Joint Publication 3-13.1

Electronic Warfare

08 February 2012

Intentionally Blank

PREFACE

1. Scope

This publication provides joint doctrine for the planning, execution, and assessment of electronic warfare across the range of military operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations, education, and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, commanders of combatant commands, subunified commands, joint task forces, subordinate components of these commands, and the Services.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current

and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-13.1
DATED 25 JANUARY 2007

- **Adds a discussion on joint electromagnetic spectrum operations.**
- **Adds a discussion on the electromagnetic operational environment.**
- **Adds a discussion on electromagnetic battle management.**
- **Adds a discussion on joint electromagnetic spectrum management operations.**
- **Adds a discussion on electronic warfare's (EW's) relationship to irregular warfare, EW's relationship to space operations, EW's relationship to cyberspace operations, and EW's relationship to navigation warfare.**
- **Changes the electronic warfare coordination cell to the electronic warfare cell.**
- **Addresses component-level EW support activities referred to as EW elements: land-EW element, air-EW element, and maritime-EW element.**
- **Adds a discussion in Chapter III, "Planning Joint Electronic Warfare," on "chemical, biological, radiological, and nuclear considerations."**
- **Adds a discussion in Chapter IV, "Coordinating Joint Electronic Warfare," on EW and interagency coordination.**
- **Adds appendices: "Electronic Warfare Joint Munitions Effectiveness Manual Planning" and "SPECTRUM XXI."**
- **Changes the Appendix, "Joint Spectrum Center Support to Joint Electronic Warfare," to "Organizations Supporting Joint Electronic Warfare;" and adds discussions, on the Electromagnetic-Space Analysis Center, Global Positioning System Operations Center, Joint Electronic Warfare Center, Joint Navigation Warfare Center, and Information Operations Range in addition to the discussion on the Joint Spectrum Center.**
- **Deletes the Appendix, "Service Perspectives of Electronic Warfare" and added text to Chapter II, "Organizing for Joint Electronic Warfare," Paragraph 6, "Service Organization for Electronic Warfare."**
- **Adds definitions for the terms "electromagnetic battle management" and "electromagnetic spectrum control."**

- **Modifies the definitions of the terms "directed-energy device," "directed-energy weapon," "electronic warfare reprogramming," "electro-optical-infrared countermeasure," "TABOO frequencies," and "verification."**

- **Assumes proponency for the terms "chaff," "countermeasures," "directed energy," "direction finding," "electronic probing," and "wartime reserve modes."**

- **Removes the terms "acoustical surveillance," "acoustic jamming," "barrage jamming," "control of electromagnetic radiation," "directed-energy protective measures," "emission control orders," "ferret," "imitative communications deception," "imitative electromagnetic deception," "information," "jamming," "manipulative electromagnetic deception," "meaconing," "pulse duration," "radar spoking," "scan," "scan period," " scan type," and "simulative electromagnetic deception" from Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.***

TABLE OF CONTENTS

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an Overview of Electronic Warfare**
- **Describes Organizing for Joint Electronic Warfare**
- **Explains Planning Joint Electronic Warfare**
- **Discusses Coordinating Joint Electronic Warfare**
- **Addresses Multinational Aspects of Electronic Warfare**

Overview of Electronic Warfare

Military operations are executed in an environment complicated by increasingly complex demands on the electromagnetic spectrum.

All modern forces depend on the electromagnetic spectrum (EMS). The military requirement for unimpeded access to, and use of, the EMS is the key focus for joint electromagnetic spectrum operations (JEMSO), both in support of military operations and as the focus of operations themselves. **Electronic warfare (EW) is essential for protecting friendly operations and denying adversary operations within the EMS throughout the operational environment.**

Military Operations and the Electromagnetic Environment

As with the operational environment, the goal of the joint force commander (JFC) is to shape and control the electromagnetic operational environment.

JEMSO are the coordinated efforts of EW and joint electromagnetic spectrum management operations (JEMSMO) to exploit, attack, protect, and manage the electromagnetic operational environment (EMOE). The impact of an EMOE upon the operational capability of military forces, equipment, systems, and platforms is referred to as electromagnetic environmental effects. It encompasses all electromagnetic (EM) disciplines to include electromagnetic compatibility; electromagnetic interference; EM vulnerability; electromagnetic pulse (EMP); electronic protection (EP); hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects such as sunspots, lightning, and precipitation static.

Role of Electronic Warfare Across the Range of Military Operations

The term EW refers to military action involving the **use of EM energy and directed energy (DE) to control the EMS or to attack the enemy. EW consists of three divisions:** electronic attack (EA), EP, and electronic warfare support (ES).

Electronic Attack

EA refers to the division of EW involving the use of **EM energy, DE, 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.

Electronic Protection

EP refers to the division of EW involving actions taken **to protect personnel, facilities, and equipment** from any effects of friendly, neutral, or enemy use of the EMS, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability.

Electronic Warfare Support

ES refers to the division of EW 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 EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

Principal Electronic Warfare Activities

The principal EW activities have been developed over time to exploit the opportunities and vulnerabilities inherent in the physics of EM energy. The principal activities used in EW include the following: countermeasures, EM battle management (EMBM), EM compatibility; EM deception; EM hardening, EM interference resolution, EM intrusion, EM jamming, EMP, EM spectrum control, electronic intelligence collection, electronic masking, electronic probing, electronic reconnaissance, electronics security, EW reprogramming, emission control, JEMSO, JEMSMO, low-observability/stealth, meaconing, navigation warfare (NAVWAR), precision geolocation, and wartime reserve modes.

Electronic Warfare Capabilities and Potential Effects

As an adaptive and responsive form of disruptive or destructive fires, EA's purpose is to gain and maintain friendly advantage within the EMOE and ensure requisite friendly access to the EMS. EW may adversely affect friendly forces when not properly integrated and coordinated. EW is employed to create decisive, standalone effects, or to support military operations by generating various levels of control, detection, denial,

deception, disruption, degradation, exploitation, protection, and destruction.

Electronic Warfare's Role in Irregular Warfare

During irregular warfare, adversaries may operate with unsophisticated electronic means to achieve their objectives. EW can influence the adversary, friendly population, and neutral population, with the joint force commander's (JFC's) information operations (IO) message, in effort to change/win popular support.

Electronic Warfare's Role in Information Operations

EW contributes to the success of IO by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EMS while protecting friendly freedom of action.

Electronic Warfare's Role in Space Operations

Since space-based operations depend on the EMS, EW must be considered. Most operations in space beyond uncontested communications, physical maneuvering, and uncontested EM collection involve some form of EW.

Electronic Warfare's Role in Cyberspace Operations

Since cyberspace requires both wired and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the EMS for the enabling of effects in cyberspace. Due to the complementary nature and potential synergistic effects of EW and computer network operations, they must be coordinated to ensure they are applied to maximize effectiveness.

Electronic Warfare's Relationship to Navigation Warfare

EW produces NAVWAR effects by protecting or denying transmitted global navigation satellite system or other radio navigation aid signals.

Directed Energy

DE is an umbrella term covering technologies that produce concentrated EM energy and atomic or subatomic particles. A **DE weapon** is a system using DE primarily as a means to incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel.

Intelligence and Electronic Warfare Support

The distinction between whether a given asset is performing an ES mission or an intelligence mission is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. ES and signals intelligence (SIGINT) operations often share the same or similar assets and resources, and may be tasked to simultaneously collect information that meets both requirements.

Organizing for Joint Electronic Warfare

Responsibilities

How joint staffs are organized to plan and execute electronic warfare is a prerogative of the JFC.

EW planning and operations can be divided among multiple directorates of a joint staff based on long-, mid-, and near-term functionality and based upon availability of qualified EW personnel. **Long-range planning** of EW normally occurs under the plans directorate of a joint staff, while **near/mid-term planning and the supervision** of EW execution normally falls within the purview of the operations directorate of a joint staff (J-3).

Joint Electronic Warfare Organization

Joint Force Commander's EW Staff (JCEWS). The JCEWS is headed by the command electronic warfare officer (EWO), who is designated as the JCEWS chief. The JCEWS develops operation plans (OPLANs) and concept plans and monitors routine EW operations and activities.

Joint Electronic Warfare Cell. The JFC may designate and empower a joint electronic warfare cell (EWC) to organize, execute, and oversee conduct of EW.

Joint Frequency Management Organization

Each geographic combatant commander is specifically tasked by policy to establish a frequency management structure that includes a **joint frequency management office (JFMO)** and to establish procedures to support planned and ongoing operations. To accomplish these tasks, each supported combatant commander establishes a JFMO, typically under the cognizance of the communications system directorate of a joint staff, to **support joint planning, coordination, and operational control of the EMS** for assigned forces.

Organization of Intelligence Support to Electronic Warfare

At the national level, organizations and agencies such as the Central Intelligence Agency, National Security Agency/Central Security Service, National Geospatial-Intelligence Agency, and Defense Intelligence Agency are constantly seeking to identify, catalog, and update the electronic order of battle (EOB) of identified or potential adversaries. The joint intelligence operations center responds to theater-level EW-related intelligence requirements and forwards requests that require national-level assets to the defense collection coordination center or other national-level organizations according to established procedures. The intelligence directorate of a joint staff (J-2) [at the subordinate joint force level] normally assigns one or more members of the staff to act as a liaison

between the J-2 section and the IO cell where EW planners are normally assigned.

Service Organization for Electronic Warfare

Each Service has a different approach to organizing its forces.

Army

The Army is organized to work in the structure of an electronic warfare working group with the foundation of the group centered on the EWO, the EW technician, and the EW specialist, who comprise the electronic warfare coordination cell (EWCC).

Marines

Marine EW assets are integral to the Marine air-ground task force (MAGTF). The MAGTF command element task organizes and coordinates EW systems to meet MAGTF EW needs and ultimately achieve the JFC's objectives.

Navy

Navy EW is executed by surface ships, aircraft, and submarines organized in strike groups. For each strike group, the IO warfare commander is responsible for coordinating and integrating EW, typically through the strike group EWO, into naval and joint operations.

Air Force

Within the Air Force component, dedicated EW support assets conduct a variety of EA, EP, and ES operations and support suppression of enemy air defenses (SEAD) and IO mission areas. These are all under the operational control of the commander, Air Force forces.

Planning Joint Electronic Warfare

Joint electronic warfare is centrally planned and directed and decentrally executed.

EW is a complex mission area that should be fully integrated with other aspects of joint operations in order to achieve its full potential. Such integration requires careful planning. EW planners must coordinate their planned activities with other aspects of military operations that use the EMS, as well as third party users that EW does not wish to disrupt.

Electronic Warfare Planning Considerations

Some of the considerations for planning EW in support of military operations include EMS management, EW support of SEAD, EW support against a nontraditional threat, EW reprogramming, electronic masking, interoperability, rules of engagement (ROE), unintended consequences, meteorological and oceanographic considerations, and chemical, biological, radiological, and nuclear considerations. Since EW activity may create effects within and throughout the entire EMS, joint EW planners

must closely coordinate their efforts with those members of the joint staff who are concerned with managing military EMS use. EW activities frequently involve a unique set of complex issues. There are Department of Defense directives and instructions, laws, rules, law of armed conflict, and theater ROE that may affect EW activities. Commanders should seek legal review during all levels of EW planning and execution, to include development of theater ROE.

Joint Electronic Warfare Planning Process

In order to be fully integrated into other aspects of a planned operation, the EWC conducts joint EW planning beginning as early as possible and coordinates it with other aspects of the plan throughout the joint operation planning process. Proper EW planning requires understanding of the joint planning and decision-making processes; nature of time constrained operations; potential contributions of EW; and employment of joint EW. During execution, EW planners must monitor the plan's progress and be prepared to make modifications to the plan as the dynamics of the operation evolve.

Electronic Warfare Planning Guidance

Planning guidance for EW is included as tab D (EW) to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN. EW plans should identify the desired EM profile; identify EW missions and tasks to Service or functional component commanders; evaluate adversary threats; and reflect the guidance, policies, and EW employment authorities.

Electronic Warfare Planning Aids

There are a number of automated planning tools available to help joint EW planners carry out their responsibilities. These tools can be divided into three broad categories: databases, planning process aids, and spatial and propagation modeling tools. **Databases** can assist EW planners by providing easy access to a wide variety of platform-specific technical data used in assessing the EW threat and planning appropriate friendly responses to that threat. **Planning process aids** include aids that automate OPLAN development and automated frequency management tools. Geographic information systems [**spatial and propagation modeling tools**] enable analysis and display of geographically referenced information.

Coordinating Joint Electronic Warfare

Once a plan has been approved and an operation has commenced, the preponderance of electronic warfare staff effort shifts to electromagnetic battle management.

EMBM includes continuous monitoring of the EMOE, EMS management, and the dynamic reallocation of EW assets based on emerging operational issues. Normally, this monitoring is performed by personnel on watch in the joint operations center (JOC).

Joint Electronic Warfare Coordination and Control

At combatant commands and subordinate unified commands, the J-3 is primarily responsible for the EW coordination function. The EW division of the J-3 staff should engage in the full range of EW functions to include deliberate planning; day-to-day planning and monitoring of routine theater EW activities in conjunction with the combatant command's theater campaign plan; and crisis action planning in preparation for EW as part of emergent joint operations. Since EW is concerned with **attacking personnel, facilities, or equipment (EA); protecting capabilities and EMS access (EP); and monitoring, exploiting, and targeting use of the EMS (ES),** EW staff personnel have a role in the **dynamic management** of the EMS, via tools and processes, during operations. A **comprehensive and well-thought-out joint restricted frequency list and emission control plan** are two significant tools that **permit flexibility of EW actions** during an operation without compromising friendly EMS use. The **electronic warfare control authority**, the senior EA authority in the operational area, develops guidance for performing EA on behalf of the JFC.

Service Component Coordination Procedures

Components requiring electronic warfare support from another component should be encouraged to directly coordinate that support when possible.

When the JFC has chosen to conduct operations through functional components, the functional component commanders will determine how their components are organized and what procedures are used. EW planners should coordinate with the functional component electronic warfare elements to determine how they are organized and what procedures are being used by functional component forces.

Army

The Army Service component command or Army component operations staff office (Army division or higher staff) plans, coordinates, and integrates EW requirements in support of the JFC's objectives.

Marines

The MAGTF headquarters EWCC, if established, or the MAGTF EWO, if there is no EWCC, is responsible for coordination of the joint aspects of MAGTF EW requirements.

Navy

The Navy operations directorate is responsible for all Navy EW efforts and provides coordination and tasking to task forces assigned.

Air Force

Air Force requirements for other component EW support are established through close coordination between the JFC's EWC and the commander, Air Force forces' operations directorate (or equivalent operations directorate) or plans directorate (or equivalent plans directorate), in coordination with the Director for Intelligence, A-2.

Special Operations Forces

Requirements from special operations units for EW support will be transmitted to the joint force special operations component command JOC for coordination with the joint force special operations component command IO cell.

United States Coast Guard

During both peacetime and war, joint operations may include United States Coast Guard (USCG) assets that possess EW capabilities. Coordination with USCG assets should be through assigned USCG liaison personnel or operational procedures specified in the OPLAN or operation order.

Electronic Warfare and Intelligence, Surveillance, and Reconnaissance Coordination

It is vital that all prudent measures are taken to **ensure EMS activities are closely and continuously deconflicted with ES** and intelligence collection activities. The J-2 must ensure that EW collection priorities and ES sensors are integrated into a **complete intelligence collection plan.**

Electronic Warfare and Interagency Coordination

Although there may not be intentional targeting of the EMS, inadvertent and unintentional interference may wreak havoc on the systems being used to support the execution of interagency operations. As such, constant and detailed coordination is essential between EW activities and relevant interagency organizations.

Multinational Aspects of Electronic Warfare

As in joint operations, electronic warfare is an integral part of multinational operations.

US planners should integrate US and partner nations' EW capabilities into an overall EW plan, provide partner nations with information concerning US EW capabilities, and provide EW support to partner nations. The planning of multinational force (MNF) EW is made more difficult because of security issues, different cryptographic equipment, differences in the level of training of involved forces, and language barriers.

Multinational Force Electronic Warfare Organization and Command and Control

The multinational force commander (MNFC) **provides guidance for planning and conducting EW operations to the MNF** through the operations directorate's combined EWCC.

Multinational Electronic Warfare Coordination Cell with Allies and Other Friendly Forces

The MNFC should include EWOs from supporting MNFs within the EWCC. Should this not be practical for security reasons or availability, the MNFC should, based on the mission, be prepared to provide EW support and the appropriate liaison officers to the multinational units.

Electronic Warfare Mutual Support

Exchange of SIGINT information in support of EW operations should be conducted in accordance with standard NATO, American, British, Canadian, Australian Armies Program, and Air and Space Interoperability Council procedures, as appropriate. **Exchange of EOB i**n peacetime is normally achieved under bilateral agreement. **Reprogramming** of EW equipment is a national responsibility. However, the EWCC chief should be aware of reprogramming efforts being conducted within the MNF.

Releasability of Electronic Warfare Information to Multinational Forces

A clear, easily understood policy on the disclosure of EW information requested by multinational partners should be developed by the commander's foreign disclosure officer as early as possible.

CONCLUSION

This publication provides joint doctrine for the planning, execution, and assessment of electronic warfare across the range of military operations.

Intentionally Blank

CHAPTER I
OVERVIEW OF ELECTRONIC WARFARE

"There is much more to electronic warfare than simply detecting enemy transmissions."

Martin Van Creveld
***Technology and War,* 1989**

1. Introduction

Military operations are executed in an environment complicated by increasingly complex demands on the electromagnetic spectrum (EMS). All modern forces depend on the EMS. The EMS is the entire range of electromagnetic (EM) radiation. At one end of the spectrum are gamma rays, which have the shortest wavelengths and high frequencies. At the other end are radio waves, which have the longest wavelengths and low frequencies. The EMS is used to organize and explain the types of EM energy that exist in our world and throughout the universe. Devices whose functions depend upon the EMS are used by both civilian and military organizations and individuals for **intelligence; communications; positioning, navigation, and timing (PNT); sensing; command and control (C2); attack; ranging; data transmission; and information storage and processing**. The military requirement for unimpeded access to, and use of, the EMS is the key focus for joint electromagnetic spectrum operations (JEMSO), both in support of military operations and as the focus of operations themselves. Electronic warfare (EW) is essential for protecting friendly operations and denying adversary operations within the EMS throughout the operational environment (OE).

2. Military Operations and the Electromagnetic Environment

a. The Electromagnetic Spectrum

(1) The EMS is a highly regulated continuum of EM waves arranged according to frequency and wavelengths. The EMS (Figure I-1) includes the full range of all possible frequencies of EM radiation.

(2) The use of the EMS is essential to control the OE during all military operations. The transfer of information from the collectors to the platforms will use the EMS. The EMS is constrained by both civil uses and adversary attempts to deny the use of the EMS—creating a congested and contested environment.

b. Joint Electromagnetic Spectrum Operations

(1) JEMSO includes all activities to successfully plan and execute joint or multinational operations in order to control the electromagnetic operational environment (EMOE).

(2) JEMSO are the coordinated efforts of EW and joint electromagnetic spectrum management operations (JEMSMO) to exploit, attack, protect, and manage the EMOE. They

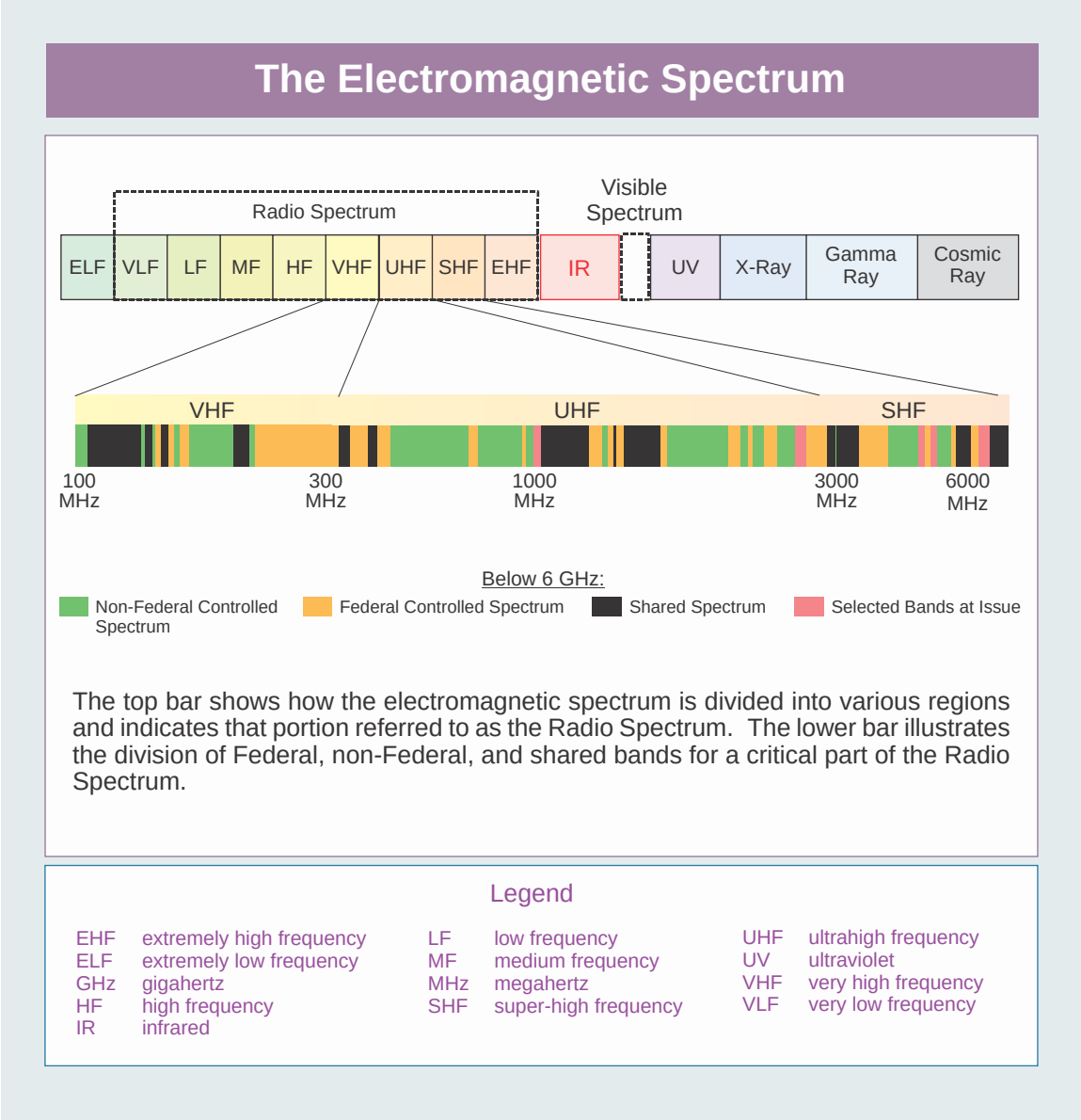


Figure I-1. The Electromagnetic Spectrum

enable EMS-dependent systems to function in the intended OE. JEMSO enable and support the six joint functions through all phases of military operations.

c. The Electromagnetic Operational Environment

(1) As discussed in Joint Publication (JP) 3-0, *Joint Operations*, the OE is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace) (see Figure I-2). The joint force commander (JFC) defines these areas with geographical boundaries in order to facilitate coordination, integration, and deconfliction of joint operations among joint force components and supporting commands.

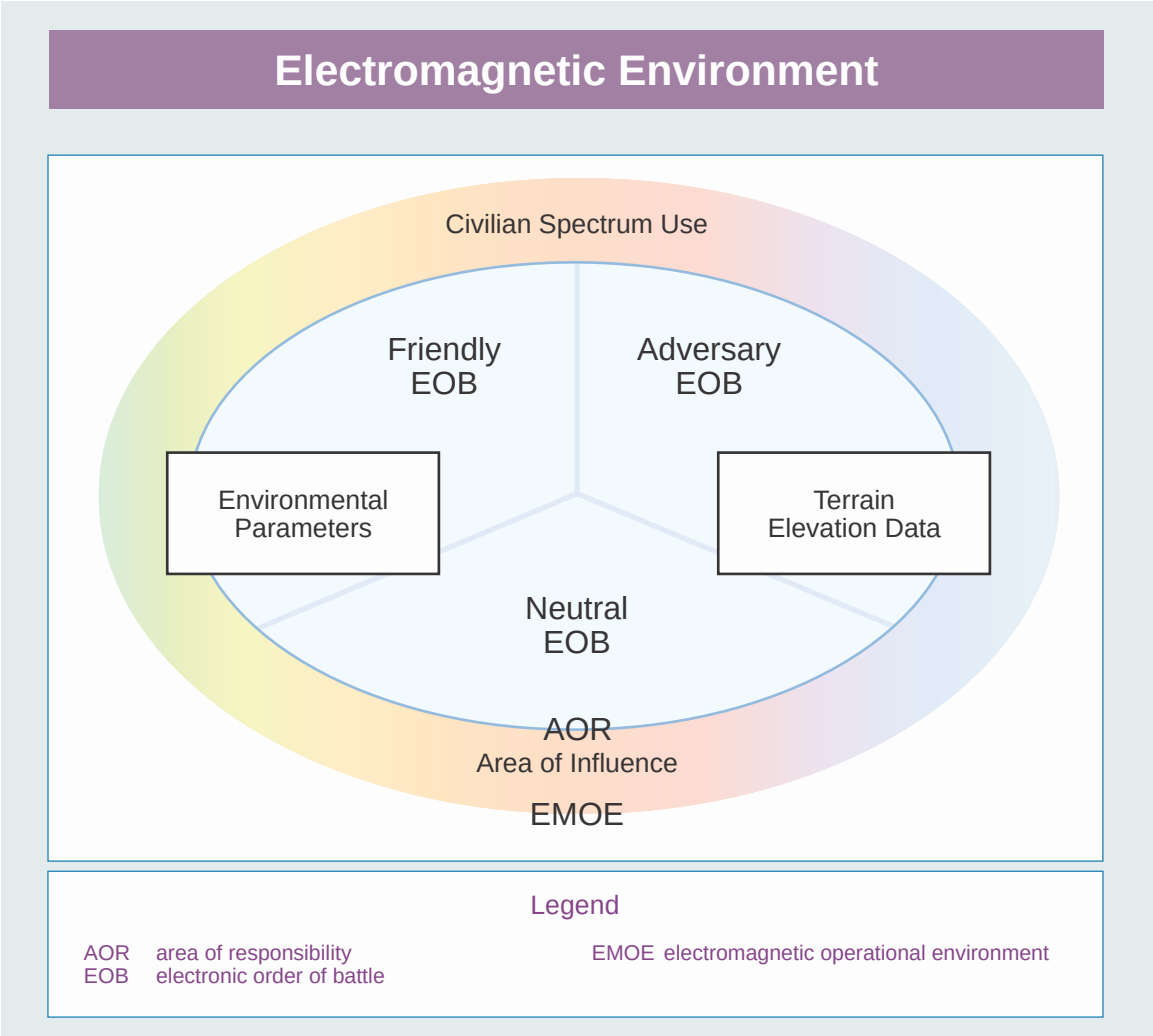


Figure I-2. Electromagnetic Environment

As with the OE, the goal of the JFC is to shape and control the EMOE. However, the electromagnetic environment (EME) in which this occurs transcends all physical domains and the information environment, and extends beyond defined borders or boundaries, thus complicating JEMSO. A variety of factors, including the types of equipment employed, users of the equipment (e.g., air, naval, and land forces), adversary capabilities, geography, and weather also significantly influence the conduct of JEMSO.

(2) The EME is described as the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted EM emissions that may be encountered by a military force, system, or platform when performing its assigned mission in its intended OE. It is the sum of electromagnetic interference (EMI); electromagnetic pulse (EMP); hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of sunspots, lightning, and precipitation static. Essentially, the EME is the global EM background.

(3) The EMOE is the background EME and the friendly, neutral, and adversarial electronic order of battle (EOB) within the EM area of influence associated with a given operational area (OA). This is the portion of the EME where JEMSO is conducted at a given time.

(4) EMS-dependent systems operate more efficiently in specific frequency bands depending on their function. These systems are also affected by different elements of the operating environment (e.g., jungle, urban, or harsh climatic environments). Examples include the adverse effects of fog, rain, and snow on super-high frequencies used for satellite communications (SATCOM); the effects of solar activities such as sunspots, solar flares, and atmospheric fluctuations on systems that use high frequency for propagation; and the effects of man-made interference from other transmitters, power lines, or static electricity on all systems.

d. **Electromagnetic Environmental Effects (E3).** The impact of an EMOE upon the operational capability of military forces, equipment, systems, and platforms is referred to as E3. It encompasses all EM disciplines to include electromagnetic compatibility (EMC); EMI; EM vulnerability; EMP; electronic protection (EP); hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects such as sunspots, lightning, and precipitation static. All EM-dependent systems are vulnerable, to some degree, to the effects of EM energy.

3. Role of Electronic Warfare Across the Range of Military Operations

a. The term EW refers to military action involving the **use of EM energy and directed energy (DE) to control the EMS or to attack the enemy. EW consists of three divisions:** electronic attack (EA), EP, and electronic warfare support (ES). DE is an umbrella term covering technologies that produce concentrated EM energy or atomic or subatomic particles. DE capabilities complement and optimize the use of EW because DE is an enabler for all mission areas. Figure I-3 depicts an overview of EW, the relationships of the three divisions, and the relationship of the divisions to principal EW activities.

b. **Electronic Attack.** EA refers to the division of EW involving the use of **EM energy, DE, 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 (see JP 3-09, *Joint Fire Support*). EA:

(1) Includes actions taken to prevent or reduce an enemy's effective use of the EMS via employment of systems or weapons that use EM energy (e.g., jamming in the form of EM disruption, degradation, denial, and deception). EA includes both active EA, in which EA systems or weapons radiate in the EMS, as well as passive EA (non-radiating/re-radiating) such as chaff.

(2) Includes employment of systems or weapons that use radiated EM energy (to include DE) as their primary disruptive or destructive mechanism. Examples include lasers, electro-optical, infrared (IR), and radio frequency (RF) weapons such as high-power microwave (HPM) or those employing an EMP.

