synchronization matrix	4-7
Table A-1. Radio and radar designators and frequency bands	A-3
Table E-1. Army and joint electronic warfare capabilities	E-13
Table E-2. Electronic warfare systems and platforms resources.....	E-14

**This publication is available at
Army Knowledge Online (AKO) (www.us.army.mil)
and the Reimer Digital Library (RDL) at
(www.adtdl.army.mil)**

Preface

PURPOSE

FM 3-36 provides Army doctrine for electronic warfare (EW) planning, preparation, execution, and assessment in support of full spectrum operations. Users of FM 3-36 must be familiar with full spectrum operations established in FM 3-0; the military decisionmaking process established in FM 5-0; the operations process established in FMI 5-0.1; commander's visualization described in FM 6-0; and electronic warfare described in JP 3-13.1.

SCOPE

FM 3-36 is organized into seven chapters and six appendixes. Each chapter addresses a major aspect of Army EW operations. The appendixes address aspects of EW operations that complement the operational doctrine. A glossary contains selected terms.

- Chapter 1 discusses the nature and scope of electronic warfare and the impact of the electromagnetic environment on Army operations.
- Chapter 2 offers a discussion of EW support to full spectrum operations, combat power, the warfighting functions, and information tasks.
- Chapter 3 introduces the organizational framework for command and control of EW operations.
- Chapter 4 describes how commanders integrate EW operations throughout the operations process.
- Chapter 5 discusses the coordination required to synchronize and deconflict EW operations effectively.
- Chapter 6 provides the baseline for integrating EW operations into joint and multinational operations.
- Chapter 7 discusses the enabling activities that support EW operations, such as command and control, intelligence, logistics, technical support and EW training.
- Appendix A discusses the electromagnetic environment.
- Appendix B illustrates an EW appendix to an operation order.
- Appendix C illustrates an EW running estimate.
- Appendix D discusses EW related reports and messages.
- Appendix E offers a reference guide to Army and joint EW capabilities.
- Appendix F discusses EW-related tools and resources.

APPLICABILITY

FM 3-36 provides guidance on EW operations for commanders and staffs at all echelons. This FM serves as an authoritative reference for personnel who—

- Develop doctrine (fundamental principles and tactics, techniques, and procedures), materiel, and force structure.
- Develop institutional and unit training.
- Develop standing operating procedures for unit operations.
- Conduct planning, preparation, execution and assessment of electronic warfare.

FM 3-36 applies to the Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve, unless otherwise stated.

ADMINISTRATIVE INFORMATION

Headquarters, U.S. Army Training and Doctrine Command, is the proponent for this publication. The preparing agency is the U.S. Army Electronic Warfare Proponent, U.S. Army Combined Arms Center. Send written comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-CSB-EW (FM 3-36), 950 Bluntville Lane, Building 391, Fort Leavenworth, KS 66027-2337; by e-mail to usacewpops@conus.army.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Chapter 1

Electronic Warfare Overview

This chapter provides an overview of electronic warfare and the conceptual foundation that leaders require to understand the electromagnetic environment and its impact on Army operations.

OPERATIONAL ENVIRONMENTS

1-1. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An operational environment includes physical areas—the air, land, maritime, and space domains. It also includes the information that shapes the operational environment as well as enemy, adversary, friendly, and neutral systems relevant to a joint operation. Joint planners analyze operational environments in terms of six interrelated operational variables: political, military, economic, social, information, and infrastructure. To these variables Army doctrine adds two more: physical environment and time. (See FM 3-0 for additional information on the operational variables). Army leaders use operational variables to understand and analyze the broad environment in which they are conducting operations.

1-2. Army leaders use mission variables to synthesize operational variables and tactical-level information with local knowledge about conditions relevant to their mission. They use mission variables to focus analysis on specific elements that directly affect their mission. Upon receipt of a warning order or mission, Army tactical leaders narrow their focus to six mission variables known as METT-TC. They are mission, enemy, terrain and weather, troops and support available, time available and civil considerations. The mission variables outline the situation as it applies to a specific Army unit.