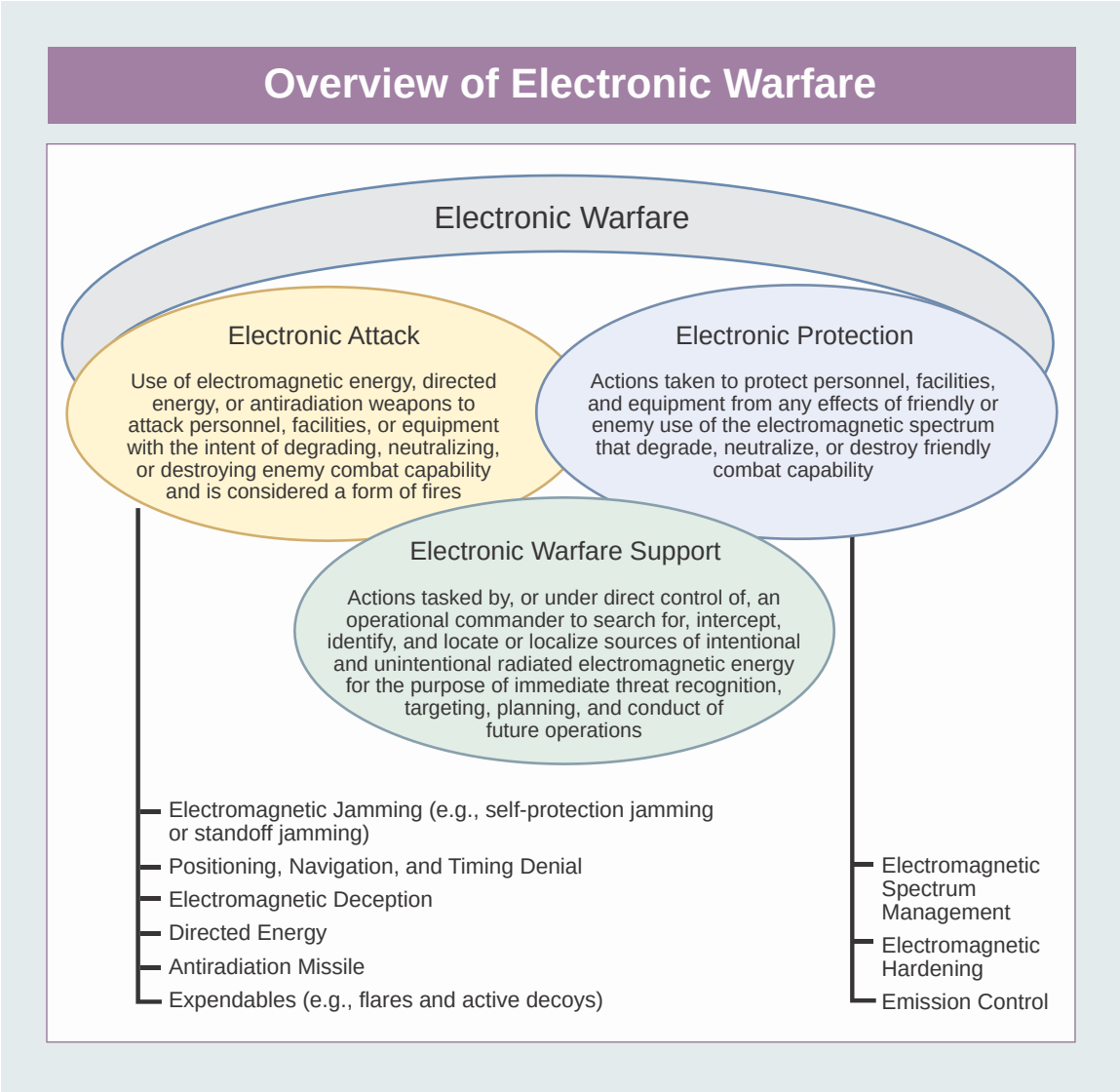


Figure I-3. Overview of Electronic Warfare

(3) Can be used for both offensive and defensive purposes.

(a) Offensive EA activities are generally conducted at the request and onset of friendly force engagement of the enemy. In many cases, these activities suppress a threat for only a limited period of time. Examples include employing self-propelled decoys; jamming an adversary's radar or C2 systems; using antiradiation missiles to suppress an adversary's air defenses; using electronic deception techniques to confuse an adversary's intelligence, surveillance, and reconnaissance (ISR) systems; and using DE weapons to disable an adversary's personnel, facilities, or equipment and disable or destroy material (e.g., satellites on orbit, airborne optical sensors, or massed land forces).

(b) Defensive EA activities use the EMS to protect personnel, facilities, capabilities and equipment. Examples include self-protection and force protection measures

such as use of expendables (e.g., flares and active decoys), protection jammers and lasers, towed decoys, and DE IR countermeasures systems.

c. **Electronic Protection.** EP refers to the division of EW involving actions taken **to protect personnel, facilities, and equipment** from any effects of friendly, neutral, or enemy use of the EMS, as well as naturally occurring phenomena that degrade, neutralize, or destroy friendly combat capability. EP focuses on system or process attributes or capabilities. Inherent hardware features minimize the impact of unplanned/undesired EM signals on an EM-dependent system's operation. EP processes are designed to eliminate, reduce, or mitigate the impact of the same unplanned/undesired EM signals. These features and processes combine to allow friendly capabilities to continue to function, as intended, in contested and congested EMOEs.

(1) EP includes actions taken to ensure friendly use of the EMS, such as frequency agility in a radio, variable pulse repetition frequency in a radar, receiver/signal processing, spread spectrum technology, spectrum management processes, frequency coordination measures (e.g., joint restricted frequency list [JRFL]), Global Positioning System (GPS) signal protection measures, selective opacity (i.e., the phenomenon of not permitting the passage of EM radiation) of optical apertures, emission control (EMCON) procedures, and use of wartime reserve modes (WARMs).

(2) EP is not force protection or self-protection. EP is an EMS-dependent system's use of EM 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. The use of flare rejection logic on an IR missile (i.e., allowing the IR missile to continue to function despite an adversary's use of flares) is EP. The flare rejection technique ensures friendly use of the EMS to track the intended target despite the adversary's self-protection/defensive EA actions (i.e., the flare) to prevent or reduce friendly use of the EMS. Although defensive EA actions and EP both protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA (friendly and/or adversary) or EMI, while defensive EA is primarily used to protect against lethal attacks by denying adversary use of the EMS to target, guide, and/or trigger weapons.

d. **Electronic Warfare Support.** ES refers to the division of EW 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 EM energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. ES prepares the EME for the commander to perform operational missions. ES synchronizes and integrates the planning and operational use of sensors, assets, and processes within a specific battle space to reduce uncertainties concerning the enemy, environment, time, and terrain. ES data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or physical attack, and produce measurement and signature intelligence.

4. Principal Electronic Warfare Activities

The principal EW activities have been developed over time to **exploit the opportunities and vulnerabilities inherent in the physics of EM energy.** Although the basic physics of EM energy has remained constant, activities using convenient and affordable technology have changed dramatically and continue to be a challenge. The principal activities used in EW include the following:

a. **Countermeasures.** Countermeasures are that form of military science that, by the employment of devices and/or techniques, is designed to impair the operational effectiveness of enemy activity. Countermeasures can be active or passive and can be deployed preemptively or reactively. Examples include electro-optical-infrared (EO-IR) and RF countermeasures such as flares or chaff.

(1) **Electro-Optical-Infrared Countermeasures (EO-IR CMs).** Any device or technique employing EO-IR materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. EO-IR CMs may use laser jammers, smokes/aerosols, signature suppressants, decoys, pyrotechnics/pyrophorics, high-energy lasers, or directed IR energy countermeasures.

(2) **Radio Frequency Countermeasures.** Devices and techniques that employ RF technology to impair the effectiveness of adversary activity (e.g., precision-guided or radio-controlled weapons, communications equipment, and sensor systems).

b. **Electromagnetic Battle Management (EMBM).** EMBM is the dynamic monitoring, assessing, planning and directing of JEMSO in support of the commander's scheme of maneuver. EMBM will proactively harness multiple platforms and diverse capabilities into a networked and cohesive sensor/decision/target/engagement system, as well as protect friendly use of the EMS while strategically denying benefits to the adversary.

c. **Electromagnetic Compatibility. EMC** is the ability of systems, equipment, and devices that utilize the EMS to operate in their intended OE **without suffering unacceptable degradation or causing unintentional degradation** because of EM radiation or response. EMC involves the application of sound EMS management: planning, coordinating, and managing joint use of the EMS through operational, engineering, and administrative procedures that ensure interference-free operation; and clear concepts and doctrine that maximize operational effectiveness.

d. **Electromagnetic Deception.** EM deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner **intended to convey misleading information to an enemy** or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of EM deception are the following:

(1) **Manipulative.** This involves actions to eliminate revealing, or convey misleading, EM telltale indicators that may be used by hostile forces.

(2) **Simulative.** This involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.

(3) **Imitative.** This involves actions to imitate enemy emissions to mislead hostile forces.

e. **Electromagnetic Hardening.** EM hardening consists of actions taken to protect personnel, facilities, and equipment by **filtering, attenuating, grounding, bonding, blanking, and shielding** against undesirable effects of EM energy. EM hardening is an EP activity.

f. **Electromagnetic Interference Resolution.** EMI resolution is the step-by-step process used to systematically diagnose the cause or source of EMI. EMI is any EM 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 EA, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and inadequate EMS management.

g. **Electromagnetic Intrusion.** EM intrusion is the intentional insertion of EM energy into transmission paths in any manner, with the objective of **deceiving operators or causing confusion**.

h. **Electromagnetic Jamming.** EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of **preventing or reducing an enemy's effective use of the EMS,** and with the intent of degrading or neutralizing the enemy's combat capability.

i. **Electromagnetic Pulse.** EMP is EM radiation from a strong electronic pulse that can be produced by a nuclear explosion or generated conventionally that may couple with electrical or electronic systems to produce damaging current and voltage surges. EMP may be employed as a weapon (i.e., EA) or accounted for in the shielding and protection (i.e., EP) of friendly equipment, personnel, and facilities against its effects. EMP is one way that a nuclear detonation produces its damaging effects. The effects of EMP can extend to hundreds of kilometers depending on the height and yield of a nuclear burst. A high-altitude electromagnetic pulse (HEMP) can generate significant disruptive field strengths over a continental-size area. The portion of the EMS most affected by EMP and HEMP is the radio spectrum. Planning for communications system protection is significant when the potential for EMP is likely.

For more information on EMP considerations during military operations, refer to JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments*; JP 3-41,* Chemical, Biological, Radiological, and Nuclear Consequence Management*; and Field Manual (FM) 3-11.4/Marine Corps Warfighting Publication (MCWP) 3-37.2/Navy Tactics, Techniques, and Procedures (NTTP) 3-11.27/Air Force Tactics, Techniques, and Procedures (Instruction) (AFTTP[I]) 3-2.46,* Multi-Service Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Protection.

j. **Electromagnetic Spectrum Control**. Freedom of action in the EMOE is achieved through the coordinated execution of JEMSO with other lethal and nonlethal operations impacting the EMOE.

k. **Electronic Intelligence (ELINT) Collection.** ELINT, a subcomponent of SIGINT, is the **technical and geospatial intelligence derived from foreign noncommunications EM radiations** emanating from other than nuclear detonations or radioactive sources.

l. **Electronic Masking.** Electronic masking is the **controlled radiation of EM energy on friendly frequencies** in a manner to protect the emissions of friendly communications and electronic systems against enemy ES measures/SIGINT without significantly degrading the operation of friendly systems.

m. **Electronic Probing.** 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 or systems.

n. **Electronic Reconnaissance.** Electronic reconnaissance is the **detection, location, identification, and evaluation of foreign EM radiations.**

o. **Electronics Security.** 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 communications and noncommunications EM radiations (e.g., radar).

p. **Electronic Warfare Reprogramming.** EW reprogramming is the **deliberate alteration or modification of EW or target sensing systems (TSSs)** in response to validated changes in equipment, tactics, or the EME. These changes may be the result of deliberate actions on the part of friendly, adversary, or third parties, or may be brought about by EMI or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems.

q. **Emission Control.** The selective and controlled use of EM, acoustic, or other emitters to **optimize C2 capabilities** while minimizing, for operations security (OPSEC):

(1) Detection by enemy sensors.

(2) Mutual interference among friendly systems.

(3) Enemy interference with the ability to execute a military deception (MILDEC) plan.

r. **Joint Electromagnetic Spectrum Operations.** JEMSO are the coordinated efforts of EW and JEMSMO to exploit, attack, protect, and manage the EMOE to achieve the commander's objectives.

s. **Joint Electromagnetic Spectrum Management Operations (JEMSMO).** Effective JEMSMO is integral to the successful execution of military operations. They consist of planning, coordinating, and managing joint use of the EMS through **operational, engineering, and administrative procedures.** The primary goal of JEMSMO is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

For more information on JEMSMO, refer to JP 6-01, Joint Electromagnetic Spectrum Management Operations.

t. **Low-Observability/Stealth.** All equipment, personnel, and facilities emit and reflect EM energy as discernible and often characteristic signatures (e.g., heat, light, magnetic, and RF) that can be collected and exploited. Assets involved in operations may incorporate low-observability/stealth EP attributes, thereby increasing their ability to operate in the physical domains by reducing the possibility of their detection and exploitation by adversaries. Low-observability/stealth and other signature reduction techniques also improve the effectiveness of EO-IR CMs.

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

v. **Navigation Warfare (NAVWAR).** NAVWAR refers to deliberate defensive and offensive action to assure and prevent PNT information through coordinated employment of space, cyberspace, and EW operations.

w. **Precision Geolocation.** Precision geolocation involves planning, coordinating, and managing friendly assets to perform the function of geolocating enemy RF systems for the purposes of targeting, using EW assets among other sources of information, and intelligence data.

x. **Wartime Reserve Modes.** WARM are characteristics and operating procedures of sensors, 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. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use.

5. Electronic Warfare Capabilities and Potential Effects

a. EW is conducted to secure and maintain freedom of action in the EMOE for friendly forces to deny the same to the adversary. As an adaptive and responsive form of disruptive or destructive fires, EA's purpose is to gain and maintain friendly advantage within the EMOE and ensure requisite friendly access to the EMS. EW can be applied from all physical domains by manned and unmanned systems. EW may adversely affect friendly forces when not properly integrated and coordinated. EW is employed to create decisive, standalone effects, or to support military operations by generating various levels of control, detection, denial, deception, disruption, degradation, exploitation, protection, and

destruction. EW can further affect the OE by influencing both friendly and adversary leaders and population. EW plays a role at the tactical, operational, and strategic levels of war. Performing EA against an early warning radar, for example, has effects at all levels of war. Tactically, it affects cueing of engagement systems. Operationally, it affects the adversary's ability to mass and synchronize forces. Strategically, it prevents the adversary's senior leadership from maintaining a coherent picture of the national security environment. In another scenario, operational remediation of EMI against a national space-based asset (an EP-related process) would call for direction finding (DF) and geolocation of the source (through ES), and perhaps the decision to conduct EA on that source if attributed to hostile intent. While the actions described in this scenario occur within a tactical, time-sensitive context, the ramifications of the events could have strategic or operational-level significance. The value of EW is manifested fully only when commanders consider and employ capabilities across the OE.

b. EW is vital throughout all phases (shape, deter, seize initiative, dominate, stabilize, and enable civil authority) of an operation or campaign. EP attributes and processes are essential across all phases of conflict to ensure all EMS-dependent capabilities are able to operate effectively in operationally stressed EMOEs. During the shape and deter phases, ES assets contribute to the overall understanding of the OE. A judicious commander may employ EW to implement favorable intelligence preparation of the OE without prematurely crossing the threshold to conflict. The potential to employ nondestructive and nonlethal capabilities make EW assets vital to the preparation of the OE. Using EW, joint forces may set the conditions for combat when imminent and prosecute the attack once combat is under way. The ability to achieve an objective through nondestructive means may allow a more rapid transition from the seize initiative and dominate phases to support operations in the stabilize phase. EW may also employ destructive EM fires, decisive for achieving campaign objectives during the seize initiative and dominate phases. From the stabilize to enable civil authority phase, EW can foster restorative operations by offering nonlethal options such as force protection through ES to monitor subversive elements; EP for ensuring communications capabilities continue to function in EMOEs; EA to counter radio-controlled improvised explosive devices; or broadcasting selected themes and messages, to include civil defense messages, to assist civil authorities.

c. EW applications in support of homeland defense are vital to deter, detect, prevent, and defeat external threats such as ballistic missiles, aircraft (manned and unmanned), maritime vessels, land threats, hostile space systems, domestic/international terrorism, and cyberspace threats.

d. When used in support of a deterrence activity or operation, the role of EW goes beyond simply being available to support potential combat operations. EW can support the shaping of adversaries' perceptions and morale, as well as unit cohesion. EW applied toward deterrence objectives can sever lines of communications, logistics, C2, and other key functions while simultaneously protecting friendly capabilities. The physical presence of EW assets (e.g., airborne ES platforms), as well as enabling freedom of navigation activities, can reinforce the deterrent message.

e. **Control.** The overall goal of EW involves the use of EM energy and DE to control the EMS or to attack the enemy. Control of the EMS is achieved by effective management, coordination, and integration of friendly EMS-dependent systems (e.g., communications, ISR, EW, computer networks) while countering and exploiting adversary systems. EA limits adversary use of the EMS; EP secures use of the EMS for friendly forces; and ES enables the commanders to identify and monitor actions in the EMS throughout the OA. EMBM provides the enabling JEMSO processes to ensure effective control of the EMOE. Additionally, commanders should maximize integration among EW and their other combat capabilities as part of their combined arms operations. Activities in control of the EMS can include, but are not limited to:

(1) **Detection.** Detection is identification of potential enemy EM emissions through use of ES measures. It is the essential first step in any follow-on EW activity. Friendly forces must have the capability to detect and characterize interference as hostile jamming or unintentional EMI.

(2) **Exploitation.** Exploitation is taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. In an EW context, exploitation is ES that refers to taking full advantage of adversary radiated EM energy to identify, recognize, characterize, locate, and track EM radiation sources to support current and future operations. Data transmissions produce EM energy for exploitation by SIGINT, provide targeting for EM or destructive attacks, and develop awareness of operational trends. Examples of exploitation include geolocation of terrestrial EMI sources impacting space assets, terminal homing on adversary communication devices, determination of enemy indications and warnings, and geolocation of RF apertures in cyberspace for targeting. Exploitation may be enhanced or enabled by EA to stimulate target EMS-dependent systems.

(3) **Denial.** Denial is the prevention of access to or use of systems or services. This can be accomplished through numerous means (e.g., EW, computer network operations [CNO], destruction). Denial, in an EW context, is the prevention of an adversary from using EMS-dependent systems (e.g., communications equipment, radar) by affecting a particular portion of the EMS in a specific geographical area for a specific period of time. Denial prevents an adversary from acquiring accurate information about friendly forces. Denial is accomplished through EA techniques (degradation, disruption, or deception); expendable countermeasures; destructive measures; network applications; tactics, techniques, and procedures (TTP); and/or EMCON.

(4) **Disruption.** Disruption is to interrupt the operation of adversary EMS-dependent systems. The techniques interfere with the adversary's use of the EMS to limit the adversary's combat capabilities. A trained adversary operator may be able to thwart disruption through effective EP actions such as changing frequency, EM shielding, etc. The goal of disruption is to confuse or delay adversary action. Disruption is achieved with EM jamming, EM deception, and EM intrusion. These enhance attacks on hostile forces and act as force multipliers by increasing adversary uncertainty while reducing uncertainty for friendly forces. Advanced EA techniques offer the opportunity to nondestructively disrupt or degrade adversary infrastructure.

(5) **Degradation**. Degradation is to reduce the effectiveness or efficiency of adversary EMS-dependent systems. Degradation may confuse or delay the actions of an adversary, but a proficient operator may be able to work around the effects. Degradation is achieved with EM jamming, EM deception, and EM intrusion. Degradation may be the best choice to stimulate the adversary to determine the adversary's response or for EA conditioning.

(6) **Deception.** Deception is measures designed to mislead the adversary by manipulation, distortion, or falsification of evidence to induce the adversary to react in a manner prejudicial to the adversary's interests. Deception in an EW context presents adversary operators and higher-level processing functions with erroneous inputs, either directly through the sensors themselves or through EMS-based networks such as voice communications or data links. Through use of the EMS, EW manipulates the adversary's decision loop, making it difficult to establish an accurate perception of objective reality.

(7) **Destruction.** Destruction is to make the condition of a target so damaged that it can neither function as intended nor be restored to a usable condition. When used in the EW context, destruction is the use of EA to eliminate targeted adversary personnel, facilities, or equipment. Sensors and C2 nodes are lucrative targets because their destruction strongly influences the adversary's perceptions and ability to coordinate actions. Space assets on orbit, as well as computer services in cyberspace, are potentially lucrative targets as well. EW, through ES, supports destruction by providing actionable target locations and/or information. While destruction of adversary equipment is an effective means to permanently eliminate aspects of an adversary's capability, the duration of the effect on operations will depend on the adversary's ability to reconstitute.

(8) **Protection.** Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given OA. It involves the use of physical properties, operational TTP, as well as planning and employment processes to ensure friendly use of the EMS. This includes ensuring that EW activities do not electromagnetically destroy or degrade friendly intelligence sensors, communications systems, PNT capabilities, and other EMS-dependent systems and capabilities. Protection is achieved by component hardening, EMCON, EMS management and deconfliction, and other means to counterattack and defeat adversary attempts to control the EMS. Spectrum management and EW work collaboratively to accomplish active EMS deconfliction, which includes the capabilities to detect, characterize, geolocate, and mitigate EMI that affects operations. Additionally, structures such as a joint force commander's electronic warfare staff (JCEWS) or electronic warfare cell (EWC) enhance operational-level EP through coordination and integration of EW into the overall scheme of maneuver. It is not always possible to prevent the degradation of friendly systems from the effects of friendly forces' EW operations. In these cases, the JFC should make a determination on which system has a higher priority based on the capability provided by each system.

f. **EA Delivery**

EW effects can be generated from a variety of platforms including, but not limited to, aircraft, ground sites, maritime vessels, space assets, and cyberspace. In many cases, techniques and equipment that work in one arena will provide similar success in disparate environments. The same techniques and equipment for isolating the OE may be applicable regardless of whether the target is in a physical domain or the information environment (which includes cyberspace).

6. Electronic Warfare's Role in Irregular Warfare

EW plays a vital role in countering the adversary's use of the EMS during conventional operations or in irregular warfare (IW). During IW, adversaries may operate with unsophisticated electronic means to achieve their objectives. EW is an enabling capability that when integrated into the JFC's concept of operations (CONOPS) will improve the capacity of the joint forces, indigenous government, and its security forces' ability to wage IW. For this reason, it is important to integrate EW early during IW, especially as current and future uses of the EMS multiply. EW can influence the adversary, friendly population, and neutral population, with the JFC's information operations (IO) message, in effort to change/win popular support. Improper application or inadvertent targeting of friendly assets by EW forces may undermine popular support and legitimacy similar to kinetic collateral damage. Proper planning and deconfliction must be accomplished at all levels.

7. Electronic Warfare's Role in Information Operations

a. IO is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation (LOOs) to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting those of friendly forces.

b. EW contributes to the success of IO by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EMS while protecting friendly freedom of action. Expanding reliance on the EMS for a wide range of purposes increases both the potential and the challenges of EW in IO. The increasing prevalence of wireless telephone and computer usage extends both the utility and threat of EW, offering opportunities to exploit an adversary's EM vulnerabilities and a requirement to identify and protect friendly communications from similar exploitation.

c. All EW activities conducted in joint operations should be coordinated through JCEWS or joint EWC. These staffs should integrate their efforts into the JFC's targeting cycle to coordinate nonlethal and lethal fires in strike operations. In addition, they should participate in, and coordinate with, the JFC's IO cell, to align objective priorities and help synchronize EW employment with information-related capabilities and operations.

For more information on IO, refer to JP 3-13, Information Operations.

8. Electronic Warfare's Role in Space Operations

Space operations and space control are enabled by EW. Since space-based operations depend on the EMS, EW must be considered. Most operations in space beyond uncontested communications, physical maneuvering, and uncontested EM collection involve some form of EW. For example, EA may be used to deny an adversary freedom of action in space by preventing the C2 of space assets or by preventing or negating the ability to use space systems and services for purposes hostile to the US. EP aids in the protection of space capabilities of national interest from adversary interference. Finally, ES may be used to maintain awareness of the location and status of friendly and adversary space assets or used to find and fix sources of EMI affecting friendly space-based assets.

For more information on space operations, refer to JP 3-14, Space Operations.

9. Electronic Warfare's Role in Cyberspace Operations

a. The advances in, and proliferation of, advanced technology have created an increasingly complex OE. Wired and wireless networks continue to evolve, and mobile computing devices continue to grow in both capability and number. Couple these emerging trends with an adversary's adaptive use of the EMS and the task becomes all the more challenging. Since cyberspace requires both wired and wireless links to transport information, both offensive and defensive cyberspace operations may require use of the EMS for the enabling of effects in cyberspace. Due to the complementary nature and potential synergistic effects of EW and CNO, they must be coordinated to ensure they are applied to maximize effectiveness. Cyberspace operations may be used to force an adversary from wired to wireless networks that are vulnerable to EA. EW may be used to set favorable conditions for cyberspace operations by stimulating networked sensors, denying wireless networks, or other related actions. In the defensive environment, EW systems may detect and defeat attacks across wireless access points.

b. Primary considerations of EW activities should be their intended and unintended effects on the information technology infrastructures of cyberspace and the broader range of communications architectures comprising the Department of Defense (DOD) information networks, including the possibility of EMI or EM fratricide on friendly communications. The increasing wireless and spaced-based communication path dependencies of cyberspace/DOD information networks infrastructure are susceptible to interference and attack from EW. Therefore, EW and spectrum management experts within the JCEWS or EWC must coordinate closely with the combatant command's theater network operations control center (TNCC) and designated joint frequency management office (JFMO). The TNCC coordinates with United States Cyber Command (USCYBERCOM) to deconflict the anticipated effects of friendly and, if possible, adversary EW operations on cyberspace/DOD information networks infrastructure. In support of United States Strategic Command's (USSTRATCOM's) Unified Command Plan-assigned mission, USCYBERCOM directs operation and defense of the DOD information networks.

c. Network operations (NETOPS) and computer network defense are continuous operations in cyberspace, just as EP and spectrum management are continuous operations in

the EMS. NETOPS are the DOD-wide operational, organizational, and technical capabilities for operating and defending the DOD information networks. NETOPS include, but are not limited to, enterprise management, net assurance, and content management. A secure network is a necessary prerequisite to successful operations. Control of the EMS is a prerequisite to the security of DOD networks due to their increasing reliance on the EMS. EW provides the security for those networks in the EMS as the control and protection mechanism of JEMSO.

10. Electronic Warfare's Relationship to Nuclear Operations

Nuclear operations require a specialized focus, understanding, and an appropriate application of EW. EW during nuclear operations is essential to mission success and therefore must be organized, planned, and coordinated at the national and multinational levels.

11. Electronic Warfare's Relationship to Navigation Warfare

EW produces NAVWAR effects by protecting or denying transmitted global navigation satellite system (GNSS) or other radio navigation aid signals. Delivery of NAVWAR capabilities is also supported by efforts in space control, space force enhancement, and cyberspace operations. EA is used to create NAVWAR effects by degrading, disrupting, or deceptively manipulating PNT transmissions. EP is used to deliver NAVWAR capabilities protecting space, control, or user segments of the GPS/GNSS architecture from disruption or destruction. ES assists NAVWAR through DF and geolocation of intended or unintended transmissions that interfere with effective and timely PNT signal reception.

12. Directed Energy

a. DE is an umbrella term covering technologies that produce concentrated EM energy and atomic or subatomic particles. A **DE weapon** is a system using DE primarily as a means to incapacitate, damage, disable, or destroy enemy equipment, facilities, and/or personnel. **Directed-energy warfare (DEW)** is military action involving the use of DE weapons, devices, and countermeasures to incapacitate, cause direct damage or destruction of adversary equipment, facilities, and/or personnel, or to determine, exploit, reduce, or prevent hostile use of the EMS through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the EMS. With the maturation of DE technology, weaponized DE systems are becoming more prolific, powerful, and a significant subset of the EW mission area. DE examples include active denial technology, lasers, RF weapons, and DE anti-satellite and HPM weapon systems.

b. DEW applications exist in their traditional EW roles as well as fitting into evolving fires applications. For example, a laser designed to blind or disrupt optical sensors is EA. A more powerful version of that laser could be targeted to destroy the aperture or chassis of a satellite on orbit, again performing EA. A laser warning receiver designed to detect and analyze a laser signal is ES, while a visor or goggle designed to filter out the harmful wavelength of laser light is EP.

c. The threat of an adversary's use of destructive DE weapons is growing. Intelligence efforts and assets can be tasked to collect information about this threat, and joint planning should include the development of courses of action (COAs) to mitigate the effects of an adversary's use of these weapons against friendly forces. Intelligence or other data concerning an adversary's deliberate use of a blinding laser weapon should be preserved as evidence of a possible violation of international law (e.g., Protocol IV of the 1980 Convention on Certain Conventional Weapons that prohibits the use of laser weapons with a combat function to cause permanent blindness).

d. DE weapons and devices create effects on designated targets, to include personnel and material. DE weapons may provide precise engagement on a target with limited or no collateral damage. DE weapons also support "escalation of force" efforts when directed by the JFC.

13. Intelligence and Electronic Warfare Support

Intelligence gathering comprises an important portion of the day-to-day activities of the intelligence community (IC) support to military operations. The distinction between whether a given asset is performing an ES mission or an intelligence mission is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. See Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.03C, *Joint Electronic Warfare Policy,* for a classified in-depth discussion of the relationship and distinctions between ES and SIGINT. In simpler terms, the distinction between ES and SIGINT is delineated by purpose, scope, and context. ES assets are tasked by operational commanders **to search for, intercept, identify, and locate or localize** sources of intentional or unintentional radiated EM energy. In contrast, SIGINT assets are tasked by Director, National Security Agency (NSA)/Chief, Central Security Service (CSS) or understanding or temporary SIGINT operational tasking authority by an operational commander. The purpose of ES tasking is **immediate threat recognition, planning, and conduct of future operations,** and other tactical actions such as threat avoidance, targeting, and homing. ES is intended to respond to an **immediate operational requirement.** ES and SIGINT operations often share the same or similar assets and resources, and may be tasked to simultaneously collect information that meets both requirements. That is not to say that data collected for intelligence cannot meet immediate operational requirements. Information collected for ES purposes is normally also processed by the appropriate parts of the IC for further exploitation after the operational commander's ES requirements are met. As such, it can be said that information collected from the EMS has "two lives." The first is as ES, unprocessed information used by operational forces to develop and maintain situational awareness for an operationally defined period of time. The second is as SIGINT, retained and processed under appropriate intelligence authorities in response to specified intelligence requirements. In cases where planned ES operations conflict with intelligence collection efforts, the commander with tasking authority will decide which mission has priority.

Intentionally Blank

CHAPTER II
ORGANIZING FOR JOINT ELECTRONIC WARFARE

"The secret of all victory lies in the organization of the non-obvious."

Marcus Aurelius
Roman Emperor, A.D. 121–180

1. Introduction

How joint staffs are organized to plan and execute EW is a **prerogative of the JFC.** The size of the commander's staff, the mission or missions the joint force is tasked to accomplish, and the time allocated to accomplish the mission or missions are just some of the factors that affect the organization of the staff. This chapter discusses nominal **requirements, organizations, and staff functions** to plan and execute EW in joint operations. It also summarizes EMS management functions and joint-level organization of intelligence support to EW. A brief introduction to **how the Army, Marines, Navy, and Air Force are organized to plan and execute EW** is included to provide background on how joint staff EW functions interact with Service components.

2. Responsibilities

a. As with other combat, combat support, and combat service support functions, EW planning and operations can be divided among multiple directorates of a joint staff based on long-, mid-, and near-term functionality and based upon availability of qualified EW personnel. **Long-range planning** of EW normally occurs under the plans directorate of a joint staff (J-5), while **near/mid-term planning and the supervision** of EW execution normally falls within the purview of the operations directorate of a joint staff (J-3). All aspects of joint EW should be coordinated closely with joint force components. EA should be synchronized with the spectrum management office of the communications system directorate of a joint staff (J-6), and EA and ES activities with the collection management office of the intelligence directorate of a joint staff (J-2). The JRFL is prepared and promulgated by the J-6, coordinated through the EWC, and approved by the J-3. EA, EP, and ES functions significantly affect, and conversely are affected by, activities within the J-2, J-3, and J-6. Examples include ES for collection, management, and dissemination as well as all source analysis of information (J-2); overall EW operations to include OPSEC planning and integration within the IO division (J-3); and day-to-day operations of the DOD information networks, JRFL planning and integration, and EP considerations (J-6).

b. **J-3.** Authority for planning and supervising joint EW is **normally delegated by the JFC to the J-3.** When so authorized, the J-3 will have primary staff responsibility for **planning, coordinating, integrating, and monitoring execution of joint force EW operations.** The J-3 may delegate staff responsibility for EW as appropriate for the size of the staff and scope of J-3 responsibilities.

c. **Command Electronic Warfare Officer (EWO).** Normally, the command EWO is the **principal EW planner** on a joint staff. The scope and nature of the command EWO's

responsibilities are dependent on the size of the staff, the OA of the JFC that the staff supports, and the type of mission or operation the staff must plan. The command EWO is part of the J-3 staff and coordinates internally with other staff organizations and outside organizations, as required.

3. Joint Electronic Warfare Organization

a. **Joint Force Commander's EW Staff.** The JCEWS is headed by the command EWO, who is designated as the JCEWS chief. The JCEWS develops operation plans (OPLANs) and concept plans (CONPLANs) and monitors routine EW operations and activities. It also focuses its efforts on potential contingency areas within the OA and develops the information and knowledge necessary to support contingency planning (e.g., JRFL development). The JCEWS maintains habitual relationships with key individuals (e.g., component liaison officers [LNOs]) and enabling organizations such as Service, functional, and multinational EW cells, the USSTRATCOM Joint Electronic Warfare Center (JEWC), Electromagnetic-Space Analysis Center (ESAC), Joint Spectrum Center (JSC), and Service spectrum management offices. The relationships are refined during training and exercises and optimized via a network of collaboration throughout planning, execution, and assessment.

(1) **Organization of the JCEWS.** The JCEWS should be a standing joint planning group (JPG) with multi-directorate membership. The JCEWS does not require that the headquarters' (HQ's) staff be augmented; rather, it uses existing staff members to participate in a staff organization that focuses on joint EW planning and execution. At a minimum, the JCEWS should consist of core membership from the combatant command/subordinate unified command HQ's J-2, J-3, and J-6. The J-3 and J-6 coordinate to synchronize EW activity that might affect the DOD information networks with USCYBERCOM, through the theater NETOPS centers and TNCCs. The JCEWS should also network with representatives from joint force components (Service and/or functional) and other supporting organizations or agencies. JCEWS membership should be a long-term assignment, and members should be designated spokespersons for their respective organizations. JCEWS membership may include:

(a) JCEWS chief (command EWO).

(b) Standing joint force HQ EW planner (may be dual-hatted as the deputy command EWO when assigned).

(c) JFMO representative.

(d) J-2 SIGINT collection manager.

(e) NSA Cryptologic Support Group (CSG) J-2 representative.

(f) Special technical operations (STO) planner.

(g) J-3 or space NAVWAR representative.

(h) Cyberspace representative.

(i) EM modeling and analysis engineer/representative.

(j) J-2 targets EW lead representative.

(2) JCEWS networked representation may include:

(a) Component EW planners.

(b) LNOs from subordinate and supporting commands.

b. **Joint Electronic Warfare Cell.** The JFC may designate and empower a joint EWC to organize, execute, and oversee conduct of EW. The JFC's decision to designate the joint EWC depends on the anticipated role of EW in the operation. To avoid confusion with the joint EWC (organizationally located with the JFC staff), component-level EW support activities are referred to as electronic warfare elements (EWEs). The land, air, and maritime component EWEs are designated as land-electronic warfare element (L-EWE), air-EWE, and maritime-EWE, respectively. When both the Army and Marine components provide L-EWEs, they should be referred to as Army L-EWE and Marine L-EWE, respectively, to avoid confusion. EWEs may be tasked temporarily with joint EWC responsibilities for the EW aspects of an operation until a joint EWC can be designated and sufficiently manned. The EWC may be part of the JFC's staff or assigned to the J-3. Supporting EWEs placed under a component command must guard against becoming focused on that component's EW issues to the exclusion of the other components. As soon as practical, the EWC should be aligned organizationally and, if possible, geographically colocated with the JFC.

(1) Members of a fully staffed joint EWC should include:

(a) EWC director (should be an EWO).

(b) EWC deputy director.

(c) EWC operations chief.

(d) EWC plans chief.

(e) EW duty officer(s).

(f) EW planner(s).

(g) Operations analyst(s).

(h) SIGINT and/or ELINT analyst(s).

(i) STO planner.

(j) Spectrum manager.

(k) EW asset LNOs.

(l) NAVWAR planner.

(m) Space representative.

(n) Cyberspace representative.

(o) Ground EW logistics planner.

(p) Electrical engineer/EM modeling analyst.

(q) Meteorological and oceanographic (METOC) officer.

(r) Joint interface control officer network manager.

(s) Ground EW asset manager.

(t) SIGINT planner(s).

(2) Joint EWC networked representation should include:

(a) Service/functional component LNOs.

(b) Other government department and agency representatives.

(c) Coalition partner representatives.

c. JCEWS and joint EWC responsibilities:

(1) Specific JCEWS functions and responsibilities:

(a) Maintain EW support to current theater OPLANs and CONPLANs.

(b) Prepare EW portion of estimates and tabs to joint force OPLANs.

(c) Formulate, recommend, and develop EW targets to support the JFC's OPLAN.

(d) Implement and manage EW policies.

(e) Develop and maintain contingency/EWC manning options and COAs.

(2) The following functions may be performed by the JCEWS and will transfer to the joint EWC once established by the JFC:

(a) Provide EW planning and coordination expertise to the JFC. Develop a daily EW battle rhythm that supports EW planning and operations requirements.

(b) Prepare the EW portion of estimates and tabs for operation orders (OPORDs) and identify authorities necessary to implement the OPORD.

(c) Identify requirements for intelligence support to joint EW operations, including assistance to the J-2 in planning the collection and dissemination of ES information.

(d) Define and develop intelligence requirements to support EW operations.

(e) Coordinate with intelligence organizations, collections managers, ISR assets, and national agencies when assessing adversary EW capabilities and limitations.

(f) Coordinate with appropriate DOD intelligence or ISR organizations and national agencies to weigh intelligence gain/loss (IGL) of EA or the physical destruction of targets, and if necessary, coordinate the resolution of these conflicts. Resolution of IGL conflicts resides with the J-3. Request support form J-2 targets if needed.

(g) Plan, coordinate, and assess offensive and defensive EA requirements.

(h) Maintain current assessment of EW resources available to the JFC (to include number, type, and status of EW assets) and analyze what resources are necessary to accomplish the JFC's objective.

(i) Assist JFC by recommending the level of EW support required of the component commanders.

(j) Prioritize EW targets based on JFC objectives, the EW plan, and available assets.

(k) Represent EW within the joint targeting coordination board (JTCB).

(l) Predict effects of friendly and enemy EW activity on joint and multinational operations using applicable modeling and simulation tools.

(m) Plan, coordinate, and assess EP (e.g., spectrum management procedures, EW deconfliction, and EMCON).

(n) Coordinate joint/urgent operational needs statements that affect the EMS.

(o) Coordinate entry of EW systems into the OA.

(p) Coordinate regularly with joint spectrum management element (JSME), and direct activities to resolve spectrum use conflicts resulting from EW activities.

(q) Carry out electronic warfare control authority (EWCA) responsibilities.

(r) Coordinate and monitor joint coordination of electronic warfare reprogramming (JCEWR) by identifying where EW reprogramming decisions and

reprogramming actions affect joint force tactical operations and disseminating theater-wide EW plans, as required.

(s) Recommend and promulgate EW special instructions and rules of engagement (ROE).

(t) Plan, coordinate, integrate, and deconflict EW in current and future operations taking into consideration nontraditional capabilities (e.g., space, special operations, and STO) within the OA.

(u) Compile and coordinate EW support requests from all components according to the priorities set by the JFC.

(v) Coordinate, through the chain of command, to resolve any component or multinational EW requests that cannot be met at the JCEWS/EWC level.

(w) Monitor and adapt execution of EW plans in current operations and exercises.

(x) Reference lessons learned information systems during the planning process, archive EW planning and execution data, and document EW lessons learned in accordance with the joint lessons learned program. The Joint Lessons Learned Information System Web site can be found at https://www.jllis.mil or http://www.jllis.smil.mil.

(y) Coordinate actively with the J-6 to document incoming and outgoing EW and EMS-dependent systems so EMS databases can be accurately maintained.

(z) Coordinate, plan, and oversee execution of NAVWAR EW activities that ensure friendly force access to GPS/PNT sources while denying adversary access to GPS/GNSS/PNT sources.

(aa) Develop and coordinate corrective actions to be taken to maintain friendly force connectivity before, during, and after EW operations are employed.

(3) Joint EWC Support Requirements. When activated, the EWC should be located in, or have access to, a sensitive compartmented information facility (SCIF) to allow for appropriate security. Optimal EWC staffing will include STO cleared personnel in order to coordinate and deconflict STO issues and capabilities. The EWC will also require access to the administrative, intelligence, logistics, legal, and communications/network support made available to the J-3 staff.

(a) Administrative. Administrative support includes, but is not limited to, clerical assistance; classified material control; publications management; update, maintenance, and display of operational SIGINT data; and the provision of general administrative materials.

(b) Intelligence. The EWC will require direct access to all-source intelligence to maintain full knowledge of an adversary's intentions and capabilities. Intelligence support

should include specific and detailed combat information, intelligence, and ES information (e.g., adversary electronic systems; scheme of maneuver; communications system capabilities and deployment; EMS-dependent weapon systems capabilities and deployment; PNT dependencies and EA capabilities; EW activities; and SIGINT collection plans). The J-2 and theater EW units should continually coordinate to ensure mission reports are received in a timely manner and disseminated to the staff and other agencies, as required.

(c) Logistics. Logistic support for the EWC includes, but is not limited to, storage containers for classified material, desks, maps, information display facilities, and messing and billeting of assigned personnel.

(d) Communications. The EWC should keep the J-6 aware of its communication/network requirements. These requirements depend directly on the level of EW activities involved in joint operations. Provisions must be made for secure, reliable, and timely communications support. The EWC should be able to communicate with both component EW authorities/agencies and appropriate external authorities concerning coordination of EW activities. The EWC must also be able to communicate with coalition partners within releasability restraints.

(e) Legal. Support for the joint EWC includes legal support to review and obtain the necessary authorities and to review the plan for compliance with ROE and applicable domestic and international law, including law of armed conflict (LOAC).

4. Joint Frequency Management Organization

Each geographic combatant commander (GCC) is specifically tasked by policy (CJCSI 3320.01C, *Electromagnetic Spectrum Use in Joint Military Operations*) to establish a frequency management structure that includes a **JFMO** and to **establish procedures** to support planned and ongoing operations. The supported combatant commander (CCDR) authorizes and controls use of EMS resources by the military forces under his command. Each supported GCC establishes a command policy on how the EMS will be used in his area of responsibility (AOR), obtains clearance (or approval) from host nations (HNs) for use of the EMS (through existing coordination procedures), and ensures assigned military forces are authorized sufficient use of the EMS to execute their designated missions. To accomplish these tasks, each supported CCDR establishes a JFMO, typically under the cognizance of the J-6, to **support joint planning, coordination, and operational control of the EMS** for assigned forces. A JSME may be established at any level of command. The combatant command JFMO, or the JSME within a joint task force (JTF), may be assigned from the J-6 staff, from a component's staff, or from an external organization such as the JSC (see Annex E, "Joint Spectrum Center," to Appendix B, "Organizations Supporting Joint Electronic Warfare"). In any event, the combatant command JFMO, or the JSME within a JTF, should be staffed with trained spectrum managers, preferably with experience in joint EMS use and knowledge of the EMS requirements of the combatant command component forces.

For more information on the basic process the combatant command JFMO or the JSME within a JTF uses to carry out its primary responsibilities, refer to Chapter III, "Planning Joint Electronic Warfare," and Chapter IV, "Coordinating Joint Electronic Warfare." For

more information about the JFMO/JSME and their functions and processes, refer to Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3320.01B, Joint Operations in the Electromagnetic Battlespace.

5. Organization of Intelligence Support to Electronic Warfare

a. **Intelligence support** to joint military operations is organized into four levels (see Figure II-1). Each of these levels is closely and continuously involved in providing support for EW.

b. **National-Level Intelligence Organizations.** At the national level, organizations and agencies such as the Central Intelligence Agency (CIA), NSA/CSS, National Geospatial-Intelligence Agency (NGA), and Defense Intelligence Agency (DIA) are constantly seeking to **identify, catalog, and update the EOB** of identified or potential adversaries. The ESAC

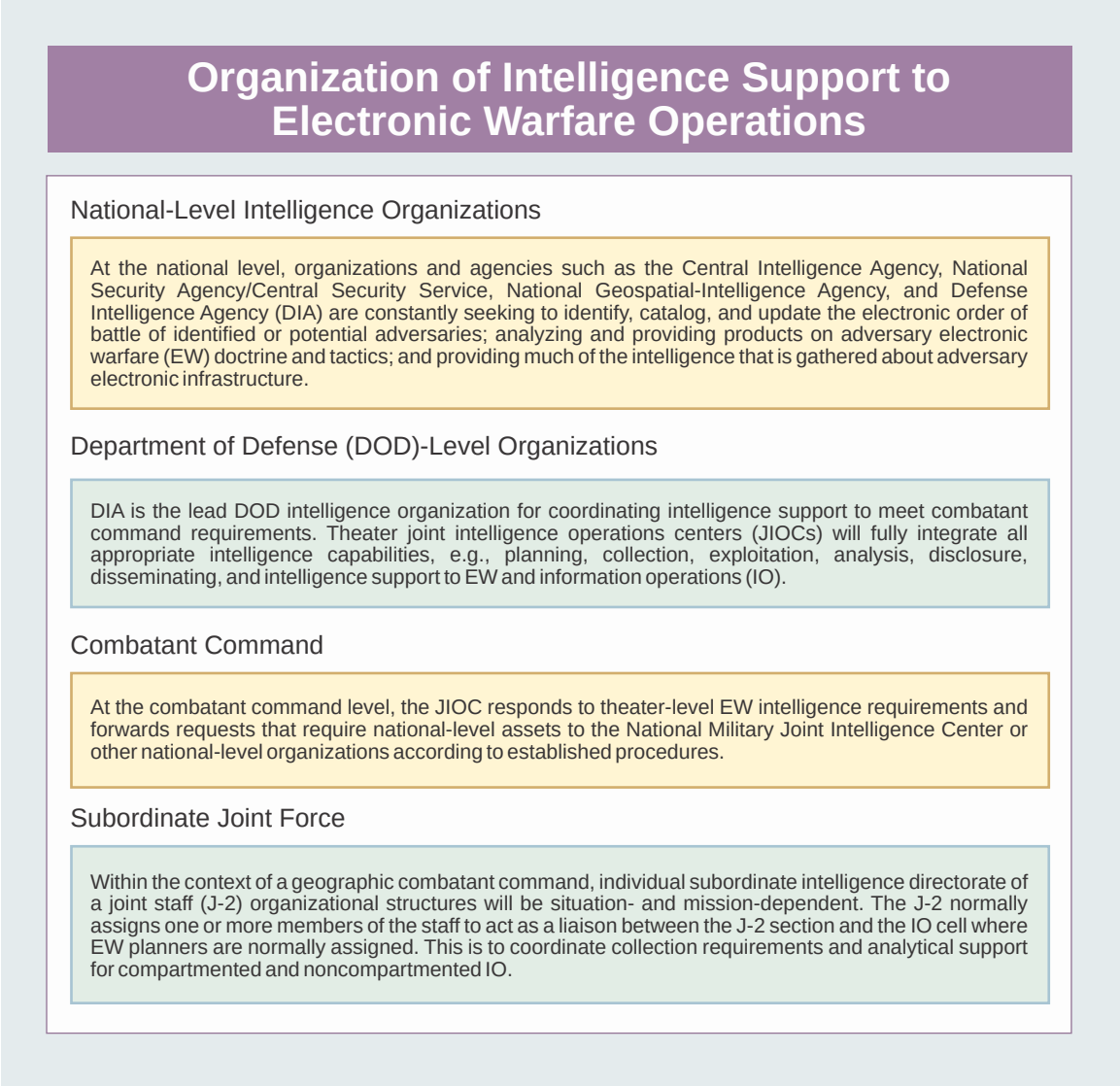


Figure II-1. Organization of Intelligence Support to Electronic Warfare Operations

serves as an operationally focused analytical clearinghouse for all EMS-related databases that provide intelligence support to EW. National-level organizations such as the National Air and Space Intelligence Center (NASIC), National Ground Intelligence Center (NGIC), and National Maritime Intelligence Center not only define EW target parameters and associated system performance, but also analyze and provide intelligence on adversary EW doctrine and tactics. National-level collection efforts also provide much of the intelligence gathered about adversary EM infrastructures. The DIA defense collection coordination center (DCCC) is the focal point for tasking national assets to collect intelligence in response to EW intelligence requirements. EW intelligence requirements that cannot be met by lower-level intelligence assets are forwarded to DCCC or other national-level organizations according to established procedures for prioritization and tasking to national assets.

For more information on the organization of national-level intelligence support, refer to JP 2-01, Joint and National Intelligence Support to Military Operations.

c. **Combatant Command.** At the combatant command level, intelligence support to military operations is focused in the **joint intelligence operations center (JIOC).** The JIOC responds to theater-level EW-related intelligence requirements and forwards requests that require national-level assets to the DCCC or other national-level organizations according to established procedures. EW planners at the combatant command level work with the command's J-2 staff to **satisfy EW intelligence requirements** according to command-specific procedures established by each CCDR.

For more information on theater-level intelligence support and multinational intelligence sharing, refer to JP 2-0, Joint Intelligence.

d. **Subordinate Joint Force.** The J-2 is the **primary point of contact** for providing intelligence support to joint EW. At the discretion of the JFC, a JTF **joint intelligence support element (JISE)** may be established to augment the subordinate joint force J-2 element. Under the direction of the joint force J-2, a JISE normally **manages the intelligence collection, production, and dissemination** of a joint force. The J-2 normally assigns one or more members of its staff to act as a liaison between the J-2 section of the staff and the EWC. The purpose of this liaison is to coordinate collection requirements and analytical support for compartmented and non-compartmented IO. Because of the close interrelationship between some ES and SIGINT activities, EW planners may find it necessary to work with a wide variety of personnel in the intelligence section of the staff.

For more information on how the IC is organized to support joint military operations, refer to JP 2-01, Joint and National Intelligence Support to Military Operations.

6. Service Organization for Electronic Warfare

a. Each Service has a different approach to organizing its forces. Therefore, a basic understanding of each Service's EW organization facilitates planning and coordination of EW at the joint level.

b. **Army**

(1) Army EW operations provide the land force commander with EW capabilities to fully support EMS operations, necessary to effectively conduct maneuver warfare on the modern battlefield. The ability to deny adversary use of the EMS, while preserving friendly EMS use, is imperative in the support of all six joint functions. Commanders and staffs determine which resident and joint force EW capabilities to leverage in support of operations. As commanders apply the appropriate level of EW effort, they can seize, retain, and exploit the initiative within their EMOE.

(2) The Army is organized to work in the structure of an electronic warfare working group (EWWG) with the foundation of the group centered on the EWO, the EW technician, and the EW specialist, who comprise the electronic warfare coordination cell (EWCC).

(3) The EWWG is comprised of, but not limited to, members of the following:

(a) Army component operations staff office (Army division or higher staff) (G-3)/S-3 (battalion or brigade operations staff office [Army battalion or regiment]).

(b) Army component intelligence staff office (Army division or higher staff) (G-2)/battalion or brigade intelligence staff office (Army battalion or regiment) (S-2).

(c) G-5 (Army component plans staff office [Army division or higher staff])/ S-5 (battalion or brigade plans staff office [Army battalion or regiment]).

(d) Army component communications staff office (Army division or higher staff) (G-6)/battalion or brigade communications staff office (Army battalion or regiment) (S-6).

(e) Army component information operations staff office (Army division or higher staff) (G-7)/ S-7 (battalion or brigade information operations staff office [Army battalion or regiment]).

(f) EWCC.

(g) Fires.

(h) Air LNO.

(i) STO/technical operations planner.

(j) Space operations.

(k) Maneuver LNOs.

(l) Special operations forces LNO.

(4) As a team lead by the EWO, the EWWG will provide the ground commander with available EW options, capabilities, and limitations during the military decision-making process to best organize all EW assets at the unit's disposal for full-spectrum operations. If assets are nonorganic to the unit, the EWO/EWCC has the knowledge, skills, and abilities to coordinate with higher headquarter to request the proper support at the proper time and location. It provides advice on technical and tactical employment of all assigned EW systems and tasked or requested nonorganic EW systems to include ES and EP activities. In coordination with G-2/S-2 and G-6/S-6, the EWCC identifies emerging EW threats or trends and develops mitigation measures to overcome new adversarial EW actions. It also recommends the use of ES for immediate target prosecution and triggering criteria and EP measures to provide resolution. As key EW planners and integrators, members of the EWCC provide EW input to the brigade ISR synchronization meeting, operations and intelligence working group, and targeting/planning meetings. As additional necessary tasks, the EWCC, or the EWCC in concert with the EWWG, will do the following:

(a) Generate and update EW staff estimates.

(b) Update and disseminate changes to the enemy tactical EW order of battle to include associated targeting information and necessary intelligence generation.

(c) Monitor and prioritize the processing of EA and review EW battle damage assessment.

(d) Coordinate with legal section to ensure EW operations comply with LOAC and ROE criteria.

(e) Advise members of the command group or staff on all matters concerning Army EW requests, requirements, and priorities.

(5) The EWO is part of the Army EWE of the fires functional cell at brigade and above. At the battalion level, an EW noncommissioned officer is part of the battalion staff. With responsibility for the overall planning, coordination, and supervision of Army EW actions, they are responsible for facilitating the internal (Army) and external (joint) integration, synchronization, and deconfliction of EW actions with the joint functions. The EWO reports through the chief of fires (fire support officer for brigade and below) for those EW actions. For planning, synchronizing, and deconflicting EW actions in support of EMS operations, the EWO coordinates with G-7, G-6, and G-2 elements, and the air LNO through the tactical air control party.

(6) Given the Army's dependence on cyberspace as well as the EMS, commanders must fully integrate cyberspace/electromagnetic activities within the overall operation. These activities employ a combined arms approach to operations in contested cyberspace and a congested EMS. Cyberspace/EM activities focus on seizing, retaining, and exploiting advantages in cyberspace and the EMS. Cyberspace/EM activities are divided into two lines of effort (LOEs). The cyberspace operations LOE aims to achieve objectives in and through cyberspace. The EW LOE aims to control the EMS or to attack the enemy. The Army's

EWE and working group will coordinate, plan, and integrate cyberspace/EM activities for the commander.

For more information on the joint functions, refer to JP 3-0, Joint Operations.

c. **Marine Corps**

(1) The Marine Corps employs EW as a part of maneuver warfare with the intent to disrupt the adversary's ability to command and control forces, thereby influencing the adversary's decision cycle. Marine EW assets are integral to the Marine air-ground task force (MAGTF). Marine EW units are found across the entire MAGTF. The MAGTF command element task organizes and coordinates EW systems to meet MAGTF EW needs and ultimately achieve the JFC's objectives.

(2) EW units are integrated into the commander's CONOPS and scheme of maneuver to enhance the MAGTF's inherent combined arms capabilities. Through this integration of aviation and ground EW capabilities, the MAGTF is able to exploit both the long- and short-term effects of EW, conducting active EA, EP, and ES operations to support the operational requirements of the MAGTF commander, as well as those of the JFC during joint operations.

(3) The MAGTF operations officer or one of the staff officers has responsibility for planning and coordinating MAGTF EW operations and activities. Ground-based EW is provided by the radio battalion (RADBN), and airborne EW is provided by EA-6Bs from the Marine tactical electronic warfare squadrons (VMAQs). The RADBN is organized and equipped to conduct tactical SIGINT and ground-based EA and ES in support of the MAGTF. To accomplish this mission, the RADBN provides the MAGTF with task-organized detachments. VMAQs conduct EW, tactical electronic reconnaissance, and ELINT operations in support of the MAGTF. With the employment of RADBNs and VMAQs, the Marine Corps possesses a unique capability to provide **EW support and SIGINT to the MAGTF commander and any subordinate elements** while also providing invaluable support and information to the JFC. The MAGTF commander will normally plan, synchronize, coordinate, and deconflict EW operations through an EWCC, which is under the cognizance of the fires or effects cells. The EWCC will have a resident EWO (serving as the MAGTF EWO) who is responsible for ensuring all EW plans are included in the appropriate OPLAN annex. The MAGTF EWO assumes overall responsibility for planning and coordinating EW operations. When participating in joint or multinational operations, the joint force air component commander (JFACC) (if established) will coordinate with the MAGTF for scheduling Marine Corps air assets in the air tasking order (ATO). When airborne assets are apportioned to support joint air operations, they will be monitored by the EWC for EW missions and be under tactical control of the JFACC.

d. **Navy**

(1) Navy EW is executed by surface ships, aircraft, and submarines organized in strike groups. For each strike group, the information operations warfare commander (IWC) is responsible for **coordinating and integrating** EW, typically through the strike group

EWO, into naval and joint operations. EW execution requires continual monitoring by EW personnel and is delegated to the EW control ship, usually an aircraft carrier or large deck amphibious ship serving with the strike group. Naval strike groups employ a variety of organic shipboard EW systems. Emphasis is on:

(a) ES to detect, identify, and locate potential threats and friendly forces, enhancing situational awareness.

(b) EA for self-protection, principally to defeat incoming anti-ship missiles and to deny adversary use of the EMS.

(c) Maintaining friendly force availability of EMS and space resources to ensure robust communication, surveillance, reconnaissance, data correlation, and navigation capabilities.

(2) Naval aviation is the primary means the Navy uses to project EW at extended ranges. Carrier and land-based EA-6B Prowlers and EA-18G Growlers use a variety of onboard systems to conduct EA (including both standoff and close-in jamming) and ES in support of suppression of enemy air defenses (SEAD), communications EA, and other IO taskings. Embarked airborne EA assets are normally under the direction of the strike warfare commander. When executing strike operations, air wing EA assets remain under the operational control of the strike warfare commander and come under the tactical control of the airborne mission commander. When participating in joint or multinational operations, the strike warfare commander is responsible for coordinating, with the JFACC or combined force air component commander, integration of air wing assets into the ATO. Additional EW tasking may originate with the EWC and be coordinated with the JFACC. When EA airborne assets are assigned ashore as part of an expeditionary force, they will be under the tactical control of the JFACC. Shore-based aircraft such as the EP-3E Aries II primarily provide Navy airborne ES. Either will be assigned national tasking or strike group tasking, or the JFACC will assign joint force tasking as scheduled by the ATO. Each will have tactical control of these aircraft.

(3) **Navy Coordination Procedures.** A maritime operations center (MOC) at each numbered fleet conducts operational-level coordination. The MOC IO cell is responsible for all Navy EW efforts and provides coordination and tasking to task forces assigned. Each MOC should have an EWO and a senior cryptologic technician—technical to conduct EW coordination as members of the IO cell and in liaison with other cells requiring EW expertise. The IWC at the strike group integrates and executes EW at the tactical level. When naval task forces are operating as a component of a joint force, the IWC provides an assessment of Navy EW capabilities to the other component operation centers and coordinates EW operations with appropriate component EW agencies.

For more information, refer to NTTP 3-51.1, Navy Electronic Warfare, *and NTTP 3-13.2,* Information Operations Warfare Commander's Manual.

e. **Air Force**

(1) Within the Air Force component, dedicated EW support assets conduct a variety of EA, EP, and ES operations and support SEAD and IO mission areas. These are all under the operational control of the **commander, Air Force forces (COMAFFOR).** The objective of all Air Force EW operations is to attack the adversary, enhance the effectiveness of other military operations, increase the probability of mission success, and increase aircraft survivability.

(2) The military significance of EW is directly related to the increase in mission effectiveness and to the reduction of risk associated with attaining air superiority. Air Force EW system development and employment focus on these tasks using an integrated mix of sensing, disruptive, and destructive EW systems to defeat hostile integrated air defenses. Disruptive EW systems (e.g., self-protection jamming and the EC-130H Compass Call) provide an immediate but perishable solution. ES systems (e.g., RC-135V/W and aircraft radar warning receivers) are key to successfully disrupting and/or destroying targets. Destructive systems provide a more permanent solution, but may take longer to achieve the desired results. The integrated use of disruptive and destructive systems offsets their individual disadvantages and results in a synergistic effect.

(3) Within the COMAFFOR HQ, the responsibility for providing EW support to joint operations lies within the operations directorate (A-3) and plans directorate (A-5). However, **functional planning for, directing, and providing of Air Force EW capabilities is normally conducted by the JFACC (when one is designated by the JFC)** through the joint air operations center's EWC. The EWC, as a part of the Air Force air and space operations center (AOC), coordinates with other planning and targeting activities to develop/monitor EW plans and operations in support of the JFC. The EWC consists of an EW plans element and an EW operations element. In response to the ATO, wing and unit staffs and individual aircrews conduct detailed tactical planning for specific EW missions. Due to the high demand for support from Air Force dedicated tactical systems, these systems are normally organized as separate EW wings and squadrons. For the same reason, within the Air Force component, Air Force EA and ES systems are normally organized within Air Force wings or squadrons. The COMAFFOR carefully allocates their employment through the ATO process in accordance with JFC priorities and in coordination with the JFC's EWC. Wing commanders are supported by staff defensive systems officers or EWOs. These officers work with the wing operations intelligence staff to analyze and evaluate the threat in the OA. The defensive systems officer, EWO, and electronic combat officer also plan available EW equipment employment and oversee radar warning receiver and EW systems reprogramming. In addition, they should participate in, and coordinate with, the JFC's IO cell, to align objectives and synchronize EW employment with other capabilities.

For more information on EW employment factors, refer to Air Force Tactics, Techniques, and Procedures (AFTTP) 3-1.IO, Information Operations Planning. Integration, and Employment Considerations, *and AFTTP 3-1,* Compass Call. *AFTTP 3-1 volumes are available online via SECRET Internet Protocol Router Network (SIPRNET) at http://www.nellis.af.smil.mil/units/561jts/.*

CHAPTER III
PLANNING JOINT ELECTRONIC WARFARE

"War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled."

Major General Carl von Clausewitz
***On War,* viii, 1832, tr. Howard and Paret**

1. Introduction

a. EW is a complex mission area that should be **fully integrated** with other aspects of joint operations in order to achieve its full potential. Such integration requires **careful planning.** EW planners must coordinate **their planned activities with other aspects of military operations that** use the EMS, as well as third party users that EW does not wish to disrupt. Coordination of military EMS use is done primarily by working with other staff sections (primarily the J-2 and J-6) and components (to include allies and coalition partners) that rely on the EMS to accomplish their mission. Coordination of EW activities, in the context of third party EMS use, is largely a matter of EMS management and adherence to established frequency usage regimens and protocols.

b. Joint EW is **centrally planned and directed and decentrally executed.** Service and functional component EW planners should be integrated into the joint planning process. The JFC may delegate control of EW operations to a component commander or other selected commanders; however, such delegation does not eliminate the requirement for joint and/or multinational coordination of EW operations. This chapter:

(1) Provides guidance on the joint EW planning process.