1-3. Commanders employ and integrate their unit's capabilities and actions within their operational environment to achieve a desired end state. Through analyzing their operational environment, commanders understand how the results of friendly, adversary, and neutral actions may impact that end state. During military operations, both friendly and enemy commanders depend on the flow of information to make informed decisions. This flow of information depends on the electronic systems and devices used to communicate, navigate, sense, store, and process information.

INFORMATION AND THE ELECTROMAGNETIC SPECTRUM

1-4. Commanders plan for and operate electronic systems and the weapon systems that depend on them in an intensive and nonpermissive electromagnetic environment. They ensure the flow of information required for their decisionmaking. (Appendix A further discusses the electromagnetic environment.) Within the electromagnetic environment, electronic systems and devices operate in the electromagnetic spectrum. (See figure 1-1, page 1-2.)

1-5. The electromagnetic spectrum has been used for commercial and military applications for over a century. However, the full potential for its use as the primary enabler of military operations is not yet fully appreciated. New technologies are expanding beyond the traditional radio frequency spectrum. They include high-power microwaves and directed-energy weapons. These new technologies are part of an electronic warfare (EW) revolution by military forces. Just as friendly forces leverage the electromagnetic spectrum to their advantage, so do capable enemies use the electromagnetic spectrum to threaten friendly force operations. The threat is compounded by the growth of a wireless world and the increasingly sophisticated use of commercial off-the-shelf technologies.