(2) Discusses some of the considerations for planning EW in support of military operations.

(3) Provides guidance on preparation of tab D (EW) to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN and/or OPORD.

(4) Briefly discusses some of the automated decision aids that may be used to assist with planning joint EW.

c. EW and its divisions create effects throughout the OE to include the physical domains and the information environment (which includes cyberspace). The nature of EW means that effects have cross-domain implications. Fires must be integrated into joint planning and execution. EW planners must coordinate EW efforts at the JFC level in order to minimize unintended consequences, collateral damage, and collateral effects.

2. Electronic Warfare Planning Considerations

a. **EMS Management.** Since EW activity may create effects within and throughout the entire EMS, joint **EW planners must closely coordinate their efforts** with those members of the joint staff who are concerned with managing military EMS use. EMS management deconflicts military, national, and HN systems (e.g., EP, communication, sensors, space/PNT, and weapons) being used in the OE. EMS management primarily involves determining the specific activities that will take place in each part of the available EMS. This is accomplished by planning, coordinating, and managing EMS use through operational, engineering, and administrative procedures. Figure III-1 shows the steps involved in JFMO spectrum management responsibilities. For operations within a GCC's AOR, the subordinate JFCs follow this spectrum management guidance as amplified by the GCC. The JTF commander coordinates and negotiates modifications necessary for a specific JTF situation with the GCC's staff. Joint EW planners should establish and maintain a close working relationship with frequency management personnel. A critical management tool to enable effective use of the EMS during military operations is the EMS database. All frequencies need to be registered in the joint EMS database. Frequencies in the database that require extra protection from EA activities need to be listed on the JRFL. The JRFL is a list that operational, intelligence, and support elements use to identify the level of protection desired for various networks and frequencies and is limited to the minimum number of frequencies necessary for friendly forces to accomplish JTF objectives. The JRFL is based on inputs from the J-2, J-3, and J-6. It is usually published, distributed, and maintained by the J-6, typically through the JFMO/JSME. The J-3 is the release authority for the coordinated listing. It may be necessary to coordinate the protection of intelligence collection frequencies via the EA request process instead of the JRFL to meet the time-sensitive needs of collection activities.

For more information on frequency deconfliction procedures and generating the JRFL, refer to Appendix D, "Electronic Warfare Frequency Deconfliction Procedures." For more information on EMS management, refer to CJCSM 3320.01B, Joint Operations in the Electromagnetic Battlespace. *For more information on the JSC, refer to Annex E, "Joint Spectrum Center," to Appendix B, "Organizations Supporting Joint Electronic Warfare."*

b. **EW Support of SEAD.** SEAD is a specific type of mission intended to **neutralize, destroy, or temporarily degrade** surface-based adversary air defenses with destructive and/or disruptive means. Joint SEAD is a broad term that includes **all SEAD activities** provided by one component of the joint force in support of another. SEAD missions are of critical importance to the success of any joint operation when control of the air is contested by an adversary. SEAD relies on a variety of EW platforms to conduct ES and EA in its support, and EW planners should coordinate closely with joint and component air planners to ensure **EW support to SEAD missions is integrated into the overall EW plan.**

For more information on SEAD, refer to JP 3-01, Countering Air and Missile Threats.

c. **EW Support Against a Nontraditional Threat.** Contingency operations have shown the enemy's ability to use commercial EM communications in a number of nontraditional ways. These include early warning and coordinated attack communication,

Joint Frequency Management Office Spectrum Management Process

1. Develops the spectrum-use plan. This is particularly vital in support of command and control hand-overs that are highly dependent on radio systems.
2. In conjunction with the J-2, J-3, J-5, J-6, and combatant command joint frequency management office (JFMO), prepares a joint restricted frequency list (JRFL) for approval by the J-3.
3. Periodically updates and distributes the JRFL, as necessitated by changes in the task organization, geography, and joint communications-electronics operation instructions and by transition through operational phases.
4. Provides administrative and technical support for military spectrum use.
5. Exercises frequency allotment and assignment authority. This may be delegated to facilitate decentralization and to provide components with the maximum latitude and flexibility in support of combat operations.
6. Establishes and maintains the common database necessary for planning, coordinating, and controlling spectrum use. This database should contain spectrum-use information on all emitters and receivers (critical, friendly, military and civilian, available enemy, and neutral) as appropriate for the area of responsibility involved.
7. Analyzes and evaluates potential spectrum-use conflicts.
8. Assists and coordinates the resolution of spectrum-use conflicts.
9. In accordance with J-5 guidance, coordinates military spectrum use with the combatant command JFMO and the spectrum authorities of the United Nations or host nations involved.
10. Receives, reports on, analyzes, and attempts to resolve incidents of unacceptable electromagnetic interference; refers incidents that cannot be resolved to the next higher spectrum management authority.

Legend

J-2	intelligence directorate of a joint staff	J-5	plans directorate of a joint staff
J-3	operations directorate of a joint staff	J-6	communications system directorate of a joint staff

Figure III-1. Joint Frequency Management Office Spectrum Management Process

detonation means for improvised explosive devices (IEDs), and the denial of GPS information. The EW planner should be able to adapt to these new and creative uses and retain the flexibility to adjust to the adversary's next innovation.

d. **EW Reprogramming.** The purpose of EW reprogramming is **to maintain or enhance the effectiveness of EW and TSS equipment.** EW reprogramming includes

changes to self-defense systems, offensive weapons systems, ES, and intelligence collection systems. The reprogramming of EW and TSS equipment is the responsibility of each Service or organization through its respective EW reprogramming support programs. The swift identification and resolution of reprogramming efforts could become a matter of life and death in a rapidly evolving, congested, and contested EMOE. Service reprogramming efforts must include coordination from the JCEWS to ensure those reprogramming requirements are identified, processed, deconflicted, and implemented in a timely manner by all affected friendly forces.

For more information on EW reprogramming, refer to Appendix E, "Electronic Warfare Reprogramming."

e. **Electronic Masking**

(1) Electronic masking is the **controlled radiation of EM energy on friendly frequencies** in a manner to protect the emissions of friendly communications and electronic systems against adversary ES and SIGINT without significantly degrading the operation of friendly systems. Electronic masking is used to **disguise, distort, or manipulate friendly EM radiation data** to conceal military operations information and/or present false perceptions to adversary commanders. Electronic masking is an **important component to a variety of military functions** (e.g., MILDEC, OPSEC, and signals security) conducted wholly, or in part, within the EMS.

(2) Effective electronic masking of joint military operations involves the proactive management of all friendly radiated EM signatures of equipment being used in, or supporting, the operation. The **degree of masking required** in the management of these signatures is a function of the:

(a) Assessed adversary ES and SIGINT collection capability (or access to third party collection).

(b) Degree to which the EM signature of joint forces must be masked in order to accomplish the assigned mission.

(3) JFCs have **two primary responsibilities** with respect to electronic masking:

(a) Provide adequate electronic masking guidance to component commands through campaign plans, contingency plans, and OPORDs.

(b) Plan and implement appropriate electronic masking measures within the joint force HQ.

(4) To accomplish these responsibilities, the **following steps should be taken early** in the planning process:

(a) Assess adversary ES and SIGINT capabilities against friendly forces.

(b) Determine whether the mission assigned to joint forces may require electronic masking and, if so, to what degree.

(c) Request staff augmentation if necessary to acquire expertise in planning and implementing electronic masking TTP.

(d) Alert component commands at the earliest opportunity of the need to be prepared to implement electronic masking measures. This will afford them the necessary lead time to augment their forces with the necessary resources and expertise.

f. **Interoperability.** Interoperability is essential in order to use EW effectively as an element of joint military power. The major requirements of interoperability are to:

(1) **Establish standards and practice procedures** that allow for integrated planning and execution of EW operations.

(2) **Exchange EW information in a timely and routine fashion.** This exchange may be conducted in either non real time or near real time via common, secure, jam-resistant radios and data links. The ability to **exchange near-real-time data (such as targeting information) to enhance situational awareness and combat coordination** between various force elements is a critical combat requirement. This exchange of data relates to EA, EP, and ES, including friendly and adversary force data. Routine exchange of data among joint force components, the joint force and supporting commands and organizations, and, when possible, allies and coalition partners greatly facilitates all types of EW planning.

g. **Rules of Engagement.** EW activities frequently involve a unique set of complex issues. There are DOD directives and instructions, laws, rules, LOAC, and theater ROE that may affect EW activities. These laws, rules, and guidelines become especially critical during peacetime operations when international and domestic laws, treaty provisions, and political agreements may affect mission planning and execution. Commanders should seek legal review during all levels of EW planning and execution, to include development of theater ROE. This can best be accomplished by ensuring the legal advisor is available to EWC planners. While ROE should be considered during the planning process, they should not inhibit developing a plan that employs available capabilities to their maximum potential. If, during the planning process, an ROE-induced restriction is identified, planners should work with staff legal advisors to clarify the ROE or develop supplemental ROE applicable to EW.

h. **Unintended Consequences.** EW planners must coordinate EW efforts at the JFC level to minimize unintended consequences, collateral damage, and collateral effects. **Friendly EA could potentially deny essential services to a local population that, in turn, could result in loss of life and/or political ramifications.** The JFMO or JSME has an automated tool that can analyze the potential for interference of EW operations on friendly EMS-dependent systems. They should coordinate military EMS use with HN EMS authorities when conducting multinational operations or exercises. Due to the dual civil-military nature of GPS/GNSS and other PNT services, potential impacts from NAVWAR efforts on nonmilitary users and the civil/commercial critical infrastructure must be thoroughly analyzed during COA development and coordinated with HN EMS authorities.

The J-6 spectrum manager can provide this analysis to the JCEWS/joint EWC to better determine the impact of EW operations.

i. **Meteorological and Oceanographic Considerations.** EW planners must consider the effects of atmospherics and space weather on available EW systems, both friendly and adversary. The various types of atmospheric conditions and phenomena can positively or negatively affect EW systems. For example, atmospheric inversions can propagate radio transmissions; high humidity and rainy climates are detrimental to IR systems; and ionospheric scintillation can adversely affect GPS. Some atmospheric effects are well known and are categorized by season and location. Planners should consult with the combatant command METOC officer to determine the type of METOC support available for their operation.

j. **Chemical, Biological, Radiological, and Nuclear Considerations.** In a CBRN-threat environment, EW planners should consider the potential effects of a CBRN attack on sensitive EW equipment. Chemical contaminants and most decontamination solutions are corrosive and may damage sensitive equipment. Additionally, systems' operations may be impeded if operators are required to wear CBRN-protective ensembles. Redundancy, dispersal, protection, and decontamination of mission-critical EW equipment will help ensure mission continuation following CBRN attack.

For additional guidance, see JP 3-11, Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments.

3. Joint Electronic Warfare Planning Process

In order to be fully integrated into other aspects of a planned operation, the EWC conducts joint EW planning beginning as early as possible and coordinates it with other aspects of the plan throughout the joint operation planning process (JOPP). Figure III-2 shows the integration of EW into the JOPP. Thorough EW planning will minimize EMS conflicts and enhance EW effectiveness during execution. Proper EW planning requires understanding of the joint planning and decision-making processes; nature of time-constrained operations; potential contributions of EW; and employment of joint EW. During execution, EW planners must **monitor the plan's progress** and be prepared to make modifications to the plan as the dynamics of the operation evolve. Joint EW planners should take the following actions during the planning process to **integrate EW into the joint plan:**

a. Determine the type, expected length, geographic location, and level of hostility expected during the operation to be planned.

b. Review the scale of anticipated operations and the number and type of friendly forces (to include allied and coalition partners) expected to participate.

c. Review current ROE and existing authorities for EW activities and recommend any necessary modifications in accordance with current staff procedures. Coordinate with the staff judge advocate to ensure requirements of ROE, legal authorities, and LOAC are met.

Electronic Warfare Cell Actions and Outcomes as Part of Joint Planning

Planning Process Steps	Electronic Warfare (EW) Cell Planning Action	EW Cell Planning Outcome
Planning Initiation	• Monitor situation. • Review guidance and estimates. • Convene EW cell. • Ensure EW representation within information operations (IO) cell. • Gauge initial scope of the EW role. • Identify organizational coordination requirements. • Initiate identification of information required for mission analysis and course of action (COA) development. • Validate, initiate, and revise priority intelligence requirements (PIRs) and requests for information (RFIs). • Recommend EW strategies and conflict resolution.	Request taskings to collect required information.
Mission Analysis	• Identify specified, implied, and essential EW tasks. • Identify assumptions, constraints, and restraints relevant to EW. • Identify EW planning support requirements (including augmentation) and issue requests for support. • Initiate development of measures of effectiveness and measures of performance. • Analyze EW capabilities available and identify authority for deployment and employment. • Obtain relevant physical, informational, and cognitive properties of the information environment from the IO cell. • Refine proposed PIRs/RFIs. • Provide EW perspective in the development of restated mission for commander's approval. • Tailor augmentation requests to missions and tasks.	List of EW tasks. List of assumptions, constraints, and restraints. Planning guidance for EW. EW augmentation request. EW portion of the commander's restated mission statement.
COA Development	• Select EW supporting and related capabilities to accomplish EW tasks for each COA. • Revise EW portion of COA to develop staff estimate. • Provide results of risk analysis for each COA.	List of objectives to effects to EW tasks to EW capabilities for each COA.
COA Analysis and Wargaming	• Analyze each COA from an EW functional perspective. • Identify key EW decision points. • Recommend EW task organization adjustments. • Provide EW data for synchronization matrix. • Identify EW portions of branches and sequels. • Identify possible high-value targets related to EW. • Recommend EW commander's critical information requirements.	EW data for overall synchronization matrix. EW portion of branches and sequels. List of high-value targets related to EW.
COA Comparison	• Compare each COA based on mission and EW tasks. • Compare each COA in relation to EW requirements versus available EW resources. • Prioritize COAs from an EW perspective.	Prioritized COAs from an EW perspective with pros and cons for each COA.
COA Approval	• No significant EW staff actions during COA approval.	Not applicable.
Plan or Order	• Refine EW tasks from the approved COA. • Identify EW capability shortfalls and recommended solutions. • Update continually all supporting organizations regarding details of the EW portion of plan details (access permitting). • Advise supported combatant commander on EW issues and concerns during supporting plan review and approval. • Participate in time-phased force and deployment data (TPFDD) refinement to ensure the EW force flow supports the concept of operations.	Updated EW estimates based on selected COA. Draft EW appendices and tabs, supporting plans. EW requirements to TPFDD development. Synchronized and integrated EW portion of operation plan.

Figure III-2. Electronic Warfare Cell Actions and Outcomes as Part of Joint Planning

d. Review, with the NETOPS community, the contribution EW can make to protect the EMS for use by the DOD information networks. This should be done through the J-6 representative assigned to the JCEWS or EWC staff.

e. Review, with other planners, the contribution EW can make to efforts in other mission areas (e.g., military information support operations [MISO], MILDEC, and CNO) and determine the level of EW platform support they expect to need during the operation.

f. Review the role EW capabilities can play in creating NAVWAR effects and determine the level of EW platform support they expect to need during the operation.

g. Review, with intelligence planners, the type of ES platforms, capabilities, and products available to support the operation. IGL analysis of EW actions should start early and be frequently reviewed during the planning and execution phases of an operation.

h. Consult with Service, functional component, and multinational EW planners, wherever the most current and relevant expertise in the employment of EW capabilities resides, in order to understand and remain current on the full range of EW capabilities available for accomplishing operational objectives.

i. Work in concert with J-6 EMS managers to improve awareness and deconflict all military, civilian, and other systems (e.g., communication systems, sensors, and EMS-dependent weapon systems) that could impact the EMOE.

j. Determine the number and type of EW platforms that could reasonably be expected to be tasked to support the joint operation being planned. Consult automated force status reports (e.g., those provided through the Defense Readiness Reporting System for US forces) for this information. Service and functional components and multinational planners should be consulted to augment automated information.

k. Review, with component air planners, the requirement for EW support to the SEAD effort.

l. Recommend, to the EWC director (or other designated member of the J-3 or J-5 staff), the type and number of EW assets to be requested from component or supporting commands for the operation being planned.

m. Estimate the size and expertise of the EW staff required to plan and coordinate execution of the EW portion of the plan. Consult with Service, functional component, and multinational EW planners to refine these estimates.

n. Recommend how best to effectively prosecute EW operations to create NAVWAR effects and maintain a PNT advantage. Estimate the impact of NAVWAR effects on both military objectives and civil/commercial users.

o. Recommend staff augmentation in accordance with staff procedures from component, supporting, and multinational forces (MNFs) as necessary to assemble the staff required to conduct EW planning.

p. Coordinate with the combatant command JFMO or JSME early in the planning process to determine if JSC assistance is required.

q. During crisis action planning, evaluate each COA considered with respect to EW resources required and the EW opportunities and vulnerabilities inherent in the COA.

r. Integrate EW into joint targeting.

4. Electronic Warfare Planning Guidance

a. Planning guidance for EW is **included as tab D (EW) to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN.**

Appendix A, "Electronic Warfare Guidance," shows the format of Joint Operation Planning and Execution System EW guidance as a tab to the IO guidance. For more information on OPLAN development, refer to CJCSM 3122.03C, Joint Operation Planning and Execution System, Volume II, Planning Formats.

b. **Planning Factors.** Development of the EW portion of the OPLAN requires consideration of a number of diverse factors about the proposed operations. These **planning factors** include, but are not limited to, the following:

(1) Identify the purpose and intent of performing EW operations, the immediate desired effects, and enabling characteristics for authorizing EW.

(2) Determination of status of EW capability of available forces relative to enemy capability, to determine if sufficient assets are available to perform the identified EW tasks. If in-place assets are insufficient, requests for support should be drafted.

(3) Determination of requirements for friendly communications nets, EM navigation systems, and radar. These requirements should be considered with respect to the anticipated operations, tactical threat expected, and EMI possibilities. Once identified, these requirements should be entered into the JRFL under appropriate categories (e.g., TABOO).

(4) Identification of measures necessary to deny OPSEC indicators to enemy passive-EM sensors.

(5) Determination of the coordination and processes that will be necessary when conducting EA in order to ensure continued effective ES. Development of the JRFL is a critical preliminary step to integrate EA and ES activities.

(6) Coordination and identification of specific resources required for interference resolution.

(7) Identification of commander's critical information requirements (CCIRs) that support EW operations. These CCIRs must be included as priority intelligence requirements in the intelligence annex (normally annex B) of the OPLAN to facilitate generation of ES.

(8) Coordination and establishment of procedures to ensure timely fulfillment of EW planning tasks, including tactical real-time dissemination.

(9) Review of ROE and applicable law to determine the authorities needed or the restrictions, if any, that apply to EW operations.

(10) Identification of EM target categories in order to guide collections priorities and support EM target development.

c. **EW plans should:**

(1) **Identify the desired EM profile** selected by the commander for the basic CONOPS and **provide EMCON guidance** to commanders so the desired EM profile is realized.

(2) Identify EW missions and tasks to Service or functional component commanders to enable them to plan for the resources required and conduct the pre-coordination necessary to deploy and employ those resources in foreign countries.

(3) **Evaluate adversary threats** to weapons systems, critical C2 communications, weapons control systems, target acquisition systems, surveillance systems, PNT systems, and computer networks. Specify EP guidance necessary to ensure effective operations.

(4) Reflect the guidance, policies, and EW employment authorities provided within instructions, regulations, or orders.

5. Electronic Warfare Planning Aids

There are a number of **automated planning tools** available to help joint EW planners carry out their responsibilities. These tools can be divided into three broad categories: **databases, planning process aids, and spatial and propagation modeling tools.**

a. **Databases.** Databases can assist EW planners by **providing easy access to a wide variety of platform-specific technical data** used in assessing the EW threat and planning appropriate friendly responses to that threat. However, planners should keep **several considerations** in mind when relying on automated data. There are two major categories for EW databases—intelligence and operational. Intelligence databases are repositories of intelligence information. They are not all-inclusive. They represent limited technical information on the capabilities, specifications, and parameters of known systems. Operational databases are complete databases required to operate models used in decision-making software such as mission planning systems. Operational databases must be complete so that operations can be conducted effectively. Engineer analysts use system knowledge, model requirements, and intent to ensure operational databases have all the necessary elements, in a form and function suitable, for operational use.

(1) There are a **large number of databases** available to military planners. The primary approved source for threat system data are DIA responsible producers: NASIC, Missile and Space Intelligence Center (MSIC), NGIC, and the 53rd Electronic Warfare Group (EWG). The Electronic Warfare Integrated Reprogramming Database is a DIA-managed database, maintained and distributed by NASIC as the executive agent. It is the primary DOD-approved source for technical parametric and performance data on non-

communications emitters and associated systems. Additionally, the ESAC at Fort Meade, MD, provides tactical and operational-level warfighters with fused, operational analysis of the various databases available. MSIC, NGIC, and the 53rd EWG are the source for early warning radars, surface-to-air missile systems, communication systems, and blue systems. These databases are maintained by the Services and other intelligence agencies. Information from other agencies, DOD organizations, allied organizations, and open sources used to prepare databases used for operations form the core intelligence databases. The compilation of accurate technical data into one place could be a lucrative target for hostile intelligence collection. For this reason, **access to friendly force data may be highly restricted** and harder for planners to obtain than threat data, which can be accessed through normal intelligence channels.

(2) The **level of detail, specific fields, and frequency of update** may vary widely across different databases dealing with the same data. The way data is organized into fields in a database and the level of detail (e.g., number of decimal places for certain technical data) depend on what the data is used for, the cost associated with data acquisition and compilation, and database maintenance.

(3) The sources of data being used for planning should be a topic of coordination among EW planners. The use of ESAC's Electromagnetic-Space (E-Space) portal as the common database source is recommended. Joint planners should understand the sources of **data being used for specific EW planning purposes and ensure those sources are current and relevant to the planned operation(s).** When planning specific operations, planners should coordinate with organizations that maintain important sources of EW data to ensure the data is current and suitable for the operation. Planners should be cautioned about using unofficial sources of data, particularly those available through the Internet that may be subject to manipulation by organizations hostile to US policies and objectives. However, **open-source intelligence** remains a viable and potentially important source of valuable information.

b. **Planning Process Aids.** There are **several automated aids** available that assist in the planning process, and others are under development. These include aids that **automate OPLAN development and automated frequency management tools.** Use of automated tools to consider disparate mission area requirements with respect to EW effects and capability employment will normally be determined by the EWC director and the director's planning staff. EW planners should ensure that any EW planning input developed separately from such systems is created in a format compatible with, and electronically transferable to, the designated planning tools. EW planning input from subordinate and supporting commands should follow the desired format.

c. **Spatial and Propagation Modeling Tools. Geographic information systems enable analysis and display of geographically referenced information. These spatial modeling tools can, for example, enhance targeting, awareness, and planning for GPS denied environments, and facilitate trends analysis.** The variables that affect the propagation of EM energy are known and **subject to mathematical predictability.** The use of propagation modeling tools **that graphically display transmission paths** of EM energy has become widespread in EW planning. However, the accuracy, speed, and flexibility of

these tools depend greatly on the accuracy of the data provided to the tool and the sophistication of the software and hardware used to manipulate the data. These tools are essentially **models for EM propagation.** The accuracy and sophistication of the software and hardware being used may not be determined from the graphics display alone. **EW planners should have an understanding of how such modeling systems are computing the graphics being displayed.** Such an understanding, combined with operational experience, is the basis on which planners judge the strengths and weaknesses of different modeling tools and determine what is, and is not, an appropriate use of such systems.

For more information on EW models and their use, refer to Appendix F, "Electronic Warfare Modeling."

d. **Reachback Resources.** If EW planners don't have the automated planning tools required on-site, reachback support is available. For joint EW planners, reachback support is available from organizations such as the ESAC; the USSTRATCOM/JEWC in San Antonio, Texas; and the JSC in Annapolis, Maryland. Support for NAVWAR and GPS is available from the Joint Navigation Warfare Center (JNWC) at Kirtland Air Force Base (AFB), New Mexico, and the Global Positioning System Operations Center (GPSOC) at Schriever AFB, Colorado, respectively. Additional resources include Army Reprogramming Analysis Team; NGIC in Charlottesville, Virginia; NSA-Electronic Intelligence; Joint Improvised Explosive Device Defeat Organization; Joint Warfare Analysis Center in Dahlgren, Virginia; and the IO Range.

For more information on the ESAC, GPSOC, JEWC, JNWC, JSC, and IO Range, refer to Appendix B, "Organizations Supporting Joint Electronic Warfare."

CHAPTER IV
COORDINATING JOINT ELECTRONIC WARFARE

"In the case of electronic warfare, as in any other kind of warfare, no weapon and no method is sufficient on its own."

Martin van Creveld
***Technology and War,* 1989**

1. Introduction

Once a plan has been approved and an operation has commenced, the preponderance of EW staff effort shifts to EMBM. **EMBM includes continuous monitoring of the EMOE, EMS management, and the dynamic reallocation of EW assets based on emerging operational issues.** Normally, this monitoring is performed by personnel on watch in the joint operations center (JOC). These watch personnel, stationed at a dedicated EW watch station, normally are tasked to alert other EW or staff personnel to carry out specific coordinating actions in response to emerging requirements. This chapter discusses the actions and concerns the EW staff personnel should focus on to accomplish such coordination.

2. Joint Electronic Warfare Coordination and Control

a. **Joint EW Organizational Coordination.** At combatant commands and subordinate unified commands, the J-3 is primarily responsible for the EW coordination function. The EW division of the J-3 staff should engage in the full range of EW functions to include deliberate planning; day-to-day planning and monitoring of routine theater EW activities in conjunction with the combatant command's theater campaign plan; and crisis action planning in preparation for EW as part of emergent joint operations. The EW division operates under the direction of the J-3 directorate and coordinates closely with other staff sections and JPGs, as required. In the very early stages of contingencies, the JCEWS should assess staffing requirements for planning and execution and should coordinate EW planning and COA development with the JFC's components. Subordinate and supporting commands should begin EW planning and activate their EWEs per CCDR or Service guidelines. When the scope of the contingency becomes clearer, the command EWO may request that the JFC stand up a joint EWC. The designated joint EWC would request additional augmentation from JFC components to form a representative and responsive EW planning and execution organization. To avoid confusion with the joint EWC (organizationally located with the JFC staff), component EW support cells are referred to as EWEs.

b. **Management of the Electromagnetic Spectrum**

(1) The J-6/J-2 pre-assessment of the EMOE—conducted during the planning phase—constitutes a best analysis based on information available at the time. Following deployment and buildup, overlaying joint force EM emissions on the existing EMOE will create a different environment. Further, this environment will constantly change as forces redeploy and C2, surveillance, weapon systems, and other spectrum-use applications realign.

Since EW is concerned with **attacking personnel, facilities, or equipment (EA); protecting capabilities and EMS access (EP); and monitoring, exploiting, and targeting use of the EMS (ES),** EW staff personnel have a role in the **dynamic management** of the EMS, via tools and processes, during operations. A **comprehensive and well-thought-out JRFL and EMCON plan** are two significant tools that **permit flexibility of EW actions** during an operation without compromising friendly EMS use. Some of the **coordination actions related to the EMS** that EW staff personnel should consider include:

(a) Monitoring compliance with the JRFL and EMCON plan by friendly EW assets, as well as remediating joint spectrum interference resolution (JSIR) events.

(b) Recommending changes to operations in the EMS based on emerging frequency deconfliction requirements.

(c) Establishing employment guidance consistent with standing ROE issued by the Chairman of the Joint Chiefs of Staff, theater-specific ROE issued by the GCC, and any mission-specific ROE issued by the Secretary of Defense (SecDef), CCDR, or JFC. Recommend supplemental ROE for EA employment as necessary.

(d) Coordinating a plan to ensure terrestrial and non-terrestrial communications net availability in the presence of EMI.

(e) Implementing a responsive plan for executing EWCA responsibilities in order to ensure operationally effective coordination, employment, targeting, and deconfliction of EA, ES, ISR, space, cyberspace, C2, and communications activities.

(f) Coordinating and deconflicting NAVWAR-related PNT EA/ES efforts. NAVWAR is a continuous effort within the EWC.

(g) Establishing and training staff on the EA request process to facilitate identification of spectrum use conflicts prior to execution of the EA.

For more information of EW frequency deconfliction, refer to Appendix D, "Electronic Warfare Frequency Deconfliction Procedures."

(2) **Electronic Warfare Control Authority.** The EWCA, the senior EA authority in the OA, develops guidance for performing EA on behalf of the JFC. EWCA can either be retained by the JFC or executed by the JFC's designated representative. Routine execution of EWCA responsibilities will normally be delegated to the staff EWO or EWC director (when an EWC is activated), and may be temporarily delegated to field units for the purpose of local/tactical mission refinement and CEASE BUZZER (an unclassified term to terminate EA activities, including the use of EW expendables) remediation. EWCA responsibilities include:

(a) Participating in JRFL development.

(b) Ensuring compliance with the approved JRFL.

(c) Gaining and maintaining situational awareness of all EA-capable systems in the OA.

(d) Acting as the JFC's executive agent for decisions on EW IGL recommendations.

(e) Coordinating introduction of new EMS-dependent systems in the OA.

(f) Coordinating with joint force components on EA requirements.

(g) Investigating and implementing corrective measures to unauthorized EA events.

(h) Contributing to the development of EA narratives in EW associated directives/guidance.

c. **Coordination Between the Divisions of EW.** There are a number of **coordinating actions that must occur** among the respective divisions of EW (EA, EP, and ES) during an operation. These actions include monitoring:

(1) The employment and effective integration of ES assets and the timely flow of ES information relevant to EA and EP to units responsible for those missions and coordinating corrective measures, as required. The deconfliction, coordination, integration, and synchronization of ES assets will normally require intensive, proactive action by the EWC director as some of these assets are controlled through SIGINT/ISR channels and organizations.

(2) Component input to the reprogramming process and coordinating urgent reprogramming actions based on recommendations from Service reprogramming centers.

(3) The interference resolution process for employment of EP, EA, and ES capabilities first requires that personnel operating an affected system recognize the problem as interference and begin the proper EP actions (e.g., WARM, reporting). If those actions cannot resolve the problem, they will need to request that EA assets cease EA activities that may be impacting their operations. If that does not resolve the problem, ES assets will need to determine the source of interference.

d. **Coordination with the IO Cell.** EW can support the IO LOO/LOE and enable or enhance other LOOs/LOEs. EW is viable in all military operations; therefore, integration of EW expertise in planning is important to creating synergistic effects to support the JFC's objectives.

(1) EA can create decisive, enhanced effects in the information environment and provide the JFC an operational advantage by gaining and maintaining information superiority. Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

(2) EW and its divisions enable operations in the air, land, maritime, and space physical domains and the information environment (which includes cyberspace). The nature of EW and its unique relationship to the EMS allow creation of effects that have implications throughout the OA and require planners to coordinate EW efforts in order to minimize unintended consequences, collateral damage, and collateral effects. When EW is employed as nonlethal fires, it often can be employed with little or no associated physical destruction. Fires must be deconflicted at the JFC level, through the JTCB or like body, to predict collateral damage and/or effects and incorporate risk mitigation strategies.