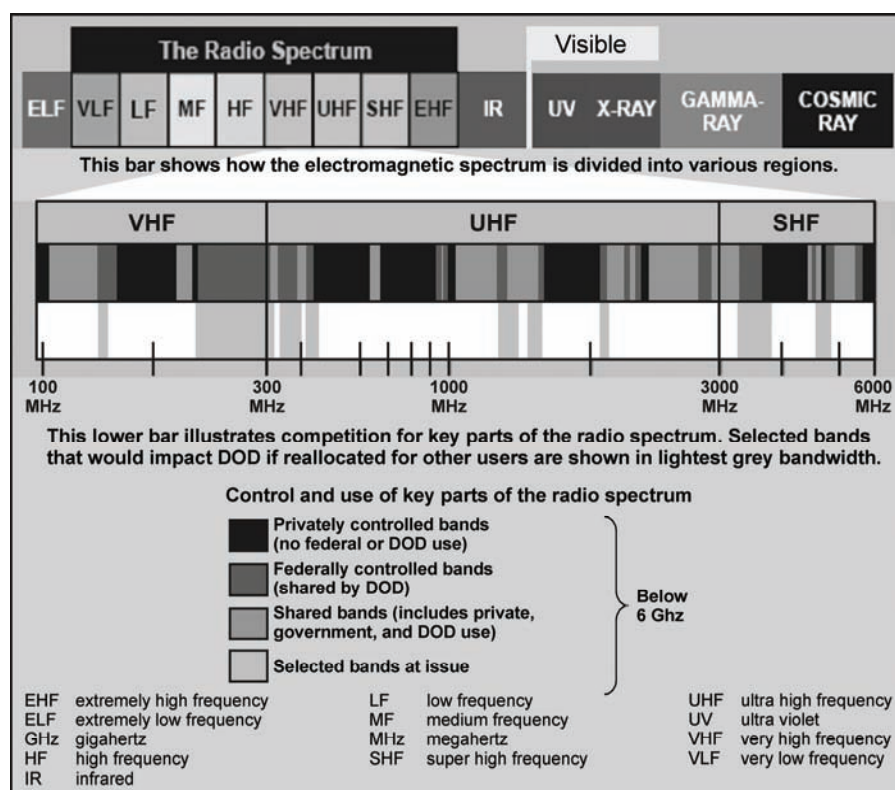


Figure 1-1. The electromagnetic spectrum

1-6. Adversaries and enemies, from small and single actors to large state, multinational, and nonstate actors, use the most modern technology. Such technology is moving into the cellular and satellite communications area. Most military and commercial operations rely on electromagnetic technologies and are susceptible to the inherent vulnerabilities associated with their use. This reliance requires Army forces to dominate the electromagnetic spectrum (within their operational environment) with the same authority that they dominate traditional land warfare operations. Emerging electromagnetic technologies offer expanded EW capabilities. They dynamically affect the electromagnetic spectrum through delivery and integration with other types of emerging weapons and capabilities. Examples are directed-energy weapons, high-powered microwaves, lasers, infrared, and electro-optical and wireless networks and devices.

1-7. In any conflict, commanders attempt to dominate the electromagnetic spectrum. They do this by locating, targeting, exploiting, disrupting, degrading, deceiving, denying, or destroying the enemy's electronic systems that support military operations or deny the spectrum's use by friendly forces. The increasing portability and affordability of sophisticated electronic equipment guarantees that the electromagnetic environment in which forces operate will become even more complex. To ensure unimpeded access to and use of the electromagnetic spectrum, commanders plan, prepare, execute, and assess EW operations against a broad set of targets within the electromagnetic spectrum. (See figure 1-2.)

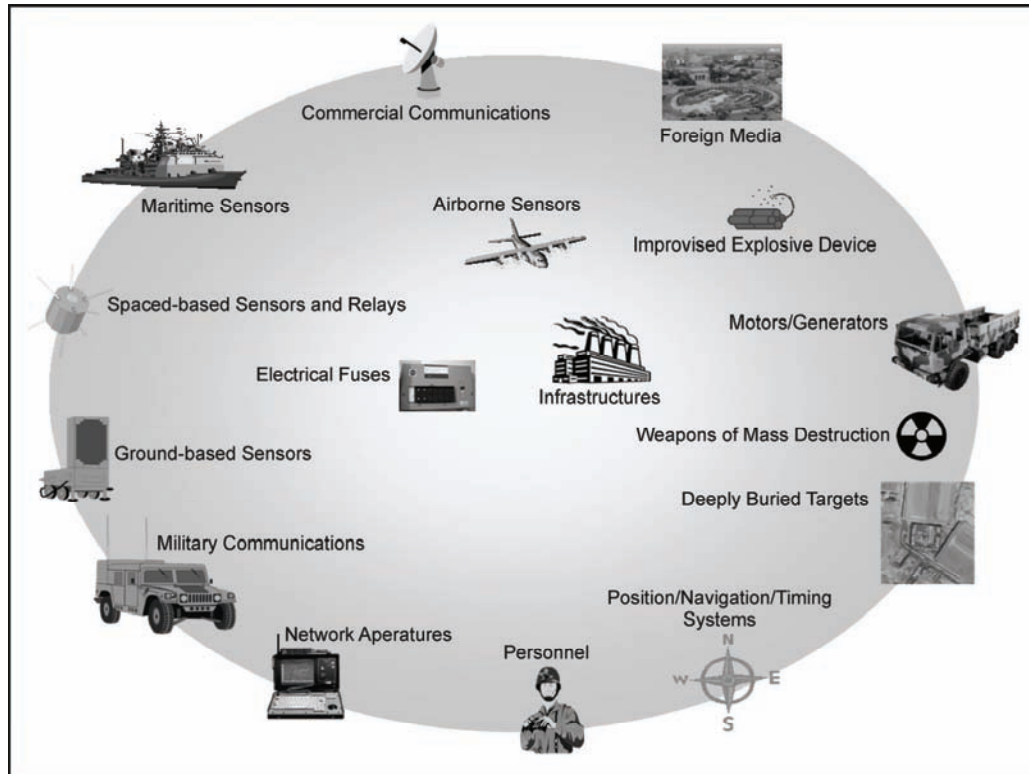


Figure 1-2. Electromagnetic spectrum targets

DIVISIONS OF ELECTRONIC WARFARE

1-8. *Electronic warfare* is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support (JP 3-13.1). (See figure 1-3.)

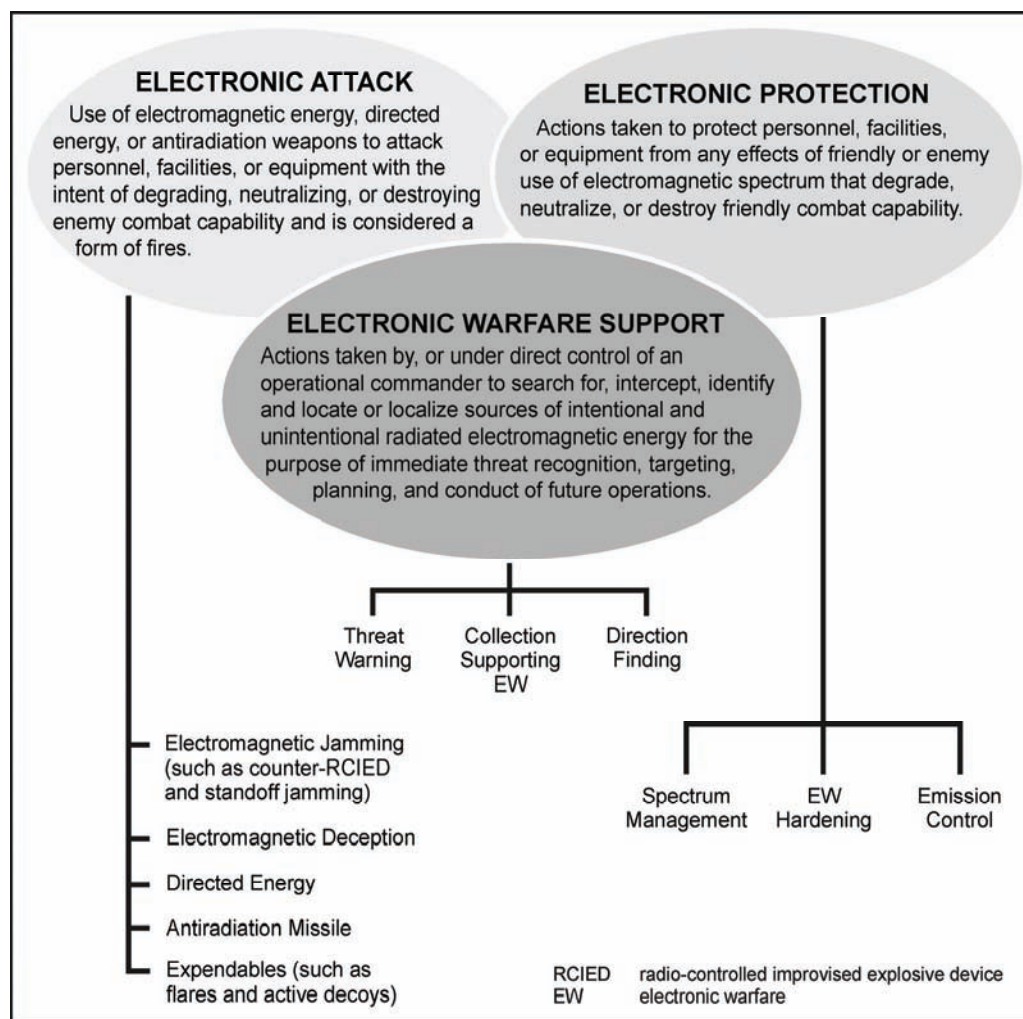


Figure 1-3. The three subdivisions of electronic warfare

ELECTRONIC ATTACK

1-9. *Electronic attack* is a 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 attack includes—

- Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception.
- Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).
- Offensive and defensive activities including countermeasures.