(3) One of the primary functions of the IO cell is to coordinate disparate military activities in order to produce optimized effects. Nearly all information-related capabilities depend on, use, or exploit the EMS for at least some of their functions. Deconfliction and coordination of EW in an operation is a continuous process and a constant consideration in IO planning efforts. Specific discussion on EW's relationship to other information-related capabilities is listed below.

For more information on IO, refer to JP 3-13, Information Operations.

(a) **Electronic Warfare and Military Information Support Operations.** MISO activities often use the EMS to broadcast their message to target audiences using platforms such as COMMANDO SOLO. EW activities support MISO by providing the means to deliver a message to a target audience via the EMS. EW planners must be aware of the potential to interfere with MISO efforts to convey information to adversaries or foreign target audiences. MISO supports EW by broadcasting products on target frequencies and by developing products for broadcast on other EW assets. MISO platforms and units depend on information gathered through ES to **warn them of potential threats and provide feedback about reaction** to MISO broadcasts and other activities. MISO units rely on effective EP efforts to prevent adversary EA activities or other inadvertent EMI from disrupting their efforts. Coordination of MISO and EW planned frequency use when developing the JRFL is the first step in deconflicting these two capabilities. During the execution phase of an operation, MISO and EW staff personnel should integrate their operations and frequency use on a regular basis.

For more information on MISO, refer to JP 3-13.2, Military Information Support Operations.

(b) **Electronic Warfare and Operations Security.** EA supports OPSEC by degrading adversary EM ISR operations against protected units and activities. ES can support the OPSEC effort by providing information about adversary capabilities and intent to collect intelligence **on friendly forces** through the EMS. ES can also be used to evaluate the effectiveness of friendly force EMCON measures and recommend modifications or improvements. An **effective and disciplined EMCON plan and other appropriate EP measures** are important aspects of good OPSEC. OPSEC supports EW by concealing EW units and systems to deny information on the extent of EW capabilities. During operations, OPSEC planners and EW staff personnel should frequently review the JFC's critical information requirements in light of the dynamics of the operation. Adjustments should be recommended to ES collection efforts, EMCON posture, and other EP measures as necessary to maintain effective OPSEC.

For more information on OPSEC, refer to JP 3-13.3, Operations Security.

(c) **Electronic Warfare and Military Deception.** EW supports MILDEC by using EA/ES as deception measures; degrading adversary capabilities to see, report, and process competing observables; and providing the enemy with information received by electronic means that is prone to misinterpretation. Knowledge of MILDEC plans and actions is normally very restricted. Designated EW planners must work through the J-3 staff for deconfliction and EW support to MILDEC operations. MILDEC frequently relies on the EMS to convey the deception to adversary intelligence or tactical sensors. Forces assigned to the deception effort are often electronically "enhanced" to project a larger or different force structure to adversary sensors. Friendly EA assets may be an integral part of the deception effort by selectively jamming, interfering, or masking the EM profile of the main operational effort. Friendly assets can also be used to stimulate air defense systems (communications and radar) through either EM or physical means. Stimulation of an air defense system enables the ability to target or map the EOB, causes the adversary to commit assets (air or ground), as well as mission deception and saturation of the defense system. At the same time, coordination within the JTF staff must occur so EA activities do not interfere with frequencies being used to convey the EM aspects of the deception to adversary sensors. Disciplined EMCON and other appropriate EP efforts, by both deception assets and those of the main effort, are essential to preventing the adversary from distinguishing deception activities from the main effort. ES assets can provide immediate warning to deception forces about adversary forces reacting to their presence or actions. ES assets are also an important means to determine that the adversary is capable of receiving the EM aspects of a deception. Since deception forces are often positioned "off axis" from the main effort, ES platforms positioned with the deception effort may assist in location of adversary forces by assisting with triangulation in DF activities. Designated EW staff personnel should have the security clearances and access necessary to work with MILDEC planners during the planning and execution phases of an operation that involves deception. MILDEC supports EW by influencing an adversary to underestimate friendly EA/ES capabilities. EW planners should ensure that EM frequencies necessary to support deception plans are accounted for in EMS management databases and on the JRFL without disclosing that specific frequencies are related to deception. During the execution of an operation, EW staff personnel should monitor EW support to the deception effort and coordinate any changes or conflicts in a timely manner.

For more information on MILDEC, refer to JP 3-13.4, Military Deception.

(d) **Electronic Warfare and Cyberspace Operations.** Cyberspace operations may be facilitated and enabled through EW, and vice versa. The increasing prevalence of wireless Internet and telephone networks in the OE has created a wide range of opportunities and vulnerabilities when EW and cyberspace operations TTP are used synergistically. While wired access to a particular computer network may be limited, EM access may prove the key to successful computer system penetrations. For example, use of an airborne weapons system to deliver malicious code into cyberspace via a wireless aperture would be characterized as "EW-delivered computer network attack (CNA)." The EMS can also be used as a vector for conveying an attack directly against the information technology infrastructures. For example, a computer server can be physically damaged or destroyed by

EM nonlethal fires (e.g., HPM or EMP weapons). EW operations (EA and ES) and attributes (EP) can assist in setting the conditions in cyberspace to ensure availability of the area requiring access, provide the ability to engage adversaries decisively, and conduct cyberspace operations to enable the creation of the desired effects in the physical domains (i.e., air, land, maritime, and space).

(e) **Electronic Warfare and Information Assurance (IA).** IA is concerned with measures that protect and defend information and information systems, and many of the measures involve the use of the EMS. EP equipment, attributes, and processes assist in assuring the availability and integrity of modulated data traversing the EMOE, whose usability and availability IA seeks to protect and defend. EA TTP assist in compromising those same qualities which adversary IA seeks to protect and defend. EMI resolution and EMS management procedures assist IA in overcoming the problem of EM fratricide.

(f) **Electronic Warfare and Physical Attack.** EW supports physical attack by providing target acquisition through ES and by destroying or degrading susceptible assets with EA. EP supports physical attack by protecting friendly targeting sensors, navigation, and communications in a contested environment. Physical attack supports EW by destroying adversary C2 targets and EMS-dependent systems. "Precision strike" is an increasingly important aspect of physical destruction actions in joint operations. EW is an important part of precision strike. Frequency management and deconfliction must account for frequencies used by various types of precision strike weapons. ES assets are an important part of efforts to dynamically map the EMOE for targeting and threat avoidance planning. Standoff munitions and anti-radiation ordnance are major assets in any operation and may, for example, be used to selectively destroy adversary emitters in support of MILDEC, SEAD, OPSEC, and MISO efforts. The employment of weapons must be carefully planned and deconflicted to prevent the engagement of unintended targets and potential fratricide. EA assets perform vital screening functions (including the use of standoff weapons) for friendly air strikes and other combat units on the ground and at sea. EA also plays an important role in defeating hostile air strikes and countering precision strike weapons. Disciplined EMCON and other EP measures are also an important part of protecting friendly air strikes and front line tactical units on the ground and at sea. EMCON and other EP measures also protect friendly forces handling or operating around live ordnance during combat operations by preventing inadvertent detonations due to hazards of EM radiation to ordnance. ES assets provide timely warning of adversary reaction to friendly air strike and other physical destruction actions that take friendly forces into hostile territory or contact with adversary combat forces. ES also performs an important combat assessment role by providing feedback about the results of friendly physical attack actions that can be obtained through SIGINT or changes in the EME. ES can also be used to evaluate the effectiveness of friendly force EMCON measures and recommend modifications or improvements. All of these factors require that joint EW staff personnel actively work with air planners, fire support personnel, and other staff personnel involved in coordinating physical destruction actions during combat operations.

For more information, refer to JP 3-09, Joint Fire Support, *and JP 3-60,* Joint Targeting.

(g) **Electronic Warfare and Physical Security.** EW supports physical security by using EP to safeguard communications used in protecting facilities. Additionally, EP features may guard personnel, facilities, and equipment from the broader effects (both intended and unintended) of EM energy. Physical security supports EW by safeguarding equipment used in EW. In an era when IEDs with radio-controlled electronic detonators have become ubiquitous, EW and physical security form one of the new, closely intertwined relationships in the EMS. EW capabilities can be used to preempt and disrupt threats that may be using part of the EMS to attack joint ground forces.

(h) **Electronic Warfare and Counterintelligence (CI).** There are many electronic aspects to CI. ES platforms, on occasion, might be called on to help monitor some aspect of CI operations in overseas locations. Frequencies used for CI operations in foreign locations should be coordinated through the JRFL. Close coordination through the J-3 EW and J-2 CI staff divisions should establish a battle rhythm and/or TTP to monitor and deconflict JRFL and other EW activities that either support or potentially jeopardize human intelligence activities.

(i) **Electronic Warfare and Combat Camera (COMCAM).** EW involves some of the most technologically sophisticated and innovative aspects of joint operations. Affording COMCAM the opportunity to capture photographs and film of EW units in action can help to convey, to domestic and foreign audiences, the technological sophistication and power of US forces, but may also divulge key operations characteristics, limitations, and vulnerabilities to adversaries, and thus should be carefully controlled.

(j) **Electronic Warfare and Public Affairs (PA).** The relationship of EW to PA is primarily one of deconfliction. News media personnel in the OA use a variety of electronic recording and transmitting devices to carry out their assignments. It is important that their equipment and operating frequencies are accounted for in the JRFL to enable deconfliction and identify potential fratricidal interference between news media equipment and friendly force military equipment.

For more information on PA, refer to JP 3-61, Public Affairs.

(k) **Electronic Warfare and Civil-Military Operations (CMO).** In support operations such as humanitarian operations, EW assets may be used to map the EMS and broadcast civil defense information similar to the way they have been used successfully to broadcast MISO messages. In all operations, CMO frequencies should be included on the JRFL to ensure deconfliction with EW assets' activities. As requirements for EW assets expand into peacetime contingency roles, it becomes more imperative that planners consider diplomatic clearance requirements of HNs as early as possible.

For more information on CMO, refer to JP 3-57, Civil-Military Operations.

(l) **Electronic Warfare and Defense Support to Public Diplomacy (DSPD).** EW support and deconfliction with DSPD parallels EW support and deconfliction with MISO.

e. **Electronic Warfare and Legal Support.** Legal review is required to ensure EW operations are in compliance with existing DOD directives and instructions, ROE, and applicable domestic and international law, including LOAC.

For more information, refer to JP 1-04, Legal Support to Military Operations.

f. **Exploitation of Captured Equipment and Personnel.** Exploitation of adversary equipment can verify adversary electronic equipment capabilities, to include WARM. This information can lead to the testing or verification of friendly EW equipment or begin the process of EW reprogramming to counter new adversary capabilities. Exploitation of captured adversary personnel can lead to discoveries of adversary capabilities, tactics, and procedures against friendly EW capabilities. Information gleaned through the interrogation of captured personnel may help EW planners **evaluate the effectiveness of friendly EW actions.** This information can also aid in **after-action report reconstruction** of EW. The joint captured materiel exploitation center and joint interrogation and debriefing center conduct exploitation of captured material and interrogation of captured personnel, respectively. The EW staff should establish EW exploitation and interrogation requirements, through the J-2, to take advantage of the opportunities that may be realized through exploitation of captured equipment and interrogation of captured personnel.

For more information, refer to JP 2-01, Joint and National Intelligence Support to Military Operations.

3. Service Component Coordination Procedures

a. Components requiring EW support from another component should be encouraged to **directly coordinate that support** when possible, informing joint EW planners of the results of such coordination, as appropriate. However, at the joint force level, EW planners should be familiar with how this coordination occurs across Service and functional component lines in order to be **prepared to assist and facilitate coordination** when necessary, or when requested. An overview of component EW coordination factors and procedures are provided in this section. When the JFC has chosen to conduct operations through functional components, the functional component commanders will determine how their components are organized and what procedures are used. EW planners should coordinate with the functional component EWEs to determine how they are organized and what procedures are being used by functional component forces.

b. **Army.** The Army Service component command (ASCC) or G-3 plans, coordinates, and integrates EW requirements in support of the JFC's objectives. At corps level, coordination with the G-3, the fire support coordination center or fire support element (FSE), and the communications systems staff officer is required. These requirements are translated into EW support requests and, where possible, are coordinated directly with the appropriate staff elements having EW staff responsibility within other component HQ. Conversely, other components requiring Army EW support initially coordinate those support requirements with the EW officer at the Army forces HQ or tactical operations center. This coordination is normally done in person or through operational channels when planning joint EW operations. However, the Global Command and Control System (GCCS) or Global

Command and Control System-Army (GCCS-A) may be used to **coordinate immediate requests for Army EW support.** In this case, other components will communicate their EW support requests via the GCCS or GCCS-A to the FSE and EW officer or to the EW section at ASCC, corps, or division level. Air Force and Army coordination will normally **flow through the battlefield coordination detachment** at the AOC. EW staffs at higher echelons monitor the EW requests and resolve conflicts, when necessary. The G-3 also:

(1) Provides an assessment of Army EW capabilities to the other component operation centers.

(2) Coordinates preplanned EW operations with other Service components.

(3) Updates preplanned EW operations in coordination with other components, as required.

(4) Coordinates with the intelligence staff officer to ensure an IGL analysis is conducted for potential EW targets.

(5) Coordinates and integrates cyberspace and EM activities.

c. **Marine Corps.** The MAGTF HQ **EWCC,** if established, or the MAGTF EWO, if there is no EWCC, is responsible for **coordination of the joint aspects of MAGTF EW requirements.** Requirements for other component EW support are established by the operations staff, in coordination with the aviation combat element, the ground combat element, and the combat logistics element of the MAGTF. These requirements are translated by the EWCC or EWO into tasks and coordinated with the other component EW staffs. In addition, the EWCC or EWO:

(1) Provides an assessment of Marine Corps forces' EW capabilities to other component operation centers to be used in planning MAGTF EW support to air, ground, and naval operations.

(2) Coordinates preplanned EW operations with appropriate component operation centers.

(3) Updates EW operations based on coordination with other component EW agencies.

(4) Coordinates with the intelligence staff officer to ensure that an IGL analysis is conducted for potential EW targets.

d. **Navy.** The Navy component commander is normally a numbered fleet commander within a theater. The Navy operations directorate is responsible for all Navy EW efforts and provides coordination and tasking to task forces assigned. The IWC at the carrier strike group or amphibious ready group-Marine expeditionary unit provides for execution at the tactical level. When naval task forces are operating as a component of a joint force, the IWC:

(1) Provides an assessment of Navy EW capabilities to the other component operation centers.

(2) Coordinates preplanned EW operations with appropriate component EW agencies.

See NTTP 3-51.1, Navy Electronic Warfare, *for a full list of IWC responsibilities to EW.*

NOTE: When employed in a strike support role, airborne EA and ES assets (e.g., EA-6B Prowler and EA-18G Growler) will be the responsibility of the strike warfare commander. The strike warfare commander is responsible for coordinating integration of air wing assets into the ATO with the JFACC.

e. **Air Force.** Air Force requirements for other component EW support are established through close coordination between the JFC's EWC and the **COMAFFOR's A-3** (or equivalent operations directorate) **or A-5** (or equivalent plans directorate), in coordination with the Director for Intelligence, A-2. Ideally, this coordination will involve the COMAFFOR's AOC and JFC's JOC. The JFC's EWC and A-3 or A-5 staff translate requirements for other component EW support into tasks and coordinate those tasks, through the EWC, with the component EWE. In addition, the A-3 or A-5 staff officer:

(1) Provides an assessment of Air Force capabilities to the joint EWC.

(2) Updates EW operations based on coordination with the joint EWC.

f. **Special Operations Forces.** The joint force special operations component commander will establish a JOC to serve as the task integration and planning center for joint force special operations. Requirements from special operations units for EW support will be transmitted to the joint force special operations component command JOC for coordination with the joint force special operations component command IO cell.

For more information, refer to JP 3-05, Special Operations.

g. **United States Coast Guard (USCG).** In peacetime, the USCG operates as part of the Department of Homeland Security (DHS). Upon the declaration of war or when the President directs, the USCG will operate as part of the DOD. During both peacetime and war, joint operations may include USCG assets that possess EW capabilities. Coordination with USCG assets should be through assigned USCG liaison personnel or operational procedures specified in the OPLAN or OPORD.

4. Electronic Warfare and Intelligence, Surveillance, and Reconnaissance Coordination

Detailed coordination is essential between the EW activities and the intelligence activities supporting an operation. A major portion of the intelligence effort, prior to and during an operation, relies on collection activities targeted against various parts of the EMS. ES depends on the **timely collection, processing, and reporting of various intelligence and combat information** to alert EW operators and other military activities about important

intelligence collected in the EMS. It is vital that all prudent measures are taken to **ensure EMS activities are closely and continuously deconflicted with ES** and intelligence collection activities. The J-2 must ensure that EW collection priorities and ES sensors are integrated into a **complete intelligence collection plan.** This plan ensures that use of scarce intelligence and ES collection assets is maximized in order to support all aspects of the JFC's objectives.

For more information, refer to JP 2-01, Joint and National Intelligence Support to Military Operations*, and its classified supplement.*

5. Electronic Warfare and Interagency Coordination

Although OPLANs and commander's intent are limited to military contexts, the desired effects, coordination required, and agencies affected within the EMOE extend beyond those contexts. The increasingly prolific and congested EMS will require a better understanding of which government, nongovernmental organization (NGO), and commercial entities affect segments of the EMS required for effective military operations (e.g., Department of State [DOS] contractors in the OA and Federal Communications Commission sale/migration of frequencies that impact DOD systems). Although there may not be intentional targeting of the EMS, inadvertent and unintentional interference may wreak havoc on the systems being used to support the execution of interagency operations. As such, constant and detailed coordination is essential between EW activities and relevant interagency organizations (e.g., DOS, DHS, CIA, and NSA). While EW operations are handled by the JCEWS or EWC, interagency coordination should be accomplished through the JSME, in concert with the JCEWS or EWC chief, to help provide separation from the more sensitive nature of EW operations. The JSME maintains a database of military EMS usage and frequency assignments and has the ability to coordinate with agency partners and collect, analyze, and deconflict frequency assignments without direct linkage to possible EW COAs or operations. In the event planning efforts are not successful in preventing EMS conflicts during the execution of interagency operations, the JSME has the capability to provide EMI and electronic countermeasures analysis and actively pursue both, as required.

Intentionally Blank

CHAPTER V
MULTINATIONAL ASPECTS OF ELECTRONIC WARFARE

"The foundation of United States, regional, and global security will remain America's relations with our allies, and our commitment to their security is unshakable."

The National Security Strategy of the United States of America 2010

1. Introduction

Operations since 2001 have reinforced the benefits of integrating US joint operations with those of our multinational partners. US planners should integrate US and partner nations' EW capabilities into an overall EW plan, provide partner nations with information concerning US EW capabilities, and provide EW support to partner nations. As in joint operations, **EW is an integral part of multinational operations.** However, the planning of MNF EW is made more difficult because of **security issues, different cryptographic equipment, differences in the level of training** of involved forces, and **language barriers.** These problems are well understood throughout North Atlantic Treaty Organization (NATO) commands and are normally addressed by **adherence to NATO standardization agreements.** Therefore, it makes sense for US forces, as participants in NATO, to adopt these procedures when working with NATO or other MNFs such as may be drawn from members of the American, British, Canadian, Australian Armies Program (ABCA) and the Air and Space Interoperability Council (ASIC) made up of the ABCA members plus New Zealand. NATO and the ABCA have developed documents to deal with MNF EW mission support. However, with the exception of Australia, Britain, and Canada (who are on the official distribution list of this publication), allied and coalition EW officers may not understand the terminology or procedures being used. A fundamental task for the EWO of a US-led MNF is to **recognize and resolve terminology and procedural issues** at the outset. This can be achieved by comparing multinational doctrine to this publication. GCCs should provide guidance to the multinational force commander (MNFC) (if the MNFC is a US Service member), within their joint OPLANs, on the release of classified material to MNFs. However, the MNFC must determine the need to know and release information essential to accomplishing the mission at the earliest stages of planning. To do this, US EW planners must be intimately aware of both sides of the issue—national security as well as mission accomplishment—in order to advise the MNFC. Intelligence components must ensure they plan sufficiently ahead for necessary approvals. See DIA Instruction 2000.001, *International Military Intelligence Relationships*, for additional information.

2. Multinational Force Electronic Warfare Organization and Command and Control

a. **MNFC.** The MNFC **provides guidance for planning and conducting EW operations to the MNF** through the operations directorate's combined EWCC. It should be recognized that the EWCC assumes responsibilities set forth in Chapter II, "Organizing for Joint Electronic Warfare."

NOTE: NATO/multinational terminology still references the EWCC. Therefore, EWCC, not EWC, will be used when discussing NATO/multinational operations.

b. **Multinational Staff.** The MNFC should assign responsibilities for management of EW resources in multinational operations among the staff for the following:

(1) **Operations Officer.** The multinational staff's operations directorate has primary responsibility for planning and integrating EW operations with other mission areas.

(2) **Staff EW Officer.** The staff EWO's primary responsibility should be to ensure the MNFC is provided the same EW support that a US JFC would expect. In addition to the duties outlined in Chapter II, "Organizing for Joint Electronic Warfare," the EWO should be responsible for the following:

(a) Ensure all component commanders of the MNF **provide qualified EWOs** as members of the MNFC EW staff. The chain of command should be established by the director for operations. The rationale for augmentee status is that partner nation officers must be full members of the multinational EW planning cell and responsible to the chain of command. They should not be subjected to the possibility of split loyalties to a lower command within the force, as could be the case if they adopted the traditional liaison role.

(b) Determine the need for placing US EW LNOs with multinational commands to ensure that the MNFC's EW **plans and procedures are correctly interpreted.**

(c) **Integrate partner nation EWO augmentees** at the initial planning stage, delegating to them duties and responsibilities similar to those given to equivalent US officers.

(d) **Coordinate the necessary EW communications connectivity** for assigned forces. Particular emphasis should be given to equipment, encryption devices and keying material, and procedural compatibility when integrating MNFs.

(e) Ensure constant liaison with the multinational staff's intelligence directorate and CSG in order to provide the most adaptive and effective intelligence support to EW efforts. Ensure planned EW targeting efforts have minimal impact on friendly C2 collection efforts.

(f) Integrate partner nation communications system directorate processes into EW planning and oversight. Integrate EW C2 requirements into the JRFL. Coordinate with the multinational staff's communications system directorate to ensure tracking and remediation of JSIR events.

(g) Provide, at the earliest possible stage, MNFs with current US EW doctrine and planning guidelines.

(3) **Partner Nation EW Officers.** Partner nation commanders should assign qualified EWOs to the MNF EW planning cell. These officers should:

(a) Have an in-depth knowledge of their own forces' operational SIGINT and EW requirements, organization, capabilities, national support facilities, and C2 structure.

(b) Possess national clearances equivalent with the level of classified US military information they are eligible to receive in accordance with US national disclosure policy. These requirements may mean the individuals concerned will be a senior O-3 or O-4 pay grade level or equivalent. As a result, they may be augmentees drawn from national sources other than the unit(s) involved in the MNF.

3. Multinational Electronic Warfare Coordination Cell with Allies and Other Friendly Forces

a. Although NATO EW policy contained in Military Committee (MC) 64/10, *NATO Electronic Warfare Policy,* is consistent with much of US EW policy, the **perspective and procedures of an MNF EWCC will be new to most.** MC 515, *Concept for the NATO SIGINT and EW Operations Centre (SEWOC),* provides the operational requirements and the operational procedures for an interoperable SEWOC to support the full range of possible NATO and NATO-led operations in a combined and joint environment. It also provides a standard of operations between agencies, services, organizations, and nodes. In addition, it outlines the basic principles, relationships, establishments, and specific details required to manage SIGINT and EW in support of NATO operations and to exercise the capability in peacetime. MC 486, *Concept for NATO Joint Electronic Warfare Core Staff (JEWCS),* describes the functions of the JEWCS. The primary functions of the JEWCS would be to provide a core staff to augment EWCCs, serve as the primary EWCC element for the NATO response force, and provide an operational planning capability for NATO operations and exercises. EWCCs and the primary EWCC element for the NATO response force are to be augmented by those nations contributing to the operation with assets using EW. The JEWCS provides EW training for NATO forces and Alliance members and provide EW support for, and analysis of, NATO and Alliance member EW systems and capabilities. At best, participants may have worked joint issues and served in adjacent forces who have exchanged EW LNOs. However, precedent exists; maritime forces have, for many years, worked multinational issues with little difficulty. Allied Tactical Publication (ATP)-08(B), *Doctrine for Amphibious Operations,* now contains a supplement on EW. This includes procedures necessary to exchange SIGINT information. In addition, Allied Joint Publication (AJP)-01(C), *Allied Joint Doctrine,* includes a chapter on EW and the EWCC. NATO members invariably base their national EW doctrine on that agreed within NATO MC 64/10. However, there is a need to ensure the most recent, releasable, US EW publications are provided to supporting MNFs. NATO has also established a NATO Emitter Database to exchange information about member countries' and nonmember countries' EM emissions and facilitate the coordination of EW.

b. Strong ties are maintained with traditional allied forces from Great Britain, Canada, and Australia. This is true particularly within the field of EW and SIGINT. **Much information is exchanged at the national level,** and this publication has been released to these nations. One example of the close ties is the Quadripartite Working Group on EW, the ABCA EW forum. Although Australia is not a party to NATO agreements, it is aware of the current status of NATO's EW policy contained in MC 64/10. Quadripartite Standardization

Agreement (QSTAG) 593, *Doctrine on Mutual Support Between EW Units*, reflects current NATO policy and meets Australia's needs. This document contains standard operating procedures for an EWCC. ASIC Working Parties (WPs) 45 (Air Operations) and 70 (Mission Avionics) both deal with EW issues. WP 45 looks at the operational employment of the MNF's EW assets, while WP 70 investigates the possibility of standardizing EW systems.

c. The principles expressed above are equally applicable to other MNFs. The MNFC should include EWOs from supporting MNFs within the EWCC. Should this not be practical for security reasons or availability, the MNFC should, based on the mission, be prepared to provide EW support and the appropriate LNOs to the multinational units.

4. Electronic Warfare Mutual Support

a. **Exchange of SIGINT information** in support of EW operations should be conducted in accordance with standard NATO, ABCA, and ASIC procedures, as appropriate. The information data elements, identified at tabs 1 and 2 and annex C, also are contained in appropriate allied publications—notably, NATO's supplement to ATP-8(A), *EW in Amphibious Operations;* ATP-44(C), *Electronic Warfare (EW) in Air Operations;* ATP-51(A), *Electronic Warfare in the Land Battle;* MC 101/12, *NATO Signals Intelligence Policy and Directive;* and ABCA's QSTAG 593, *Doctrine on Mutual Support Between EW Units.* Care should be taken not to violate SIGINT security rules when exercising EW mutual-support procedures.

b. **Exchange of Electronic Order of Battle.** In peacetime, this type of exchange is normally achieved under **bilateral agreement.** NATO has procedures in place within the major NATO commanders' precautionary system that can be put into effect during times of tension. They include the requirement to **exchange information on WARM.** The procedures also determine at what stage allied forces change to the use of WARM; however, in low-level conflict, they are unlikely to be activated. Therefore, the EWCC chief, through the EW intelligence support organization and the theater joint analysis center or theater JIOC, should ensure maintenance of an up-to-date EOB. Multinational staff officers should be included and should ensure their national commands provide appropriate updates to theater joint analysis in discussions on EOB. These staff officers should ensure their national commands provide appropriate updates to theater joint automated communication-electronics operating instructions system (JACS) and JIOCs. MC 521, *Concept for Resources and Methods to Support an Operational NATO EWCC/SEWOC,* describes a NATO EOB and who is responsible for its development and upkeep.

c. **Reprogramming.** Reprogramming of EW equipment is a **national responsibility.** However, the EWCC chief should be aware of reprogramming efforts being conducted within the MNF. The EWCC chief should keep the MNFC aware of limitations that could result in fratricide and, when necessary, seek the MNFC's assistance in attaining a solution. To do this, national and multinational commands should provide the EWCC chief with information on the following on request:

(1) Capabilities and limitations of MNF allied and/or coalition EW equipment.

(2) EW reprogramming support available within MNF allied and/or coalition units.

(3) Country-specific letters of agreement on reprogramming support for allied and/or coalition units employing US EW equipment, to include any agreement on flagging support.

(4) Country-specific letters of agreement on exchange of EW reprogramming information with those nations not employing US EW equipment.

(5) Reports from friendly units experiencing reprogramming difficulties, to include information on efforts being made to rectify the problem.

(6) Immediate reports on incidents that could have resulted in fratricide.

(7) Operational change requests sent to US reprogramming organizations that identify deficiencies in the partner nation's EW equipment and their request for reprogramming support. In turn, the EWCC chief should ensure that multinational units in the MNF receive the most recent data held within the theater tactical EOB database and, as appropriate, the associated parametric information. This should allow multinational units within the MNF to address the operational change requests, **judge the reliability of their current reprogramming data,** and, if necessary, **identify problems** to the MNF EWCC and national support agencies. Without this level of EW mutual support, fratricide may occur.

For more information on EW reprogramming, refer to Appendix E, "Electronic Warfare Reprogramming."

d. **US EW Planning Aids.** Significant improvements have been made within the US in the automation of EW planning aids. These improvements allow US EW planners to **extract information from theater and national databases and depict it in graphic format** for planning and briefing purposes. Supporting allied and/or coalition forces are unlikely to have an equal level of automation. Working with the allied and/or coalition officers, the EWCC chief should determine what EW information would assist the MNF at the planning and unit level and ensure that they get it. To do this, EWCC personnel should understand security issues that preclude the release of some data and its source but do not necessarily preclude the release of EW mission planning tools.

5. Releasability of Electronic Warfare Information to Multinational Forces

The integration of multinational EWOs into US-led MNF activities is often perceived by US staff officers as too difficult due to the complexity of national disclosure policy. As a result, this integration often occurs late in the planning process. A clear, easily understood policy on the disclosure of EW information requested by multinational partners should be developed by the commander's foreign disclosure officer as early as possible.

Intentionally Blank

APPENDIX A
ELECTRONIC WARFARE GUIDANCE

The guidance in this appendix relates to the development of tab D (Electronic Warfare) of appendix 3 (Information Operations) to annex C (Operations) of the format found in CJCSM 3122.03C, *Joint Operation Planning and Execution System, Volume II, Planning Formats*, for campaign plans, applicable contingency plans, and OPORDs. **This is guidance to supplement the format in CJCSM 3122.03.**

1. Situation

a. **Enemy**

(1) What are the capabilities, limitations, and vulnerabilities of enemy EMS-dependent (e.g., command, control, communications, computers, ISR; non-emitting; PNT service; and EW) systems?

(2) What is the enemy capability to interfere with EMS control (i.e., EW mission accomplishment and EMS management)?

(3) What are the capabilities, limitations, and vulnerabilities of enemy EMS-dependent (e.g., command, control, communications, computers, ISR; non-emitting; PNT service; and EW) systems resulting from third party support?

b. **Friendly**

(1) Is a JFC EWC currently in place? If so, is the manning adequate to address the anticipated scope of operations?

(2) What friendly EW facilities, resources, and organizations may affect or support EW planning by operational commanders?