1-10. Common types of electronic attack include spot, barrage, and sweep electromagnetic jamming. Electronic attack actions also include various electromagnetic deception techniques such as false target or duplicate target generation. (See paragraphs 1-23 to 1-31 for further discussion of electronic attack activities.)

1-11. *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 1-02). A directed-energy weapon uses directed energy primarily as a direct means to damage or destroy an enemy's equipment, facilities, and personnel. In addition to destructive effects, directed-energy weapon systems support area denial and crowd control. (See appendix A for more information on directed energy.)

1-12. Examples of offensive electronic attack include—

- Jamming enemy radar or electronic command and control systems.
- Using antiradiation missiles to suppress enemy air defenses (antiradiation weapons use radiated energy emitted from the target as their mechanism for guidance onto targeted emitters).
- Using electronic deception techniques to confuse enemy intelligence, surveillance, and reconnaissance systems.
- Using directed-energy weapons to disable an enemy's equipment or capability.

1-13. Defensive electronic attack uses the electromagnetic spectrum to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasure systems, and counter-radio-controlled improvised-explosive-device systems. (See JP 3-13.1 for more discussion of electronic attack.)

ELECTRONIC PROTECTION

1-14. *Electronic protection* is a 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). For example, electronic protection includes actions taken to ensure friendly use of the electromagnetic spectrum, such as frequency agility in a radio, or variable pulse repetition frequency in radar. Electronic protection should not be confused with self-protection. Both defensive electronic attack and electronic protection protect personnel, facilities, capabilities, and equipment. However, electronic protection protects from the effects of electronic attack (friendly and enemy), while defensive electronic attack primarily protects against lethal attacks by denying enemy use of the electromagnetic spectrum to guide or trigger weapons.

1-15. During operations, electronic protection includes, but is not limited to, the application of training and procedures for countering enemy electronic attack. Army commanders and forces understand the threat and vulnerability of friendly electronic equipment to enemy electronic attack and take appropriate actions to safeguard friendly combat capability from exploitation and attack. Electronic protection measures minimize the enemy's ability to conduct electronic warfare support (electronic warfare support is discussed in paragraphs 1-18 to 1-20) and electronic attack operations successfully against friendly forces. To protect friendly combat capabilities, units—

- Regularly brief force personnel on the EW threat.
- Ensure that electronic system capabilities are safeguarded during exercises, workups, and predeployment training.
- Coordinate and deconflict electromagnetic spectrum usage.
- Provide training during routine home station planning and training activities on appropriate electronic protection active and passive measures.
- Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennas).

1-16. Electronic protection also includes spectrum management. The spectrum manager works for the G-6 or S-6 and plays a key role in the coordination and deconfliction of spectrum resources allocated to the force. Spectrum managers or their direct representatives participate in the planning for EW operations.

1-17. The development and acquisition of communications and electronic systems includes electronic protection requirements to clarify performance parameters. Army forces design their equipment to limit inherent vulnerabilities. If electronic attack vulnerabilities are detected, then units must review these programs. (See DODI 4650.01 for information on the spectrum certification process and electromagnetic compatibility.)

ELECTRONIC WARFARE SUPPORT

1-18. *Electronic warfare support* is a division of electronic warfare involving actions tasked by, or under the 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).

1-19. Electronic warfare support systems are a source of information for immediate decisions involving electronic attack, electronic protection, avoidance, targeting, and other tactical employments of forces. Electronic warfare support systems collect data and produce information or intelligence to—

- Corroborate other sources of information or intelligence.
- Conduct or direct electronic attack operations.
- Initiate self-protection measures.
- Task weapon systems.
- Support electronic protection efforts.
- Create or update EW databases.
- Support information tasks.