(3) Who are the friendly forces with which operational commanders may operate?

(4) What are the capabilities, limitations, and vulnerabilities of friendly EMS-dependent (e.g., command, control, communications, computers, ISR; non-emitting; PNT service; and EW) systems?

(5) What are the impacts of civilian/commercial EM systems/networks on the EMOE?

c. **Assumptions.** What are the assumptions concerning friendly or enemy capabilities and COAs that significantly influence the planning of EW operations?

2. Mission

What is the joint force's mission (who, what, when, where, why)?

3. Execution

a. **Concept of Operations**

(1) What is the role of EW in the commander's strategy?

(2) What is the scope of EW operations?

(3) What methods and resources will be employed? Include organic and nonorganic capabilities.

(4) How will EW support other IO capabilities?

(5) What legal requirements exist that may affect EW operations?

b. **Tasks.** What are the individual EW tasks and responsibilities for each component or subdivision of the force? Include all instructions unique to that component or subdivision.

c. **Coordinating Instructions**

(1) What instructions, if any, are applicable to two or more components or divisions of EW?

(2) What are the requirements, if any, for the coordination of EW actions between subordinate elements?

(3) What is the guidance on the employment of each activity, special measure, or procedure that is to be used but is not covered elsewhere in this tab?

(4) What is the EMCON control guidance? Place detailed or lengthy guidance in an exhibit to this tab.

(5) What coordination between the J-2, J-3, and J-6 is required to plan, approve, and publish the JRFL?

4. Administration and Logistics

a. **Administration**

(1) What, if any, administrative guidance is required?

(2) What, if any, reports are required? Include example(s).

b. **Logistics.** What, if any, are the special instructions on logistic support for EW operations?

5. Command and Control

a. **Command Relationships**

(1) **Feedback**

(a) What is the CONOPS for monitoring the effectiveness of EW operations during execution?

(b) What are the specific intelligence requirements for feedback?

(2) **After-Action Reports.** What are the requirements for after-action reporting?

b. **Communications Systems.** What, if any, are the special or unusual EW-related communications requirements?

Intentionally Blank

APPENDIX B
ORGANIZATIONS SUPPORTING JOINT ELECTRONIC WARFARE

Annex A Electromagnetic-Space Analysis Center
B Global Positioning System Operations Center
C US Strategic Command Joint Electronic Warfare Center
D Joint Navigation Warfare Center
E Joint Spectrum Center
F Information Operations Range

Intentionally Blank

ANNEX A TO APPENDIX B
ELECTROMAGNETIC-SPACE ANALYSIS CENTER

1. General

a. As a DOD focal point, the E-Space program is chartered by the Under Secretary of Defense for Intelligence to provide combatant commands and their component commands with intelligence support for EW operations.

b. The increased operations tempo of the 1990s, beginning with Operation DESERT SHIELD/STORM, highlighted the growing requirement for intelligence support to IO planning, with a focus on EW.

c. The NSA is designated as the Executive Agent for the program. Organizationally, the E-Space Program Office (S1E) is part of the Customer Relationships Directorate within the NSA SIGINT Directorate.

d. Self-service data source portals are established on SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) to provide access to intelligence data from across DOD and the IC. This capability, combined with the all-source analytic center, provides direct support to EW consumers across the DOD intelligence, operations, planning, and communication communities. Direct support is also afforded the IC.

2. Mission

a. Deliver full EMS views of an adversary's EM space to enable CCDRs to develop operational COAs.

b. Serve operational users' needs by providing tailored support and technical analytic expertise to operational planners, tactical warfighters, EW system developers, and the modeling and simulation communities.

c. Ensure access to all-source, targetable, and operationally actionable intelligence information relating to EM capabilities and potential means of access to those targets using collaborative tools, databases, and analysis.

d. Provide holdings of information that will assist in preparation of the OE and electronic mapping of targets.

3. Electromagnetic-Space Support to Electronic Warfare

a. There are two entities within E-Space. The first is the acquisition of secure Web portals for both SIPRNET and JWICS. The second is the daily operations of an all-source intelligence analysis center with resident expertise capable of providing tailored support to US military forces conducting EW missions.

b. The E-Space secure Web portals provide users with a single point of access to a variety of data sources. They also provide an analytic environment to retrieve, assess, and

display or format data for use in external analytic tools. These portals are designed to provide those involved in EW operations with "self-service" rapid access to critical, decision quality intelligence.

c. The ESAC provides tailored all-source analysis to EW customers based on specific requests for intelligence. This joint center gathers intelligence from across DOD and the IC to produce tailored intelligence summaries for its customers. ESAC analysts leverage access to other experts, data sources, and analytic tools to provide warfighters with decision quality intelligence.

4. Mailing Address

E-Space

9800 Savage Road, Suite 6295

Fort George G. Meade, MD 20755-6295

5. Telephone Numbers

Defense Switched Network (DSN): 689-9910 (Portal)

DSN: 689-5811/9991 (ESAC)

COMMERCIAL: 443-479-5811 (ESAC)

6. E-Mail

SIPRNET: ESpace_Helpdesk@nsa.smil.mil (Portal)

JWICS: ESpace_Helpdesk@nsa.ic.gov (Portal)

SIPRNET: ESpaceAC@nsa.smil.mil (ESAC)

JWICS: ESpaceAC@nsa.ic.gov (ESAC)

7. URLs

SIPRNET: www.nsa.smil.mil/producer/other/espace/index.shtml

JWICS: www.nsa.ic.gov/producer/other/espace/index.shtml

ANNEX B TO APPENDIX B
GLOBAL POSITIONING SYSTEM OPERATIONS CENTER

1. General

The GPSOC provides a single center of excellence for user support and GPS constellation operations. The GPSOC, located at Schriever AFB, Colorado, provides DOD and allied GPS users worldwide with anomaly reports and other information 24 hours a day, seven days a week. USSTRATCOM's Joint Functional Component Command for Space (JFCC SPACE) has operational control of the GPSOC that is exercised through the Joint Space Operations Center (JSPOC).

2. Mission

a. The mission of the GPSOC is to operate, maintain, and employ GPS to produce a desired effect in support of military, civil, and allied operations. Key aspects of this mission are:

(1) Optimized constellation operations fully synchronized and supportive of CCDRs' needs and operational priorities.

(2) Robust, real-time performance monitoring and reporting to ensure a common operational picture and full situational awareness across all echelons of command. This is done through operational coordination with other PNT services.

(3) Full integration, coordination, and deconfliction of GPS NAVWAR operations with routine military and civil GPS operations for maximized impact and minimal collateral effects.

(4) Direct and immediate access to time-critical GPS products and services designed to leverage the effectiveness of operations reliant on GPS services.

(5) Rapid identification, isolation, and resolution of user reported outages or interference.

b. The GPSOC brings together the expertise, data fusion, and visualization capabilities, security controls, and performance information required to operate, maintain, and employ GPS to produce the desired effects to support military operations.

3. Global Positioning System Operations Center Support to Electronic Warfare

a. The GPSOC maintains databases and provides data about friendly force GPS system technical characteristics for use in planning EP measures. These databases provide EW planners with information covering GPS receivers and augmentations operated by DOD, other government departments and agencies, and private businesses or organizations. Information from these databases is available on a quick reaction basis in a variety of formats and media to support EW planners and spectrum managers.

b. The GPSOC assists GPS users across DOD with predicted GPS performance impacts to operations; post performance analysis of GPS constellation accuracy; DOD user reports of interference or jamming; user problems or questions regarding GPS; tactical support for planning; and assessing military missions involving GPS use. For EW planners, the GPSOC can assist with COA development for the EP of GPS frequencies and access to GPS information for authorized users. Additionally, the GPSOC can assist with ES through its monitoring of the GPS Jammer Location System hosted by NGA and the integration of Global Positioning System Interference and Navigation Tool (GIANT) to predict GPS jamming effects on GPS receivers. With additional information, GIANT can be used to model and predict the effects of blue force jamming on friendly systems and the use of blue force EA to prevent enemy use of GPS frequencies.

c. The GPSOC assists in the resolution of operational interference and jamming incidents through the use of the GPS Jammer Location System and the request for information or request for anomaly analysis process. The GPSOC also maintains a historical database of interference and jamming incident reports and solutions to assist in trend analysis and correction of recurring problems. Combatant commands, subordinate unified commands, JTFs, and their components can request assistance in resolving suspected GPS interference, jamming, and anomalous behavior.

4. Mailing Address

2nd Space Operations Squadron

300 O'Malley Avenue, Suite 41

Schriever AFB, CO 80912

5. Telephone Numbers

DSN: 560-2541/5081 (UNCLASSIFIED)

COMMERCIAL: 719-567-2541/5081

6. E-Mail

Nonsecure Internet Protocol Router Network (NIPRNET): gps_support@ schriever.af.mil

SIPRNET: gpsv3@afspc.af.smil.mil

ANNEX C TO APPENDIX B
US STRATEGIC COMMAND JOINT ELECTRONIC WARFARE CENTER

1. General

The JEWC integrates joint EW capabilities and employment in support of worldwide military operations and USSTRATCOM's Unified Command Plan EW responsibilities. The JEWC is USSTRATCOM's EW organization.

2. Mission

The mission of the JEWC is to integrate joint EW capabilities by providing adaptive operational solutions and advocating for the coherent evolution of capabilities and processes in order to control the EMS during military operations.

3. Joint Electronic Warfare Center

a. Serves as the central DOD repository for joint EW-related subject matter expertise supporting SecDef, Joint Staff, CCDRs, JFCs, and partner nations.

b. Advocates joint EW doctrinal, organizational, training, material, leadership and education, and personnel advancements in pursuit of EMS control.

c. Serves as office of the Deputy Under Secretary of Defense's single point of contact for EW vulnerabilities inherent in joint capability technology demonstration systems and technologies.

d. Provides advanced EW analysis support to JFC operations, tests, and exercises. In addition to short-suspense, crisis-action EW analysis and mission development, this support includes providing RF propagation and three-dimensional terrain modeling and simulation for airborne, ground-based, and shipboard EMS-dependent systems.

e. Maintains an EW rapid deployment team (the Joint EW Support Element) capable of supporting JFCs with a surge capability for initiating theater contingency operations.

f. Maintains, as the DOD lead for joint EW training oversight, the Joint EW Theater Operations Course. As a certified and required course for joint EWOs, it transforms Service EW experts into theater EW staff officers capable of shaping the EME for JFCs.

g. Monitors and evaluates the impact of current US and adversary EW technologies, systems, and TTP employed within the EMS. It also maintains an EM opposing force (OPFOR). The EM OPFOR (red team) replicates a coherent, realistic EME capable of mirroring adversary and civilian infrastructure in order to train and enhance DOD/United States Government (USG) EM capabilities, processes, and TTP proficiency. The red team is vital in providing blue forces the keys to developing a joint culture of robust, survivable EM processes via a contested/congested EME. For EM OPFOR applications, they provide a scalable real-world target set (primarily commercial off-the-shelf equipment such as wireless networks/computers, cellular infrastructure, SATCOM, and push-to-talk) for operators to

train against. Other capabilities include, but are not limited to, radio DF and communications intercept, RF vulnerability assessments, STO validation, and EW effects validation. The red team also supports TTP development for ground, sea, and air EW asset integration across the OE.

h. Collaborates with laboratories, joint and Service analysis centers, weapons schools, battle labs, centers of excellence, US and Allied operational EW communities, and academia to explore innovative EW employment options and concepts for capabilities against existing and emerging EM targets throughout the OE.

i. Provides oversight and advocacy for evolving EW capabilities and joint force requirements by identifying emerging capability gaps and technology trends employed within the EMS in order to advocate short-term mitigation possibilities and long-term solutions to the Services, combatant commands, and other agencies able to fund, or otherwise address, these shortfalls.

j. Assists commanders, as the executive agent for exercising JCEWR, with identification, confirmation, and dissemination of electronic threat changes; coordinates compatibility; and facilitates the joint EW reprogramming data exchange among the IC, Services, and combatant commands per CJCSI 3210.04, *Joint Electronic Warfare Reprogramming Policy.*

k. Manages, as the Joint Staff's Executive Agent and technical advisor, US participation in the NATO Emitter Database and performs management and coordination functions of the US Electromagnetic Systems Database in accordance with Memorandum Joint Chiefs of Staff 187-84 and CJCSI 3210.03C, *Joint Electronic Warfare Policy.*

4. Mailing Address

JEWC

2 Hall Boulevard, Suite 217

San Antonio, TX 78243-7074

5. Telephone Numbers

DSN: 969-5967 (UNCLASSIFIED)

COMMERCIAL: 210- 977-5967

DSN 969-2507 (Duty Officer)

COMMERCIAL 210-977-2507 (Duty Officer)

Facsimile (FAX): DSN 969-4233 (UNCLASSIFIED)

FAX: DSN 969-2507 (CLASSIFIED)

6. E-Mail

NIPRNET: ew_ewos@jiowc.osis.gov

SIPRNET: ew_ewos@jiowc.smil.mil

JWICS: ew_ewos@jiowc.ic.gov

Intentionally Blank

ANNEX D TO APPENDIX B
JOINT NAVIGATION WARFARE CENTER

1. General

The JNWC was established in 2004 under the Assistant Secretary of Defense/Networks and Information Integration. It was assigned to USSTRATCOM's JFCC SPACE in October 2007.

2. Mission

The JNWC's primary mission is to provide operation-level joint warfighter support and serve as the center of excellence for all NAVWAR-related issues. In addition, the JNWC integrates and coordinates PNT capabilities across DOD; provides a core interagency framework to coordinate, conduct, and report on NAVWAR testing and integration and identify mitigation strategies and TTP for PNT-based vulnerabilities (to include all terrestrial and space-based user equipment and platforms and their augmentation); and advises decision makers on significant NAVWAR issues.

3. Joint Navigation Warfare Center Support to Electronic Warfare

a. Develops and maintains current information on NAVWAR matters of interest to the warfighter and JFCs. These include assessments of adversary capabilities, assessments of coalition capabilities and limitations, and EW topics of special interest. The JNWC actively disseminates NAVWAR information to warfighters and JFCs, as well as joint and Service training organizations.

b. Analyzes and tests ES system capabilities, EA system TTP and EP vulnerabilities in relation to NAVWAR and submits recommendations to the Joint Staff, warfighter, trainers, and weapon system developers.

c. Provides a capability for independent field testing of EA/EP/ES against rapidly emerging NAVWAR threats.

d. Integrates NAVWAR PNT capabilities across ISR, IO, and space control.

4. Joint Navigation Warfare Center Navigation Warfare Support Cell

The Joint Navigation Warfare Center Navigation Warfare Support Cell (JNSC) provides a 24/7/365 operational reachback capability to the warfighter to address NAVWAR concerns during planning and current operations. The JNSC functions as the JNWC's operating staff and implements decisions, on behalf of the JNWC Director, and provides assistance to higher HQ and combatant commands as authorized in applicable orders. The JNSC develops operational-level support recommendations for Commander, JFCC SPACE; coordinates appropriate command responses to requests for information; responds to higher HQ tasking; assists with EMI event information collection and analysis; and assists operational planners in developing integrated NAVWAR plans. The JNWC reachback capabilities include GPS jamming modeling and simulation, access to the NAVWAR capabilities and vulnerabilities

database repository, current country-specific NAVWAR threat briefs, and consultation with operational planners.

5. Mailing Address

JNWC/J-3

2050A 2nd Street SE

Kirtland AFB, NM 87117-5669

6. Telephone Numbers

STE DSN: 312-246-6792

COMMERCIAL: 505-206-7594 (JNWC Duty Officer, available 24/7)

COMMERCIAL: 505-846-6846 (JNWC office, available during normal working hours)

DSN: 246-6846 (JNWC office, available during normal working hours)

7. E-Mail

NIPRNET: JNWC@kirtland.af.mil

SIPRNET: jnwcadmin@afmc.af.smil.mil

JWICS: ~wccas_jnwccdodiis.ic.gov

ANNEX E TO APPENDIX B
JOINT SPECTRUM CENTER

1. General

The JSC is a field activity of the Defense Information Systems Agency.

2. Mission

The mission of the JSC is to ensure DOD's effective use of the EMS in support of national security and military objectives. The JSC serves as the DOD center of excellence for EMS management matters in support of the combatant commands, Military Departments, and DOD agencies in planning, acquisition, training, and operations. Since EW is a principal use of the spectrum within the IO effort, JSC support extends to the EW aspects of joint military operations.

3. Joint Spectrum Center Support to Electronic Warfare

a. Maintains multiple databases that provide technical data about friendly force C2 system locational and nominal characteristics for use in planning EP measures. Databases maintained by the JSC provide EW planners with information covering communications, radar, navigation aids, broadcast, identification, and EW systems operated by DOD, other USG departments and agencies, and private businesses or organizations. Information from these databases is available through searchable Web portals or on a quick reaction basis in a variety of formats and media to support EW planners and spectrum managers.

b. Assists spectrum managers, the JCEWS/EWC, the IO cell, and EWOs in the development and management of the JRFL. The JSC maintains a worldwide DOD spectrum assignment database that is accessible through SPECTRUM XXI (SXXI), a spectrum management tool that has the capability to create, edit, and manage the JRFL. The JSC also has combatant command support teams consisting of trained JTF spectrum managers from each selected Service along with contractor support that can be deployed to assist combatant commands, subordinate unified commands, JTFs, or their components, when requested. These teams provide training and assistance in JRFL preparation and also serve as on-site advisors, assistants, and liaisons for EMS management operations and EW deconfliction, as required.

c. Assists in the resolution of operational interference and jamming incidents through the auspices of the JSIR program. The objective of the JSIR program is to resolve problems at the lowest possible level in the chain of command. The JSC maintains a rapid deployment team that is able to quickly locate and identify interference sources. This team recommends technical and operational fixes to resolve identified interference sources. The JSC also maintains a historical database of interference and jamming incident reports and solutions to assist in trend analysis and correction of recurring problems. Combatant commands, subordinate unified commands, JTFs, or their components should contact the JSC to request assistance in resolving suspected spectrum interference problems.

d. Provides foreign communications frequency and location data. Databases containing this data are developed primarily from open sources.

e. Provides unclassified communications area studies about the communications infrastructure of over 150 countries. These area studies are developed entirely from open-source material. Information in these studies includes an overview of telecommunications systems and EM frequencies registered for use within the geographic boundaries of each country and civilian, military, and radio and television broadcast frequencies. Frequency data is provided in automated form to facilitate direct input into automated spectrum management tools like SXXI.

4. Mailing Address

JSC/J-3

2004 Turbot Landing

Annapolis, MD 21402-5064

5. Telephone Numbers

DSN: 281-4357 (help desk)/9802/9850

COMMERCIAL: 410-293-4357 (help desk)/9850/9802

FAX: DSN 281-3763 (UNCLASSIFIED)

FAX: DSN 281-5309 (CLASSIFIED)

6. E-Mail

NIPRNET: operations@jsc.mil

SIPRNET: jscoperations@disa.smil.mil

JWICS: operations@jsc.ic.gov

ANNEX F TO APPENDIX B
INFORMATION OPERATIONS RANGE

1. General

The IO Range was established in 2006 to fill a requirement outlined in the 2003 IO Roadmap that called for the establishment of an IO Range to assess IO technologies and tactics in a representative OE against realistic targets.

2. Mission

The IO Range mission is to create a flexible, seamless, and persistent environment that allows CCDRs to gain confidence and experience in employing IO weapons with the same level of confidence that they have with other weapons.

3. Information Operations Range Support to Electronic Warfare

a. The IO Range supports operations through training, testing, and experimentation of nonlethal capabilities, to include EW. The range provides the ability to conduct secure operations and communications at multiple independent levels of security (Secret to Top Secret sensitive compartmented information/special access requirement). This provides users with an opportunity to conduct EW operations in both cooperative and segmented environments. The range provides a standing infrastructure that is always available and a closed loop network that ensures protection of EW operations, resources, and intellectual capital.

b. The IO Range provides an operationally realistic environment that allows EW forces to war game; conduct proficiency training; test COAs and TTP; and experiment with new and evolving EW capabilities utilizing targets and threat systems similar to those found in real-world areas of interest. Integration of EW onto the IO Range has added traditional RF-spectrum operations; nontraditional (e.g., wireless telephony networks) capabilities; and the ability to explore the use of DE, including HPM programs.

c. The integration of EW capability into the IO Range is based on several key concepts:

(1) A common federation of independent ranges that cross-leverage each other's EW capabilities.

(2) The ability to integrate fixed sites, mobile platforms, and transient targets.

(3) The execution of operations combining more than one capability, using full-spectrum EW against targets. Impacted targets would include traditional (e.g., RF), irregular (e.g. wireless), catastrophic (e.g., EMP), and disruptive (e.g., DE).

(4) The visualization of effects created in a multiple independent levels of security environment that allows interaction of EW range events simultaneously at the proper levels of security.

d. Cross-linking and sharing of EW capabilities maximizes use of low density/high demand assets. By linking sites, the IO Range architecture provides the right EW capabilities and targets necessary to conduct, for example, combined EW/CNA operations and generate effects. The IO Range gives its users access to a one-of-a-kind capability and difficult to obtain, perishable targets.

e. By linking multiple ranges, platforms, and targets with different EW and CNA capabilities, IO Range users can test, train, and develop technology and operational capabilities. Also, combined EW/CNA capabilities can be phased in over time, with additional classification levels, to more accurately reflect the EME representative of a larger campaign plan or tactical-level engagement. The IO Range provides opportunities for improved visualization of both EW and combined EW/CNA events for event controllers and test managers. This visualization improves operational execution, enhances situational awareness as events transpire, and provides ground truth for key individuals or organizations (e.g., the exercise/event white cell).

f. EW integrated onto the architecture of the IO Range enables, through virtual simulations, high-fidelity emulations, and actual threat systems, the following activities:

(1) Examination of the potential synergies of EW-enabled wireless CNA and computer network exploitation. The growing trend toward wireless networks, in both civil and military applications, increases the importance of leveraging existing capabilities or developing new EW capabilities to exploit these networks.

(2) Testing and training with EW capabilities for US forces. For example, to attack an integrated air defense system (IADS), US forces could employ a mix of capabilities (e.g., low-observable, standoff jamming, escort jamming, stand-in jamming, and self-protection TTP) against the tracking, targeting, and engagement radar systems, as well as CNA against the radars' C2 network. The IO Range could facilitate this type of engagement by supporting an integration of live, virtual, and constructive entities from geographically distributed sites. These sites could be physical ranges, labs, anechoic chambers, and other EW-related sites and organizations.

(3) Testing and training against an adversary's EW capabilities. A modern IADS consists of a mix of target acquisition and target tracking radar systems plus a layered system of man-portable, vehicle mounted, and fixed surface-to-air missile systems. While a few of the more capable US ranges might be able to support a subset of these systems, the IO Range allows pooling of the resources and capabilities of multiple ranges to create a more realistic representation of the threat(s). The IO Range also enhances the ability of US forces to train against a red OPFOR, which improves the abilities of US forces and hones their TTP.

g. The IO Range has personnel who serve as event coordinators. Event coordinators include EW subject matter experts, some of whom reside at the JEWC. They work as a team to identify sites with capabilities that can support the customer's mission objectives and are available for an event. The IO Range has additional personnel who serve as "technical event support." These individuals travel to approved IO Range sites to conduct site surveys and ensure the required infrastructure is in place. Once infrastructure concerns have been

addressed, technical event support team members again travel to the event site(s) to install necessary IO Range hardware, software, etc. The IO Range Network Operations Support Center ensures event synchronization, distribution of information, and, if desired, a common operational picture.

4. Mailing Address

Joint Staff, J-7, Deputy Director, Joint and Coalition Warfighting

ATTN: Joint IO Range

9712 Virginia Avenue, Building X-132

Norfolk, VA 23511-3212

5. Telephone Numbers

DSN: 836-9787 (UNCLASSIFIED)

COMMERCIAL: 757-836-9787

FAX: COMMERCIAL: 757-836-8911 (UNCLASSIFIED)

6. E-Mail

NIPRNET: IOR-Ops@hr.js.mil

7. Portal

https://us.jfcom.mil/sites/J7/IO_JMO/Range/default.aspx

Intentionally Blank

APPENDIX C
ELECTRONIC WARFARE JOINT MUNITIONS EFFECTIVENESS MANUAL PLANNING

1. General

a. The modern warfighter requires the ability to engage an adversary with a combination of lethal and nonlethal capabilities. Effective employment of these capabilities requires a planning mechanism capable of comparing lethal and nonlethal effectiveness and risks to determine the best mix of capabilities for the mission. While the planning process for lethal effects is easily quantifiable (e.g., 80 percent probability of destruction) and well established, the process for nonlethal effects is subjective (e.g., "good," "fair," "poor") and requires new analysis tools.

b. Communications and Radar Electronic Attack Planning Effectiveness Reference (CREAPER) is designed to improve both the EW community's application of EA capabilities as well as offer the opportunity to compare effectiveness predictions among nonlethal EA and lethal weapon options.

c. CREAPER is a computer application that uses the Improved Many-On-Many Engineer modeling algorithms to determine jammer and threat power levels, then references test and analysis data from the jamming weapons manager to display the relative effectiveness of EA weapons against specific targets. It is designed to be used by EWC operational planners to provide weapon-to-target pairing recommendations for task order generation. In short, it is a tool to be used in the capabilities analysis phase (phase 3) of the joint targeting cycle.

2. Current Applications

a. **Radar "Quick Look."** Provides a list of all EA weapons with published capabilities against the selected threat and includes a radial depicting the level of effectiveness relative to range. Figure C-1 provides an example of this application. It is used to determine weapons-target pairing versus radar systems and requires the following input: selected threat, protected entity identified, and penetration altitude.

b. **Communications "Quick Look."** Displays a list of published EA weapons that are available against the receiver in question and includes a range bar depicting the effectiveness relative to range of the receiver from the transmitter. It is used to determine weapons–target pairing for communications systems and requires the following input: threat transmitter and receiver (target).

c. **Radar Geospatial.** A radar analysis that aids the user in highlighting employment options and desired effects. The user can select a targeted threat radar from an order of battle display in a "quick look," selecting a protected entity and EA weapon (from the published list) that can then be located on the map and oriented to the threat. Subsequent analysis will display effectiveness (including terrain and meteorological effects) for the given EA weapon and protected entity approaching the threat from inbound radials color coded with the

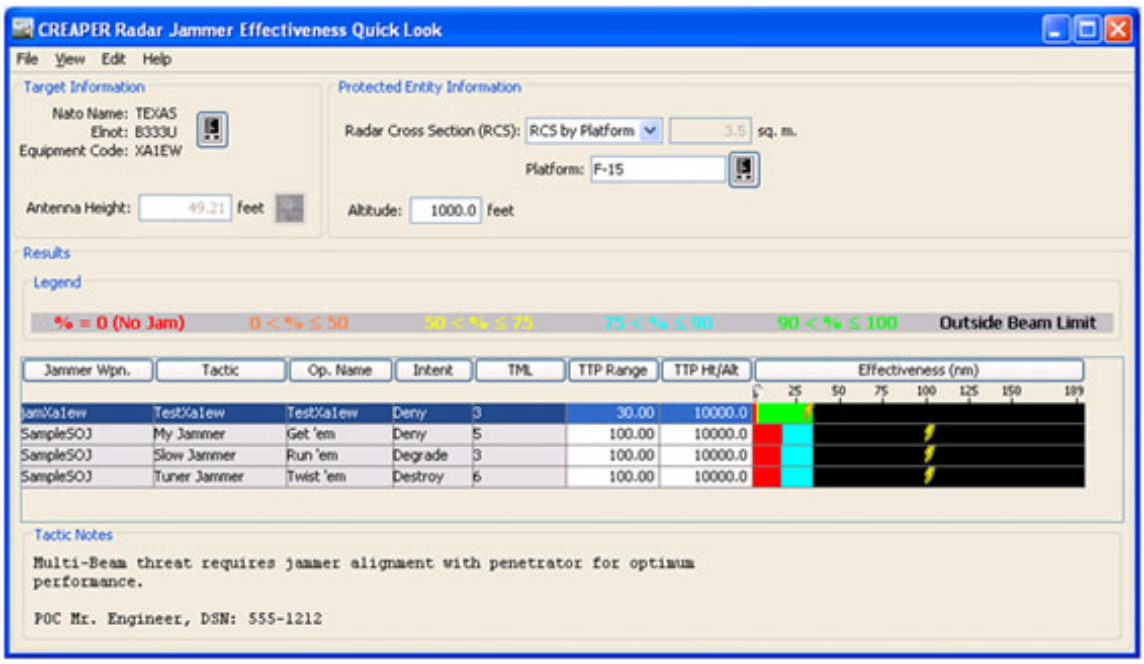


Figure C-1. Communications and Radar Electronic Attack Planning Effectiveness Reference Radar Jammer Effectiveness Quick Look

effectiveness. It is used to determine weapons–target employment and requires the following input: threat, threat location from EOB, and manual insert or live feed.

d. **Communications Geospatial.** A communication analysis that allows the user to select a transmitter and location, and a targeted receiver. By using the "quick look" against the receiver pair, the operator can select an appropriate EA weapon (from a published list), locate it on a map, and orient it to the threat. The subsequent analyses will display the effectiveness (including terrain and meteorological effects) for the given EA weapon against the receiver on any of the radials from the transmitter. It is used to determine weapons–target employment and requires the following input: transmitter geolocation and EA weapon location and orientation on the map.

e. **Ad Hoc Network.** An analysis tool used to display the portion of a designated area of operations in which communications is denied by a selected level, using percent maximum range or desired range beyond which communication is denied. Figure C-2 provides an example of this application. The Ad Hoc Network is a specialized communications jamming effectiveness tool for determining weapons-target employment and requires the following input: operating area of targeted receiver system, transmitter and receiver being targeted, desired range beyond which communications is denied, and location and orientation of the EA weapon. The resultant display shows effectiveness of the EW weapon in achieving the desired level of communications denial in the designated area of operations.

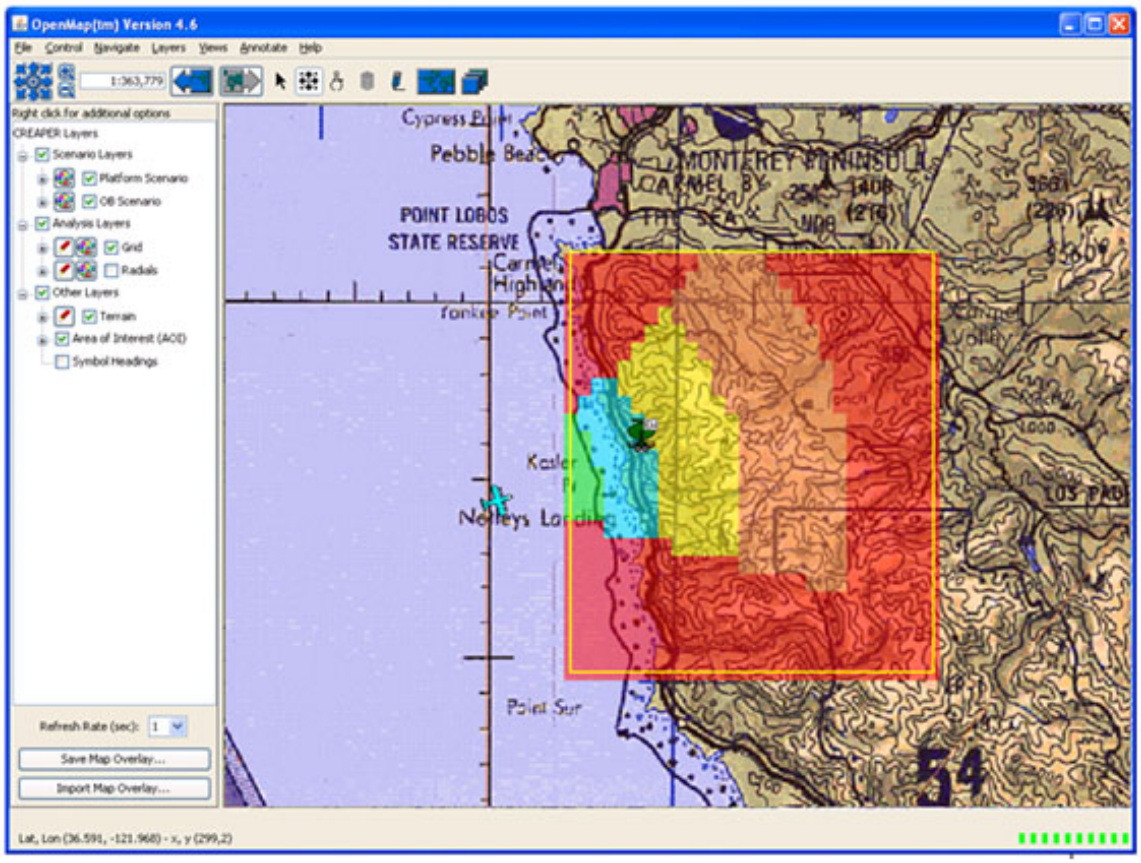


Figure C-2. Ad Hoc Network Analysis Tool

3. Applicability

a. CREAPER is designed to facilitate the selection of EA weapons by comparing systems operating in accordance with their TTP and displaying the effects against a designated threat radar or communications asset. The decision maker can then select a suitable asset to achieve his mission objectives, even if his primary expertise may be on a different platform. To further assist the decision maker, the program includes a section provided by the weapons manager for additional information, notes, warnings and cautions, as well as implementation guidance and limitations.

b. Should issues of air space allocation or potential interference from terrain and geolocation have potential impact on employment, the user can use the Radar Geospatial and Ad Hoc Network tools to perform a first order spatial analysis. This process assists the operator in both examining the impact and producing graphical displays that can be used to brief decision makers on the employment impact. For example, limiting the jammer orbit area to flight level 200 and south of the mountain range may prevent the jammer from reaching a target. However, moving the orbit area east and allowing operations at flight level 250 would provide coverage.

Intentionally Blank

APPENDIX D
ELECTRONIC WARFARE FREQUENCY DECONFLICTION PROCEDURES

1. General

Friendly, adversary, and third party operations that use or affect the EMS (e.g., communications, noncommunications, EA) have the potential to interfere with joint force communications and other EM-dependent systems. To counter this, the US military has established EMS management and EW frequency deconfliction procedures. Spectrum management is composed of an entire range of technical and nontechnical processes designed to quantify, plan, coordinate, and control the EMS to satisfy EMS-use requirements while minimizing unacceptable interference. EW frequency deconfliction is a systematic management procedure to coordinate the use of the EMS for operations, communications, and intelligence functions. While systematic, the increasingly dynamic nature of the EMOE requires that frequency deconfliction be accomplished on timescales as short as real time, depending on mission requirements. This appendix provides guidance for developing joint EW frequency deconfliction procedures. To facilitate the development process, procedures and specific staff responsibilities are discussed. To the extent possible, these procedures should be followed during joint, multinational, and single-Service operations and exercises.

2. Electronic Warfare Deconfliction Procedures

a. The steps involved in the EW frequency deconfliction process are as follows. While these steps are listed sequentially, the process is continuous and steps can occur concurrently.

b. **Define the Operations Concept and Critical Functions.** The J-3 defines the CONOPS to include each discrete phase. For each phase, the J-3 defines the critical mission functions that require uninterrupted communications connectivity or noncommunications operations. For example, communications with long-range reconnaissance elements or close air support assets could be crucial to preparing for transition from defense to offense. At the same time, noncommunications equipment such as identification, friend or foe, systems and fire-control radars also need protection. The J-3 provides this guidance to the joint force staff and subordinate commanders for planning. The J-3 also identifies these channels to the JSME for inclusion in the JRFL as either PROTECTED or TABOO.

c. **Develop the Intelligence Assessment.** Based on the CONOPS, the J-2 determines intelligence support requirements and identifies adversary EM-dependent system targets for each phase of the operation (including the critical adversary functions) and associated EM-dependent system nodes that must be guarded. For example, during the friendly attack, adversary communications and noncommunications associated with C2 of counterattack forces could be crucial to friendly forces in determining the timing and location of the counterattack. Therefore, those critical nodes should be protected from EA. To achieve that protection, the J-2 must identify to the JSME those adversary channels to be included in the JRFL as GUARDED. An IGL analysis should identify the value of the data being exploited to enable the JFC to make a decision to strike adversary C2 despite its value to intelligence.

In a dynamic situation such as troops in contact, the J-2 should work closely with the J-3 to make IGL recommendations in real time.

d. **Manage the Electromagnetic Spectrum.** The J-6 is responsible for the administrative and technical management of the EMS within the EMOE. This includes maintaining, in conjunction with the J-2 and J-3, the necessary database that contains information on all friendly, available adversary, and selected neutral or civil EM emitters or receivers. With the aid of the database, the J-6 assigns frequencies, analyzes and evaluates potential conflicts, resolves internal conflicts, recommends alternatives, and participates in EMS-use conflict resolution. The assignment of frequencies is based on the CONOPS, frequency availability, unit geographic dispersion, EM propagation, equipment technical parameters, and criticality of unit functions. Operating on assigned frequencies could spell the difference between operational success and failure.

e. **Define and Prioritize Candidate Nodes and Nets.** The joint force staff and subordinate commanders should define functions, and identify specific nodes and equipment critical to friendly and adversary operations. Candidate nodes and nets are submitted for EA protection to the JCEWS/EWC. (The submission should follow the standard JRFL format listed in paragraph 7, "Standardized Joint Restricted Frequency List Format.") Friendly and neutral EOB information is provided by the J-6 and adversary EOB information is provided by the J-2. Standard OPSEC measures should be taken when making JRFL inputs.

f. **Generate the JRFL.** The JRFL is a time- and geographic-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. The JRFL should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. The J-6 compiles the JRFL based on the coordinated inputs from the operations, intelligence, and communications staffs within the command and affected subordinate commands. An example of these inputs is the J-3 providing the J-6 with potential EA load sets for self-protection systems such as counter radio-controlled IED EW and aircraft EA in order to build coordinated communications/self-protection EA load sets. The J-6 should ensure the frequency assignments of unit nets designated for inclusion as PROTECTED or TABOO are submitted to the J-3 for final approval prior to dissemination. The restrictions imposed by the JRFL may only be removed, by direction of the J-3, if the J-3 determines the benefit of EA on a restricted frequency surpasses the immediate criticality of exploited or required information to friendly forces. Operations and intelligence functions should be consulted before this decision. However, the self-protection of friendly forces has priority over all controls. GUARDED, PROTECTED, and TABOO frequencies are as follows.

(1) **GUARDED.** GUARDED frequencies are adversary frequencies that are 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.

(2) **PROTECTED.** PROTECTED frequencies are friendly frequencies used for a particular operation, identified and protected to prevent them from being inadvertently

jammed by friendly forces while active EW operations are directed against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless absolutely necessary or until coordination with the using unit is made. They are generally time-oriented, may change with the tactical situation, and should be updated periodically.

(3) **TABOO.** TABOO frequencies are friendly frequencies of such importance that they 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. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. Specifically, 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.

g. **Disseminate the JRFL.** The JRFL is maintained and disseminated by the J-6.

h. **Update the JRFL.** The JRFL is reviewed by all joint force staff sections and subordinate commands. The J-2 might need additions, deletions, or qualified frequencies based on possible SIGINT and ES targets. The J-3 and JCEWS/EWC monitor the JRFL with respect to changes in operations, timing, dates, and TABOO frequencies. The J-6 ensures TABOO and PROTECTED frequencies are congruent with assigned frequencies. The J-6 also amends the JRFL based on J-2 and J-3 input. Supporting EW units should check the JRFL because this is the source of "no jam" frequencies. A review of the JRFL is required to identify potential conflicts between frequencies afforded protection by the JRFL and those designated for EW activities. If conflicts are identified, they should be brought to the attention of the JSME. If the JSME can't resolve the conflict, they should advise the JCEWS/EWC for final resolution. The resolution will take the form of either "override" of the JRFL protection or alter/cancel the EW activity. The decision ultimately rests with the JFC, or his designated representative, and is based on the value of the EW mission versus the gains from JRFL protection.

3. Joint Spectrum Interference Resolution Program

a. The interference reporting procedures and format are outlined in CJCSM 3320.02C, *Joint Spectrum Interference Resolution (JSIR) Procedures*. The program is coordinated and managed by the JSC and addresses all interference incidents, whether resolved or not, at the unified, subordinate unified, JTF, and component levels. The JSIR program also satisfies the requirements of the Joint Staff and the stated needs of the CCDRs for a joint-level agency to coordinate resolution of EMI incidents.

b. JSC has a 24-hour capability for receiving interference reports.

(1) The primary means for reporting EMI is through the online JSIR reporting tool that can be accessed through www.intelink.sgov.gov/sites/jsir (SIPRNET).

(2) A secondary means for submitting a JSIR report is to e-mail the report to the JSC at operations@jsc.smil.mil (SIPRNET). Enclosure C of CJCSM 3320.02C, *Joint*

Spectrum Interference Resolution (JSIR) Procedures, lists the recipients for these reports, and enclosure B contains the report format.

(3) Telephone: DSN: 281-4357, COMMERCIAL: 410-293-4357.

(4) Sensitive compartmented information traffic is serviced directly through secure FAX and Intelink in the JSC SCIF.

c. When experiencing a suspected EMI incident, resolution should be attempted at the lowest level possible in the operational chain of command. Whether a resolution is reached or not, a JSIR report should be submitted to the JSC JSIR Online Portal. If the EMI incident is resolved before the initial report is submitted, an "opening/closing" report should be submitted. If an initial report is made and the incident is resolved locally, a "closing" report should be done. These reports are necessary since the JSC JSIR team maintains a historical database in order to assist with the resolution of future problems of a similar nature. Submission of a JSIR report will not automatically generate a response or assistance from the JSC JSIR team. A response is requested in the JSIR report, including the type of assistance required.

d. Upon receipt of either a JSIR report requesting assistance or EMI support request, the JSC JSIR team performs an analysis using JSC models and databases to determine the source and works with the appropriate field activity and frequency manager to resolve interference problems. In accordance with CJCSM 3320.02C, *Joint Spectrum Interference Resolution (JSIR) Procedures*, the JSC JSIR team can deploy to the location of the victim organization to resolve interference problems. The organization requesting JSIR services is provided a report containing JSIR analysis results, and appropriate information is incorporated into the JSIR database. This database supports trend analysis and future interference analysis.

e. USSTRATCOM has overall responsibility for managing spectrum interference resolution to SATCOM systems, satellite anomaly resolutions, and global SATCOM systems for the operation and defense of the DOD information networks. Space system interference reporting and resolution is similar to the terrestrial reporting and resolution process except that the interference report is sent directly to USSTRATCOM's JSPOC from the space system manager affected. The space system includes both the space-based and earth segments. The JSPOC forwards the incident report to the appropriate lead agency for investigation and resolution. Lead agencies are the Global SATCOM Support Center for SATCOM interference and the GPSOC for GPS interference. Each lead agency coordinates with the JSC for analytical support.

4. Responsibilities

a. The responsibilities of the respective staff sections and commands in EW frequency deconfliction are noted below.

b. **J-3**

(1) Determine and define critical friendly functions (TABOO and PROTECTED) to be protected from EA and electronic deception based on the CONOPS and in coordination with components.

(2) Approve the initial JRFL and subsequent changes.

(3) Provide guidance in plans and orders as to when EA takes precedence over intelligence collection and vice versa.

(4) Resolve problems with the use of EA and electronic deception in tactical operations when conflicts arise.

(5) Weigh continually the operational advantages of employing EW against the advantages of intelligence collection.

(6) Develop and promulgate specific employment guidance and request supplemental ROE for EA and electronic deception in support of joint combat operations. Coordinate ROE and the approval process with the command staff judge advocate.

c. **J-2**

(1) In coordination with the national SIGINT authority, NSA, determine and define critical adversary functions and frequencies (GUARDED) and intelligence system processing and dissemination frequencies (PROTECTED) to be protected from friendly EA, and provide them to the J-3 (through the JCEWS/EWC) for approval.

(2) Assist in prioritizing the JRFL before J-3 approval.

(3) Develop and maintain map of nonmilitary operations in, or near, the area being jammed. Evaluate probable collateral effect on nonmilitary users.

(4) Nominate changes to the JRFL.

(5) Assist JSC in resolving reported disruption resulting from EMI.

d. **J-6**

(1) Attempt to resolve all reported non-EA-related interference.

(2) Manage all frequency assignments associated with the joint force.

(3) Conduct EW deconfliction analysis as required to support EW objectives and assist in minimizing adverse impact of friendly EA on critical networks by providing alternative frequency assignments. Compile, consolidate, coordinate, and disseminate the JRFL and provide the JCEWS/EWC with the frequency assignments for those PROTECTED or TABOO unit nets that are designated for inclusion in the JRFL.

(4) Nominate changes to the JRFL.

(5) Assist in minimizing adverse impact of friendly EA on critical networks by providing alternative communications.

e. **JCEWS/EWC**

(1) Attempt to resolve all reported EA-related interference.

(2) Coordinate and provide input to the JRFL.

(3) Recommend a joint force EW target list.

(4) Identify and resolve, if possible, conflicts that might occur between planned EA operations and the JRFL.

(5) Coordinate with J-6 and J-2 on reported interference to determine if friendly EA actions could be responsible.

(6) Establish and implement an EA request process that will identify spectrum conflicts resulting from requested EA activities.

f. **JTF Spectrum Management Element**

(1) Prepare and combine J-2, J-3, J-6, EWC, and component inputs to develop a JRFL for approval by the J-3.

(2) Update and distribute the JRFL, as required.

(3) Maintain the common EMS-use database necessary for planning and coordinating EMS control. This database contains EMS use information on all available friendly military and civilian, adversary, and neutral forces.

g. **Joint force subordinate commands and components** should, where applicable, establish a unit staff element to perform the frequency deconfliction process. This staff element should be patterned after the JCEWS/EWC and should be the focal point for frequency deconfliction for the subordinate command and component forces it represents. The responsibilities of this frequency deconfliction staff element are as follows.

(1) Submit, to the J-6, candidate nodes and nets (both friendly and adversary) with associated frequencies (if known), for inclusion in the JRFL using the format in paragraph 7, "Standardized Joint Restricted Frequency List Format." Units should specifically designate only those functions critical to current operations for inclusion in the JRFL. Overprotection of nonessential assets complicates the EA support process and significantly lengthens the time required to evaluate mission impact resulting from EMS protection. Normally, candidate nodes and nets should be submitted either through intelligence channels and consolidated by the J-2 or through operations channels and consolidated by the J-3.

(2) Identify conflicts between JRFL and friendly EA operations and request changes, as necessary, to resolve the conflicts.

(3) Report unresolved EMS disruption incidents as they occur in accordance with this publication and current interference reporting instructions.

(4) Keep the JCEWS/EWC apprised of issues that potentially impact EW planning and operations.

(5) Execute the EA request process directed by the JCEWS or EWC.

h. **JSC.** The JSC manages the DOD JSIR program as described in paragraph 3 above.

5. Frequency Deconfliction Analysis

a. Personnel analyzing frequency conflicts must consider frequency, location geometry, and time.

b. **Frequency.** The potential for interference exists whenever emitters operate at, or close to, the same frequency range. Interference can also occur through frequency harmonics, throughout the EMS, during EA operations. The JRFL limits the frequencies that require immediate review by the JCEWS/EWC. When possible, automated decision aids (e.g., SXXI, Coalition Joint Spectrum Management Planning Tool [CJSMPT]) should be used to conduct this comparison.

c. **Location Geometry.** Because of the fluid nature of the OE (mobility), the locations of friendly emitters constantly change. Locations of friendly emitters should be analyzed by the J-6 in order to predict possible interference. Analysis results depend highly on the accuracy of data and the analytical technique used.

d. **Time.** Time analysis attempts to protect critical network equipment from friendly interference during friendly EA missions. This subjective judgment is one that should be made by the J-3 or JTF commander since they must weigh the trade-off between critical EA operations and protection of vital C2 resources.

6. Automated Spectrum Management Tools

a. Commands are also encouraged to use automated spectrum management tools that will assist in developing and managing a constantly changing JRFL. To support a time and geographically oriented JRFL, automated systems must possess an engineering module that considers such factors as broadcast power, reception sensitivity, terrain, locations, distances, and time. The capability for direct computer data exchange between echelons for JRFL nominations and approval is recommended.

b. **SPECTRUM XXI.** SXXI is the DOD standard automated spectrum management tool that supports operational planning, as well as near-real-time management of the RF spectrum, with emphasis on assigning compatible frequencies and performing spectrum engineering tasks. During peacetime, SXXI is used by a joint staff at its permanent

headquarters to facilitate the complex task of EMS management during the planning and execution phases of exercises, as well as performing routine spectrum management functions. In the combat environment, SXXI is used by joint staffs to assist with joint spectrum management. It is capable of implementing any variations between peacetime and wartime operations, such as OA, frequency assignments, terrain data, equipment characteristics, and tactical constraints.

For more information on the DOD standard automated spectrum management tool, refer to Appendix G, "SPECTRUM XXI."

7. Standardized Joint Restricted Frequency List Format

The following JRFL format (see Figure D-1) is a sample listing of information for developing a JRFL. This JRFL format is unclassified but, when actually accomplished, should show the proper classification of each paragraph. The actual requirements will be determined by the JCEWS/EWC and be published in the data call for JRFL submissions.

Sample Joint Restricted Frequency List Format		
1.	CLASSIFICATION	One character (U=Unclassified, C=Confidential, S=Secret).
2.	DECLASSIFICATION	The declassification date for the frequencies to be protected.
3.	UNIT	Sixteen characters (net name as identified in the communications-electronics operating instructions). Disregard for GUARDED nominations.
4.	FREQUENCY	Twenty-four characters (K=kilohertz, M=megahertz, G=gigahertz, T=terahertz); identifies a frequency or band (e.g., M13.250-15.700).
5.	STATUS	Four characters (T=TABOO, P=PROTECTED, G=GUARDED, and a slash followed by priority A–Z and 1–9 (e.g., T/A1).
6.	START DATE	Eight characters (MM/DD/YYYY) indicate start date when protection is required, if known.
7.	END DATE	Eight characters (MM/DD/YYYY) indicate end date when protection is no longer required, if known.
8.	START HOUR	Four characters in 24-hour format (HHMM) indicate start time when protection is required, if known.
9.	END HOUR	Four characters in 24-hour format (HHMM) indicate end time when protection is no longer required, if known.
10.	TRANSMITTER COORDINATES	Fifteen characters (latitude [dd(N or S) mmss]/longitude [ddd(E or W) mmss]) provide the location to the transmitter or system, if known.
11.	RECEIVER COORDINATES	Fifteen characters (latitude [dd(N or S) mmss]/longitude [ddd(E or W) mmss]) provide the location of the receiver or system to be protected, if known.
12.	AGENCY SERIAL NUMBER	All joint restricted frequency list entries must have a frequency record in the electromagnetic spectrum database to be protected from other sources of interference. This number can be obtained from the unit frequency manager in the joint frequency management office or joint spectrum management element.
13.	POWER	Nine characters (W=watts, K=kilowatts, M=megawatts, G=gigawatts) and a maximum of five decimal places, (e.g., W10.01234), if known.
14.	EMISSION	Eleven characters (the emission designator contains the necessary bandwidth and the emission classification symbols [e.g., 3KOOJ3E]), if known.
15.	EQUIPMENT NOMENCLATURE	Eighteen characters (e.g., AN/GRC-103), if known.
16.	COMMENTS	Forty characters (provided for user remarks); optional entry.
17.	CEOI NAME	24/7 point of contact for the element operating the net that would need to be notified in the event their frequency will be targeted by planned electronic attack activities.

Figure D-1. Sample Joint Restricted Frequency List Format

Intentionally Blank

APPENDIX E
ELECTRONIC WARFARE REPROGRAMMING

1. Electronic Warfare Reprogramming

a. **Purpose.** The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and TSS equipment maintained by field and fleet units. EW reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. The reprogramming of EW and TSS equipment is the responsibility of each Service through its respective EW reprogramming support programs.

b. **Types of Changes.** Several types of changes constitute EW reprogramming. These fall into three major categories: tactics, software, and hardware.

(1) **Tactics.** Tactics changes include changes in procedures, equipment settings, or EW systems mission-planning data. These changes are usually created at the Service level by tactics developers and implemented at the unit level using organic equipment and personnel.

(2) **Software.** Software changes include actual changes to the programming of computer-based EW and TSS equipment. This type of change requires the support of a software support activity to alter programmed look-up tables, threat libraries, or signal-sorting routines.

(3) **Hardware.** Hardware changes and/or long-term system development is necessary when tactics or software changes cannot correct equipment deficiencies. These changes usually occur when the complex nature of a change leads to a system modification.

c. **EW Reprogramming Actions.** During crisis action planning or actual hostilities, EW reprogramming provides operational commanders with a timely capability to respond to changes in adversary threat systems, correct EW and TSS equipment deficiencies, and tailor equipment to meet unique theater or mission requirements.

(1) **Threat Changes.** Service EW reprogramming support programs are primarily designed to respond to adversary threat changes affecting the combat effectiveness of EW and TSS equipment. A threat change may be any change in the operation or EM signature of an adversary threat system.

(2) **Geographic Tailoring.** Geographic tailoring is the reprogramming of EW and TSS equipment for operations in a specific area or region of the world. Geographic tailoring usually reduces the number of threats in system memory. This results in decreased processing time and a reduction in system display ambiguities.

(3) **Mission Tailoring.** Mission tailoring is the reprogramming of EW and TSS equipment for the mission of the host platform. Mission tailoring may be desirable to improve system response to the priority threat(s) to the host platform.

d. **General Reprogramming Process.** The reprogramming process for EW and TSS equipment can be divided into four phases. Although the last three phases of the reprogramming process are unique by Service, each Service follows the general process described below and in FM 3-13.10, Marine Corps Reference Publication 3-40.5A, NTTP 3-51.2, AFTTP 3-2.27, *Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare Systems*.

(1) **Determine the Threat.** The first phase of reprogramming is to develop and maintain an accurate description of the equipment's OE, specifically enemy threat systems and tactics. Since EW and TSS equipment is programmed to identify and respond to particular threat or target signature data, intelligence requirements must be identified to ensure an accurate description of the EME is maintained at all times. Maintaining an accurate description of the environment requires fusion of known EM data with the collection, analysis, and validation of enemy "threat" signature changes. This first phase of the reprogramming process can be divided into the following three steps.

(a) **Collect Data.** Threat signature data collection (e.g., collection of threat system parametric information) is the responsibility of combatant and component command collection managers. Signature data may be collected as a matter of routine intelligence collection against targeted systems, while other data collection may occur as the result of urgent intelligence production requests. Regardless of the means of collection, signature data is disseminated to appropriate intelligence production centers and Service equipment support and flagging activities for analysis.

(b) **Identify Changes.** At Service equipment support and flagging activities, collected signature data is analyzed for EW and TSS equipment compatibility. Incompatible data is "flagged" for further analysis and system impact assessment. At the intelligence production centers, collected data is processed and analyzed to identify threat signature changes in the EME. Identified changes are further analyzed to ensure collector bias (i.e., collector contamination or manipulation of signature data attributed to the collector or its reporting architecture) was addressed during the analysis process.

(c) **Validate Changes.** The most important step of this initial phase of reprogramming is to validate threat signature changes. Therefore, once an identified signature change is correlated to a threat system and analyzed to ensure the reported parameters are correct and not a collector anomaly, it is further analyzed to "validate" it as an actual system capability change or identify it as a probable malfunction. Information on threat system engineering and tactical employment is critical to this validation process. Technical analysis and validation of threat changes is normally provided by one of three Service scientific and technical intelligence production centers or the DIA. During times of crisis, the combatant command must ensure this phase of the reprogramming process provides for the expeditious identification, technical analysis, and dissemination of threat change validation messages to component commands and Service reprogramming centers.

(2) **Determine the Response.** During this second phase of reprogramming, validated threat change information is used to assess its impact upon friendly EW and TSS equipment and a decision to initiate a reprogramming change is determined. If the

equipment fails to provide appropriate indications and warning or countermeasures in response to a threat change, a decision must be made to change tactics, software, or hardware to correct the deficiency. To support this decision-making process, the Service reprogramming analysis or flagging activities normally generate a system impact message (SIM) to inform combatant and component command staffs of the operational impact of the threat change to EW and TSS equipment performance. The SIM often recommends appropriate responses for each identified threat change. The Service component employing the affected equipment is ultimately responsible for determining the appropriate response to validated threat changes.

(3) **Create the Change.** The third phase of the reprogramming process is to develop tactics, software, or hardware changes to regain or improve equipment performance and combat effectiveness. A change in tactics (e.g., avoiding the threat) is usually the first option considered because software and hardware changes take time. Often, a combination of changes (e.g., tactics and software) is prescribed to provide an immediate and long-term fix to equipment deficiencies. Regardless of the type of change created, reprogramming support activities will verify equipment combat effectiveness through modeling and simulation, bench tests, or test range employments simulating operational conditions. Following the verification of effectiveness, the reprogramming change and implementation instructions are made available to appropriate field and fleet units worldwide.

(4) **Implement the Change.** The final phase of the reprogramming process is to actually implement the change to ensure unit combat effectiveness is regained or enhanced by the tactics, software, or hardware change(s). To accomplish this task, component commands ensure tactics changes are incorporated into mission pre-briefs, and software and hardware changes are electronically or mechanically installed in host platform EW and TSS equipment.

2. Joint Coordination of Electronic Warfare Reprogramming

a. **General.** Coordination of EW reprogramming is critical because threat signature changes and equipment reprogramming changes will affect the EME and, therefore, communications and all three divisions of joint EW operations conducted by US forces, MNFs, NGOs, and intergovernmental organizations. Combatant commands must ensure JCEWR policy and procedures are developed and exercised during all major training events and real-world operations.

b. **Policy.** The Joint Staff is responsible for JCEWR policy. Each Service is responsible for its individual EW reprogramming policies and procedures. The establishment and execution of JCEWR procedures is the responsibility of the combatant commands, component commands, and subordinate joint force commands. CJCSI 3210.04, *Joint Electronic Warfare Reprogramming Policy*, outlines policy and the responsibilities of the Joint Staff, Services, combatant commands, Service components, NSA, and the DIA regarding the JCEWR process. The instruction also sets forth joint procedures, guidelines, and criteria governing joint intelligence support to EW reprogramming.

Intentionally Blank

APPENDIX F
ELECTRONIC WARFARE MODELING

1. General

Modeling and simulation tools are essential for the evaluation of EW capabilities and vulnerabilities. These tools must cover the full EW analytical spectrum from the basic engineering/physics level through the aggregate effects at tactical, operational, and strategic applications levels. Simulations are critical because of the high cost associated with system development, field testing, and training exercises. Additionally, it is often impossible to replicate the scenarios required to test or exercise the multitude of variables, conditions, and interactions that occur at various levels of combat operations.

2. Application

a. **Operational Test Support.** Laboratory and range agencies use simulations to assist in test planning, scenario development, test equipment configuration, and data reduction and verification, as well as for extrapolating or expanding the use of test results.

b. **Analysis Support.** Combat developers and other analysis activities use simulations to conduct cost and operational effectiveness studies, assist in defining requirements, perform force mix and trade-off analyses, and develop TTP.

c. **Operational Support.** Operational commands use simulations to provide training from the individual to theater staff levels, serve as tactical decision aids, develop and evaluate OPLANs, and conduct detailed mission planning.

d. **Weapon System Development.** Materiel developers use simulations to support engineering development and design, capability/vulnerability and survivability analyses, and value-added assessments.

e. **Intelligence Support.** Intelligence agencies use simulations to evaluate raw intelligence, reverse engineer developing threats, develop threat projections, analyze threat design options, and evaluate threat tactics and employment options.

3. Modeling Agencies

a. There are numerous government agencies and contractors involved in EW modeling. The Joint Staff Director for Force Structure, Resource, and Assessment periodically publishes the *Catalog of Wargaming and Military Simulation Models.* This is the most comprehensive catalog of models available and identifies most agencies involved in EW modeling. Listed below are some of the joint and Service organizations involved with EW modeling and simulation.

b. **Joint.** Defense Modeling and Simulation Office, JIOWC, Joint Warfighting Analysis Center, Joint Training and Simulation Center, JSC, Warrior Preparation Center, and Joint Warfighting Center.

c. **Army.** Aviation and Missile Command, NGIC, Air Defense Center and School, Intelligence Center and School, US Army Training and Doctrine Command Analysis Center, 1st Information Operations Command (Land), Electronic Proving Ground, Communications Electronics Command, Army Material Systems Analysis Agency, Test and Evaluation Command, Signal Center and School, and National Simulation Center.

d. **Navy.** Navy Information Operation Commands, Naval Command and Control and Ocean Surveillance Center, Naval Air Warfare Center, Naval Research Laboratory, Navy Modeling and Simulation Office, Naval Strike Air Warfare Center, Naval Oceanographic Office, Center for Naval Analyses, Naval Space Command, Space and Naval Warfare Systems Command, and Naval Surface Warfare Center.

e. **Air Force.** Air Force Agency for Modeling and Simulation, Air Force Research Laboratory, NASIC, 53rd EWG, Air Force Operational Test and Evaluation Center, Air Force A9, Aeronautical Systems Center, Survivability and Vulnerability Information Analysis Center, Air Armaments Center, Air and Space C2 Agency, Aeronautical Systems Center Simulation and Analysis Facility, and Air Force Wargaming Centers.

f. **Marine Corps.** Commandant's Warfighting Lab, Marine Corps Combat Development Command's Wargaming and Combat Simulated Division, and MAGTF Staff Training Program's Modeling and Simulation Branch.

4. Fidelity Requirements

Fidelity is the degree of accuracy and detail to which the environment, physical entities, and their interactions are represented. Fidelity requirements vary widely depending on the particular purpose and application. Considerations in determining the proper fidelity should be based on scope (e.g., individual versus corps staff, engineering versus operational), consequences of inaccurate results (e.g., strike planning and execution), time available (minutes/hours to weeks/months), computer resources available (processing speed and memory/storage), accuracy and availability of data (level of detail, confidence level, and form/format), and allowable tolerance of results. Regardless of the fidelity required, a consistent methodology is required to define and guide the process. This typically entails problem definition (scope and objective), research (data gathering), analytical methodology development (how the data is used or applied), and the results/reporting format (satisfy objective/answer question). High-fidelity tools often are needed to generate data that can be used to aggregate realistic effects at higher order simulation levels (e.g., mission/campaign level wargaming). In such cases, audit trails should be available in analyst manuals or other documentation to document data sources, thereby simplifying assumptions, limitations, and aggregation techniques. In general, the setup time, input data requirements, run time, computer resources, and user knowledge/expertise increase proportionally with the model scope, fidelity, and flexibility of the modeling and simulation tools.