1-20. Electronic warfare support and signals intelligence missions use the same resources. The two differ in the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the time lines required. Like tactical signals intelligence, electronic warfare support missions respond to the immediate requirements of a tactical commander. Signals intelligence above the tactical level is under the operational control of the National Security Agency and directly supports the overarching national security mission. Resources that collect tactical-level electronic warfare support data can simultaneously collect national-level signals intelligence. See FM 2-0 for more information on signals intelligence.

ACTIVITIES AND TERMINOLOGY

1-21. Although new equipment and tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remains constant. Hence, effective EW activities remain the same despite changes in hardware and tactics. Principal EW activities are discussed in the following paragraphs.

PRINCIPAL ACTIVITIES

1-22. Principal EW activities support full spectrum operations by exploiting the opportunities and vulnerabilities inherent in the use of the electromagnetic spectrum. The numerous EW activities are categorized by the EW subdivisions with which they are most closely associated: electronic attack, electronic warfare support, and electronic protection. JP 3-13.1 discusses these principal activities in detail.

Electronic Attack Activities

1-23. Activities related to electronic attack are either offensive or defensive and include—

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

Countermeasures

1-24. *Countermeasures* are 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 1-02). They can be deployed preemptively or reactively. Devices and techniques used for EW countermeasures include electro-optical-infrared countermeasures and radio frequency countermeasures.

1-25. *Electro-optical-infrared countermeasures* consist of any device or technique employing electro-optical-infrared materials or technology that is intended to impair or counter the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Electro-optical-infrared is the part of the electromagnetic spectrum between the high end of the far infrared and the low end of ultraviolet. Electro-optical-infrared countermeasures may use laser and broadband jammers, smokes/aerosols, signature suppressants, decoys, pyrotechnics/pyrophorics, high-energy lasers, or directed infrared energy countermeasures (JP 3-13.1).

1-26. *Radio frequency countermeasures* consist of any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of or counter enemy activity, particularly with respect to precision guided weapons and sensor systems (JP 3-13.1).

Electromagnetic Deception

1-27. *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 enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability (JP 3-13.4). Among the types of electromagnetic deception are the following:

- Manipulative electromagnetic deception involves actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces.
- Simulative electromagnetic deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.
- Imitative electromagnetic deception introduces electromagnetic energy into enemy systems that imitates enemy emissions.

Electromagnetic Intrusion

1-28. *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 1-02).

Electromagnetic Jamming

1-29. *Electromagnetic jamming* is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability (JP 1-02).

Electromagnetic Pulse

1-30. *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 1-02).

Electronic Probing

1-31. *Electronic probing* is the intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices (JP 1-02). This activity is coordinated through joint or interagency channels and supported by Army forces.

Electronic Warfare Support Activities

1-32. Activities related to electronic warfare support include—

- Electronic reconnaissance.
- Electronic intelligence.
- Electronics security.

Electronic Reconnaissance

1-33. *Electronic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 1-02).

Electronic Intelligence

1-34. *Electronic intelligence* is technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (JP 1-02).

Electronics Security

1-35. *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 1-02).

Electronic Protection Activities

1-36. Activities related to electronic protection include—

- Electromagnetic hardening.
- Electromagnetic interference.
- Electronic masking.
- Electronic warfare reprogramming.
- Emission control.
- Spectrum management.
- Wartime reserve modes.
- Electromagnetic compatibility.

Electromagnetic Hardening

1-37. *Electromagnetic hardening* consists of action taken to protect personnel, facilities, and/or equipment by filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 1-02).

Electromagnetic Interference

1-38. *Electromagnetic interference* is any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products and the like (JP 1-02).

Electronic Masking

1-39. *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 1-02).

Electronic Warfare Reprogramming

1-40. *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. These changes may be the result of deliberate actions on the part of friendly, adversary, or third parties; or may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of electronic warfare reprogramming is to maintain or enhance the effectiveness of electronic warfare and target sensing system equipment. Electronic warfare reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems (JP 3-13.1).

Emission Control

1-41. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing transmissions 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 1-02).

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