5. Model Design

a. **User Interface, Preprocessors, and Postprocessors.** These requirements will vary widely depending on the particular application. For example, a radar design engineer will

need much more flexibility and detail for input data than a targeting analyst would need in a tactical decision aid. Other than purpose, setup, and analysis, time requirements and user expertise are key considerations in designing preprocessors and postprocessors and the user interface. In general, maximum use should be made of standard graphic user interfaces.

b. **Electronic Warfare Functions.** Depending on the analytical level, any one EW function, or various combinations of functions, may need to be replicated in the model. EW model functions and capabilities must address areas such as RF and EO-IR wavelength propagation, radar line of sight, terrain masking, self-protect jamming, standoff jamming (communications and noncommunications), ES systems, expendables (chaff and flares), decoys (active and passive), SEAD targeting, acquisition and tracking sensors (radar, EO-IR), clutter (land/sea/atmospheric), satellite coverage (polar/geosynchronous), link analysis, missile guidance and flyout, evasive maneuvers, communications processes, EP, communications targeting, and doctrinal issues.

c. **Software Architecture.** The design of an EW model or system of models should be modular and object oriented. Existing standards and commonly used commercial software packages should be used where appropriate. Standards include those from the Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute), Federal Information Processing Standards, Military Standard-498, *Military Standard: Software Development and Documentation*, Open Software Foundation, and NSA/CSS. Military Standard-498 standards should be tailored to meet the user requirements for documentation. Standards are particularly important with regard to interfaces. The primary objective of standardization is to make the simulation as machine independent as possible. To this end, the operating system environment should conform to IEEE Portable Operating System Interface for Computer Environments standards. Additionally, communications protocols and interfaces should conform to the Government Open Systems Interconnection Profile, which is the DOD implementation of international Open Systems Interconnect standards.

6. Verification and Validation

a. **Verification.** Model verification is related to the logic and mathematical accuracy of a model. Verification is accomplished through such processes as design reviews, structured walk-throughs, and numerous test runs of the model. Test runs are conducted to debug the model as well as determine the sensitivity of output to the full range of input variables. Included in verification is a review of input data for consistency, accuracy, and source. Ultimately, verification determines if the model functions as designed and advertised. Verification is rather straightforward but time-consuming.

b. **Validation.** Model validation relates to the correlation of the model with reality. In general, as the scope of a simulation increases, validation becomes more difficult. At the engineering level for a limited scope problem, it is often possible to design a laboratory experiment or field test to replicate reality. At the force level, it is not possible to replicate all the variables in the OE and their interaction. It may be possible to validate individual functional modules by comparison with test data, or previously validated engineering-level or high- to medium-resolution models. No model totally represents reality. This disparity and the number of assumptions and limitations increase as the model scope increases. At the

force level, models tend to be stochastically driven but can provide relative answers, insights, and trends so alternatives may be rank ordered. Model users must thoroughly understand the capabilities, limitations, and assumptions built into the tool and integrate results with off-line or manual methods, as necessary, to compensate for these shortfalls. Although the above methods may be used for the validation of individual modules in a force level model, three techniques are used for validating the bottom-line output of force-on-force simulations: benchmarking with an accepted simulation, comparing with historical data, and using sound military judgment. As rapidly moving technological advances are incorporated in modern force structures, availability of useful historical data becomes less prevalent for predicting outcomes in future mid- to high-intensity conflicts. The use of forecasts and assumptions becomes necessary, but such efforts tend to be less reliable the further into the future one tries to project. Benchmarking against widely accepted simulations provides a straightforward and less biased method of validation. However, problems are caused by differences in input data structures, assumptions, and output formats between the models. To the extent possible, careful review, analysis, and data manipulation must be applied to minimize the potential of creating apparent discrepancies that can result from attempts to "compare apples to oranges."

7. Databases

Numerous databases are available to support EW modeling. Data include doctrinal, order of battle, parametric, signature, antenna pattern, communications networks, and topographic. One of the most comprehensive database catalogs available is the directory of DOD-sponsored research and development databases produced by the Defense Technical Information Center. Some sources of data for EW modeling include the following:

a. **Doctrinal or Scenario Order of Battle and Communications Networks.** DIA, NSA, Joint Training and Simulation Center, Combined Arms Center, NGIC, NASIC, 688th Information Operations Wing, Naval Air Warfare Center Weapons Division, Naval Maritime Intelligence Center, Marine Corps Intelligence Activity, and Air Force Air Warfare Center.

b. **Parametric, Signature, and Antenna Pattern.** NSA, DIA, NGIC, Naval Maritime Intelligence Center, MSIC, Office of Naval Intelligence, nuclear weapons reconnaissance list, Navy Information Operations Command, NASIC, JSC, Air Force Research Lab, Army Research Lab, Navy Research Lab, and 688th Information Operations Wing.

c. **Topographic.** NGA, CIA, US Geological Survey, Army Geospatial Center, and Waterways Experiment Station.

APPENDIX G
SPECTRUM XXI

1. General

SXXI is the standard tool used by frequency managers within DOD for managing EMS use of all known emitters. Spectrum databases are maintained worldwide through SXXI connectivity to five regional servers via SIPRNET. SXXI can be operated in stand-alone capacity when SIPRNET connectivity is not available.

2. Capabilities

a. **SXXI consists of 12 modules.** Each module and one of the module's features is listed below:

b. **Frequency Assignment.** Store, retrieve, and output databases for frequency records in both standard frequency action format (SFAF) and government master file views.

c. **Data Exchange.** Perform an automated exchange of frequency records between the client computer and the SXXI server(s).

d. **System Manager.** Purge the frequency assignment database.

e. **Topoman.** Create new topographic data files from NGA source level 1 digital terrain elevation data.

f. **Interference Analysis.** Determine the potential source of unintended interference through database analysis of current frequency assignments.

g. **Interference Report.** Create and output new interference reports.

h. **Engineering Tools.** Perform a point-to-point (path profile) link analysis.

i. **Spectrum Certification System.** Contains two tools:

(1) **Data Maintenance and Retrieval.** Create, edit, query, and output spectrum certification records (DD-1494).

(2) **Analysis Tools.** Perform engineering checks for spectrum certification records to ensure equipment parameters are within the band limitations and constraints.

j. **JRFL Editor.** Create, edit, import, and export a JRFL.

k. **EW Deconfliction.** Predict and analyze frequency conflicts from the effects of EW jamming.

l. **Allotment Plan Generator.** Create, edit, export, import, output, and delete allotment (or channel) plans.

m. **Compliance.** Run validation and allocation table checks on frequency records.

3. Interfaces

a. SXXI interfaces with other spectrum management/communications planning software through the use of the SFAF. SFAF is the Military Communications-Electronics Board Pub 7 directed format to be used for all actions concerning spectrum frequency assignments, to include spectrum database storage. SXXI interfaces with the following software/systems:

b. **Joint Automated Communication-Electronics Operating Instructions System Software. JACS** is the standard tool within DOD for management of the joint communications-electronics operating instructions and allows for the seamless transfer of data between spectrum managers and communication planners.

c. **CJSMPT** provides an integrated spectrum management, modeling and simulation, and planning capability. It enables spectrum managers and communications planners to automate and accelerate spectrum planning, thereby making it easier for personnel to communicate while avoiding interference from EM jamming operations. CJSMPT enables better management of the EMS by displaying a real-time, three-dimensional view of frequency use in the OE for land, air, and space emitters. A key feature of CJSMPT is its faster-than-real-time simulation capability that can predict and visualize potential interference from maneuver forces. This allows planners to study alternatives. In addition, by coordinating all emitters and knowing their locations in an area of operations, spectrum planners can increase their reuse of specific frequencies and significantly increase communication bandwidth to MNFs.

4. SPECTRUM XXI-Online

SXXI will be replaced by SPECTRUM XXI-Online (SXXI-O). SXXI-O will utilize the spectrum management allied data exchange format as a replacement for SFAF. Spectrum management allied data exchange format will be an extensible markup language based data format that will be the standard format used by NATO members when conducting spectrum management tasks. SXXI-O will have similar software interfaces to SXXI, as those software programs also convert to, or are replaced by, programs that produce/utilize extensible markup language based data. SXXI-O will improve on SXXI by:

a. Enhancing the frequency assignment algorithms to increase spectral efficiency.

b. Migrating to a Web-based system with a simplified user interface.

c. Developing a real-time frequency scheduling capability to enable more efficient assignment of frequencies.

d. Developing an automated capability to support the Services in the acquisition of replacement systems.

APPENDIX H
REFERENCES

The development of JP 3-13.1 is based upon the following primary references.

1. Department of Defense

a. Department of Defense Directive (DODD) 3000.3, *Policy for Non-Lethal Weapons.*

b. DODD 3222.3, *DOD Electromagnetic Environmental Effects (E3) Program*.

c. DODD 5101.14, *DOD Executive Agent and Single Manager for Military Ground-Based Counter Radio-Controlled Improvised Explosive Device Electronic Warfare (CREW) Technology*.

d. DOD Instruction 4650.01, *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*.

2. Chairman of the Joint Chiefs of Staff

a. CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces*.

b. CJCSI 3150.25D, *Joint Lessons Learned Program*.

c. CJCSI 3210.03C, *Joint Electronic Warfare Policy*.

d. CJCSI 3210.04, *Joint Electronic Warfare Reprogramming Policy*.

e. CJCSI 3320.01C, *Electromagnetic Spectrum Use in Joint Military Operations*.

f. CJCSI 3320-02D-1, *Classified Supplement to the Joint Spectrum Interference Resolution (JSIR).*

g. CJCSI 6510.01F, *Information Assurance (IA) and Computer Network Defense (CND).*

h. CJCSM 3122.03C, *Joint Operation Planning and Execution System, Volume II, Planning Formats*.

i. CJCSM 3212.02C, *Performing Electronic Attack in the United States and Canada for Tests, Training, and Exercises*.

j. CJCSM 3320.01B, *Joint Operations in the Electromagnetic Battlespace*.

k. CJCSM 3320.02C, *Joint Spectrum Interference Resolution (JSIR) Procedures*.

l. CJCSM 3500.04F, *Universal Joint Task Manual*.

m. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

n. JP 1-04, *Legal Support to Military Operations*.

o. JP 2-0, *Joint Intelligence*.

p. JP 2-01, *Joint and National Intelligence Support to Military Operations*.

q. JP 3-0, *Joint Operations*.

r. JP 3-05, *Special Operations*.

s. JP 3-09, *Joint Fire Support*.

t. JP 3-11, *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments.*

u. JP 3-13, *Information Operations*.

v. JP 3-13.2, *Military Information Support Operations*.

w. JP 3-13.3, *Operations Security*.

x. JP 3-13.4, *Military Deception*.

y. JP 3-14, *Space Operations*.

z. JP 3-41, *Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management*.

aa. JP 3-57, *Civil-Military Operations*.

bb. JP 3-60, *Joint Targeting*.

cc. JP 3-61, *Public Affairs*.

dd. JP 5-0, *Joint Operation Planning*.

ee. JP 6-0, *Joint Communications System*.

ff. JP 6-01, *Joint Electromagnetic Spectrum Management Operations*.

3. Service

a. Air Force Doctrine Document (AFDD) 3-13, *Information Operations*.

b. AFDD 3-51, *Electronic Warfare*.

c. Air Force Instruction 10-703, *Electronic Warfare Integrated Reprogramming*.

d. Army Regulation 525-22, *US Army Electronic Warfare*.

e. FM 2-0, *Intelligence*.

f. FM 3-0, *Operations*.

g. FM 3-05.120, *Army Special Operations Forces Intelligence.*

h. FM 3-36, *Electronic Warfare in Operations*.

i. NTTP 3-13.2, *Navy Information Operation Warfare Commander's Manual.*

j. NTTP 3-51.1, *Navy Electronic Warfare.*

4. Multi-Service

a. FM 3-11.4/MCWP 3-37.2/NTTP 3-11.27/AFTTP(I) 3-2.46, *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical Protection*.

b. FM 3-13.10, MCRP 3-40.5A, NTTP 3-51.2, AFTTP 3-2.7, *Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare Systems*.

5. Multinational

a. MC 64/10 NATO, *Electronic Warfare Policy*.

b. MC 101/10 NATO, *SIGINT Policy and Directive*.

c. MC 486 NATO, *Concept for NATO Joint Electronic Warfare Core Staff (JEWCS).*

d. MC 515, *Concept for the NATO SIGINT & Electronic Warfare Operations Centre (SEWOC).*

e. MC 521, *Concept for Resources and Methods to Support an Operational NATO EW Coordination Cell/SIGINT & EW Operations Centre (EWCC/SEWOC).*

f. Air STD 45/14, *Electronic Warfare*.

g. Air STD 45/3B, *Joint Air Operations Doctrine*.

h. AJP-01(C), *Allied Joint Doctrine*.

i. AJP-2, *Allied Joint Intelligence, Counter Intelligence and Security Doctrine*.

j. AJP-3.6(A), *Allied Joint Electronic Warfare Doctrine*.

k. ATP-8(B), *Doctrine for Amphibious Operations*.

l. ATP-44(C), *Electronic Warfare (EW) in Air Operations*.

m. ATP-51(A), *Electronic Warfare in the Land Battle*.

n. QSTAG 593, *Doctrine on Mutual Support Between EW Units*.

o. QSTAG 1022, *Electronic Warfare in the Land Battle*.

APPENDIX J
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Joint Staff J-7, Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, ATTN: Joint Doctrine Support Division, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent for this publication is Joint Staff, J-7, Deputy Director, Joint and Coalition Warfighting. The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

3. Supersession

This publication supersedes JP 3-13.1, 25 January 2007, *Electronic Warfare*.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: JOINT STAFF WASHINGTON DC//J-3-DDGO//

INFO: JOINT STAFF WASHINGTON DC//J-7-JEDD//

b. Routine changes should be submitted electronically to the Deputy Director, Joint and Coalition Warfighting, Joint and Coalition Warfighting Center, Joint Doctrine Support Division, and info the lead agent and the Director for Joint Force Development J-7/JEDD.

c. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Distribution of Printed Publications

Local reproduction is authorized, and access to unclassified JPs is unrestricted. However, access to and reproduction authorization for classified JPs must be in accordance with DOD 5200.1-R, *Information Security Program*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET) and https://jdeis.js.smil.mil (SIPRNET), and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved JPs and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified JP to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA, Defense Foreign Liaison/IE-3, 200 MacDill Blvd., Joint Base Anacostia-Bolling, Washington, DC 20340-5100.

c. CD-ROM. Upon request of a JDDC member, the Joint Staff J-7 will produce and deliver one CD-ROM with current JPs.

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

A-3	operations directorate (COMAFFOR staff)
A-5	plans directorate (COMAFFOR staff)
ABCA	American, British, Canadian, Australian Armies Program
AFB	Air Force base
AFDD	Air Force doctrine document
AFTTP	Air Force tactics, techniques, and procedures
AFTTP(I)	Air Force tactics, techniques, and procedures (instruction)
AJP	allied joint publication
AOC	air and space operations center (USAF)
AOR	area of responsibility
ASCC	Army Service component command
ASIC	Air and Space Interoperability Council
ATO	air tasking order
ATP	allied tactical publication
C2	command and control
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCIR	commander's critical information requirement
CI	counterintelligence
CIA	Central Intelligence Agency
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJSMPT	Coalition Joint Spectrum Management Planning Tool
CMO	civil-military operations
CNA	computer network attack
CNO	computer network operations
COA	course of action
COMAFFOR	commander, Air Force forces
COMCAM	combat camera
CONOPS	concept of operations
CONPLAN	concept plan
CREAPER	Communications and Radar Electronic Attack Planning Effectiveness Reference
CSG	Cryptologic Support Group
CSS	central security service
DCCC	defense collection coordination center
DE	directed energy
DEW	directed-energy warfare
DF	direction finding
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency

DOD	Department of Defense
DODD	Department of Defense directive
DOS	Department of State
DSN	Defense Switched Network
DSPD	defense support to public diplomacy
E3	electromagnetic environmental effects
EA	electronic attack
ELINT	electronic intelligence
EM	electromagnetic
EMBM	electromagnetic battle management
EMC	electromagnetic compatibility
EMCON	emission control
EME	electromagnetic environment
EMI	electromagnetic interference
EMOE	electromagnetic operational environment
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EOB	electronic order of battle
EO-IR	electro-optical-infrared
EO-IR CM	electro-optical-infrared countermeasure
EP	electronic protection
ES	electronic warfare support
ESAC	Electromagnetic-Space Analysis Center (NSA)
E-Space	Electromagnetic-Space
EW	electronic warfare
EWC	electronic warfare cell
EWCA	electronic warfare control authority
EWCC	electronic warfare coordination cell
EWE	electronic warfare element
EWG	electronic warfare group
EWO	electronic warfare officer
EWWG	electronic warfare working group
FAX	facsimile
FM	field manual (Army)
FSE	fire support element
G-2	Army or Marine Corps component intelligence staff officer
G-3	Army or Marine Corps component operations staff officer
G-6	Army or Marine Corps component command, control, communications, and computer systems staff officer
G-7	Army component information operations staff officer
GCC	geographic combatant commander
GCCS	Global Command and Control System

GCCS-A	Global Command and Control System-Army
GIANT	Global Positioning System Interference and Navigation Tool
GNSS	global navigation satellite system
GPS	Global Positioning System
GPSOC	Global Positioning System Operations Center
HEMP	high-altitude electromagnetic pulse
HN	host nation
HPM	high-power microwave
HQ	headquarters
IA	information assurance
IADS	integrated air defense system
IC	intelligence community
IED	improvised explosive device
IEEE	Institute of Electrical and Electronics Engineers
IGL	intelligence gain/loss
IO	information operations
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
IW	irregular warfare
IWC	information operations warfare commander
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	communications system directorate of a joint staff
JACS	joint automated communication-electronics operating instructions system
JCEWR	joint coordination of electronic warfare reprogramming
JCEWS	joint force commander’s electronic warfare staff
JEMSMO	joint electromagnetic spectrum management operations
JEMSO	joint electromagnetic spectrum operations
JEWC	Joint Electronic Warfare Center (USSTRATCOM)
JEWCS	Joint Electronic Warfare Core Staff (NATO)
JFACC	joint force air component commander
JFC	joint force commander
JFCC SPACE	Joint Functional Component Command for Space
JFMO	joint frequency management office
JIOC	joint intelligence operations center
JISE	joint intelligence support element
JNSC	Joint Navigation Warfare Center Navigation Warfare Support Cell
JNWC	Joint Navigation Warfare Center
JOC	joint operations center

JOPP	joint operation planning process
JP	joint publication
JPG	joint planning group
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JSIR	joint spectrum interference resolution
JSME	joint spectrum management element
JSPOC	Joint Space Operations Center
JTCB	joint targeting coordination board
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications System
L-EWE	land-electronic warfare element
LNO	liaison officer
LOAC	law of armed conflict
LOE	line of effort
LOO	line of operation
MAGTF	Marine air-ground task force
MC	Military Committee (NATO)
MCWP	Marine Corps warfighting publication
METOC	meteorological and oceanographic
MILDEC	military deception
MISO	military information support operations
MNF	multinational force
MNFC	multinational force commander
MOC	maritime operations center
MSIC	Missile and Space Intelligence Center
NASIC	National Air and Space Intelligence Center
NATO	North Atlantic Treaty Organization
NAVWAR	navigation warfare
NETOPS	network operations
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIPRNET	Nonsecure Internet Protocol Router Network
NSA	National Security Agency
NTTP	Navy tactics, techniques, and procedures
OA	operational area
OE	operational environment
OPFOR	opposing force
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security

PA	public affairs
PNT	positioning, navigation, and timing
QSTAG	quadripartite standardization agreement
RADBN	radio battalion
RF	radio frequency
ROE	rules of engagement
S-2	battalion or brigade intelligence staff office (Army battalion or regiment)
S-6	battalion or brigade communications staff office (Army battalion or regiment)
SATCOM	satellite communications
SCIF	sensitive compartmented information facility
SEAD	suppression of enemy air defenses
SecDef	Secretary of Defense
SEWOC	signals intelligence/electronic warfare operations centre (NATO)
SFAF	standard frequency action format
SIGINT	signals intelligence
SIM	system impact message
SIPRNET	SECRET Internet Protocol Router Network
STO	special technical operations
SXXI	SPECTRUM XXI
SXXI-O	SPECTRUM XXI-Online
TNCC	theater network operations control center
TSS	target sensing system
TTP	tactics, techniques, and procedures
USCG	United States Coast Guard
USCYBERCOM	United States Cyber Command
USG	United States Government
USSTRATCOM	United States Strategic Command
VMAQ	Marine tactical electronic warfare squadron
WARM	wartime reserve mode
WP	working party

PART II—TERMS AND DEFINITIONS

acoustical surveillance. None. (Approved for removal from JP 1-02.)

acoustic jamming. None. (Approved for removal from JP 1-02.)

barrage jamming. None. (Approved for removal from JP 1-02.)

chaff. Radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes. (Approved for incorporation into JP 1-02.)

control of electromagnetic radiation. None. (Approved for removal from JP 1-02.)

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. (Approved for incorporation into JP 1-02 with JP 3-13.1 as the source JP.)

directed energy. An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called **DE.** (Approved for incorporation into JP 1-02 with JP 3-13.1 as the source JP.)

directed-energy device. A system using directed energy primarily for a purpose other than as a weapon. (Approved for incorporation into JP 1-02.)

directed-energy protective measures. None. (Approved for removal from JP 1-02.)

directed-energy warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures. Also called **DEW.** (Approved for incorporation into JP 1-02.)

directed-energy weapon. A weapon or system that uses directed energy to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel. (Approved for incorporation into JP 1-02.)

direction finding. A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. Also called **DF.** (Approved for incorporation into JP 1-02.)

electromagnetic battle management. The dynamic monitoring, assessing, planning, and directing of joint electromagnetic spectrum operations in support of the commander's scheme of maneuver. Also called **EMBM.** (Approved for inclusion in JP 1-02.)

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. Also called **EMC.** (Approved for incorporation into JP 1-02.)

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.** (Approved for incorporation into JP 1-02.)

electromagnetic environmental effects. The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. Also called **E3.** (Approved for incorporation into JP 1-02.)

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. (Approved for incorporation into JP 1-02.)

electromagnetic interference. Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. Also called **EMI.** (Approved for incorporation into JP 1-02.)

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 1-02. SOURCE: 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 1-02. SOURCE: 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. Also called **EMP.** (JP 1-02. SOURCE: JP 3-13.1)

electromagnetic radiation hazard. Transmitter or antenna installation that generates or increases electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels. Also called **EMR hazard** or **RADHAZ.** (Approved for incorporation into JP 1-02.)

electromagnetic spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02. SOURCE: JP 3-13.1)

electromagnetic spectrum control. The coordinated execution of joint electromagnetic spectrum operations with other lethal and nonlethal operations that enable freedom of action in the electromagnetic operational environment. Also called **EMSC.** (Approved for inclusion in JP 1-02.)

electromagnetic vulnerability. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. Also called **EMV.** (JP 1-02. SOURCE: JP 3-13.1)

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 1-02. SOURCE: JP 3-13.1)

electronic intelligence. Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called **ELINT.** (JP 1-02. SOURCE: 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 systems. (JP 1-02. SOURCE: JP 3-13.1)

electronic probing. 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 or systems. (JP 1-02. SOURCE: 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 1-02. SOURCE: JP 3-13.1)

electronic reconnaissance. The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 1-02. SOURCE: 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 1-02. SOURCE: 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.** (Approved for incorporation into JP 1-02.)

electronic warfare frequency deconfliction. Actions taken to integrate those frequencies used by electronic warfare systems into the overall frequency deconfliction process. (JP 1-02. SOURCE: 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. (Approved for incorporation into JP 1-02.)

electronic warfare support. 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 1-02. SOURCE: JP 3-13.1)

electro-optical-infrared countermeasure. A device or technique employing electro-optical-infrared materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called **EO-IR CM.** (Approved for incorporation into JP 1-02.)

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. Also called **EMCON.** (JP 1-02. SOURCE: JP 3-13.1)

emission control orders. None. (Approved for removal from JP 1-02.)

ferret. None. (Approved for removal from JP 1-02.)

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 1-02. SOURCE: JP 3-13.1)

guarded frequencies. A list of time-oriented, enemy frequencies that are currently being exploited for combat information and intelligence or jammed after the commander has weighed the potential operational gain against the loss of the technical information. (Approved for incorporation into JP 1-02.)

imitative communications deception. None. (Approved for removal from JP 1-02.)

information. None. (Approved for removal from JP 1-02.)

jamming. None. (Approved for removal from JP 1-02.)

joint restricted frequency list. A time and geographically oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies and limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Also called **JRFL.** (Approved for incorporation into JP 1-02.)

meaconing. None. (Approved for removal from JP 1-02.)

nondestructive electronic warfare. None. (Upon approval of this revised publication, this term and its definition will be removed from JP 1-02.)

precipitation static. Charged precipitation particles that strike antennas and gradually charge the antenna, which ultimately discharges across the insulator, causing a burst of static. Also called **P-STATIC.** (JP 1-02. SOURCE: JP 3-13.1)

protected frequencies. Friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electronic warfare operations are directed against hostile forces. (Approved for incorporation into JP 1-02.)

pulse duration. None. (Approved for removal from JP 1-02.)

radar spoking. None. (Approved for removal from JP 1-02.)

radio frequency countermeasures. Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called **RF CM.** (JP 1-02. SOURCE: JP 3-13.1)

scan. None. (Approved for removal from JP 1-02.)

scan period. None. (Approved for removal from JP 1-02.)

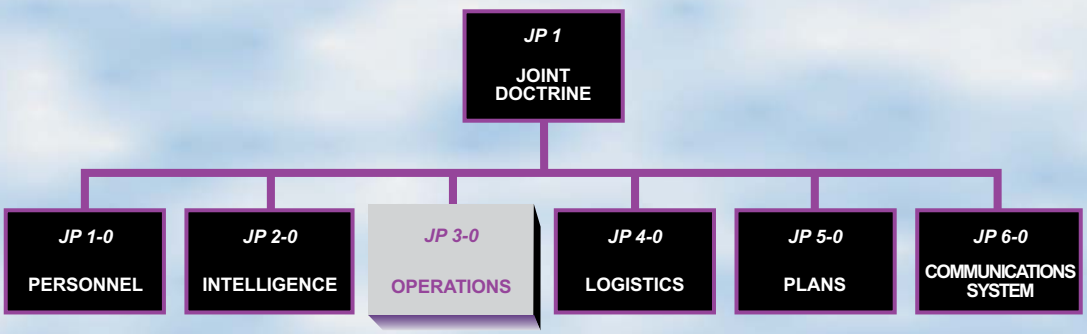
scan type. None. (Approved for removal from JP 1-02.)

TABOO frequencies. Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies. (Approved for incorporation into JP 1-02.)

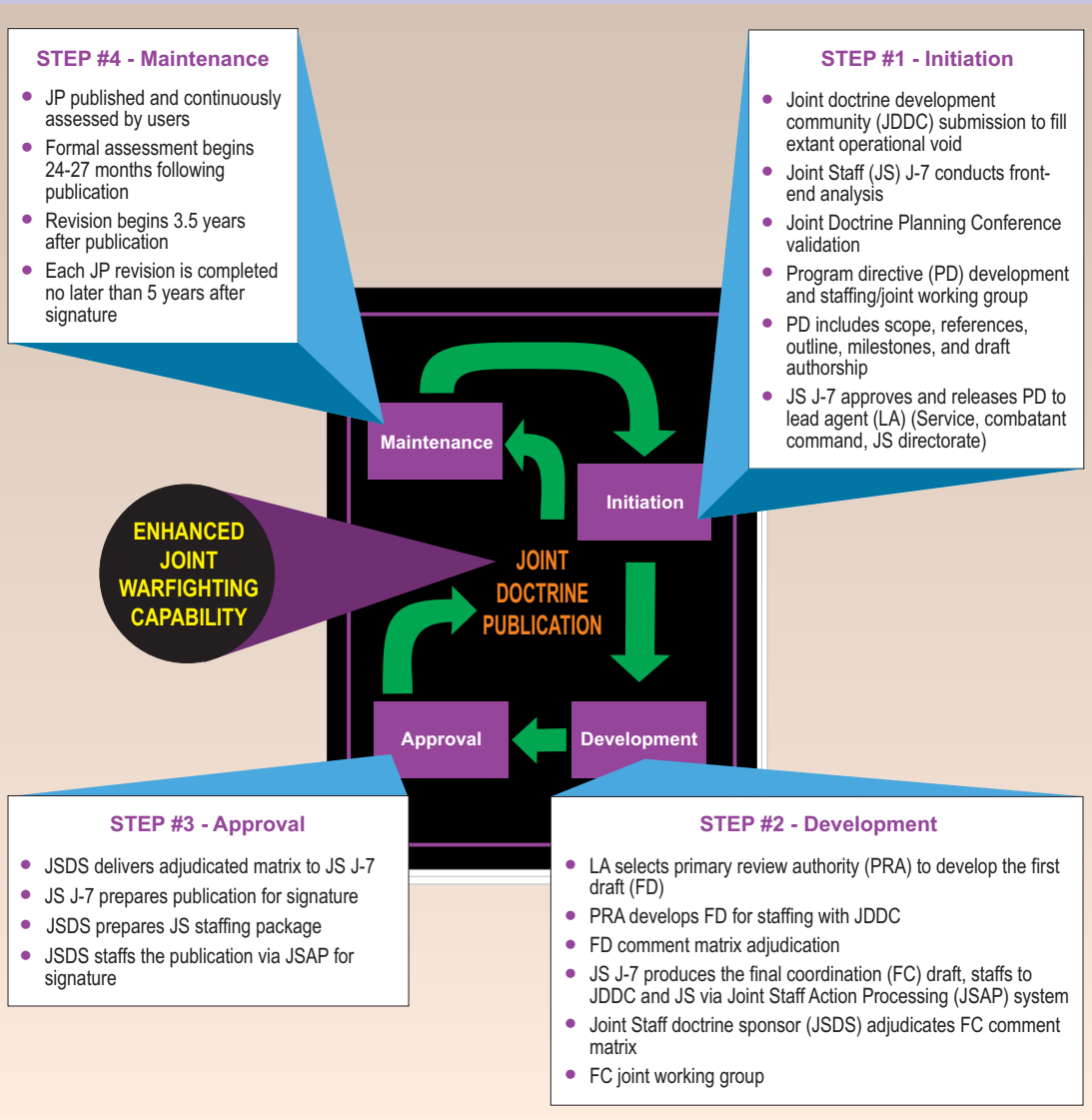
verification. 1. In arms control, any action, including inspection, detection, and identification, taken to ascertain compliance with agreed measures. (JP 3-41) 2. In computer modeling and simulation, the process of determining that a model or simulation implementation accurately represents the developer's conceptual description and specifications. (JP 3-13.1) (Approved for incorporation into JP 1-02 with JP 3-41 and JP 3-13.1 as the source JPs.

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. Also called **WARM.** (Approved for incorporation into JP 1-02.)

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-13.1** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF