Joint Publication 3-13.1

Electronic Warfare

25 January 2007

PREFACE

1. Scope

This publication provides joint doctrine for electronic warfare planning, preparation, execution, and assessment in support of joint operations 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 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 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 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:

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Intentionally Blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY v

CHAPTER I
OVERVIEW OF ELECTRONIC WARFARE

- Introduction I-1
- Electromagnetic Environment I-1
- Military Operations and the Electromagnetic Environment I-1
- Role of Electronic Warfare in Military Operations I-2
- Effects of Electronic Warfare I-4
- Electronic Warfare's Relationship to the Global Information Grid I-7
- Electronic Warfare's Relationship to Information Operations I-7
- Directed Energy as a Part of Electronic Warfare I-8
- Principal Electronic Warfare Activities I-8
- Intelligence and Electronic Warfare Support I-11
- Service Perspectives of Electronic Warfare I-11

CHAPTER II
ORGANIZING FOR JOINT ELECTRONIC WARFARE

- Introduction II-1
- Joint Electronic Warfare Responsibility II-1
- Joint Electronic Warfare Organization II-2
- Joint Frequency Management Organization II-6
- Organization of Intelligence Support to Electronic Warfare II-7
- Service Organization for Electronic Warfare II-8

CHAPTER III
PLANNING JOINT ELECTRONIC WARFARE

- Introduction III-1
- Electronic Warfare Planning Considerations III-1
- Joint Electronic Warfare Planning Process III-6
- Electronic Warfare Planning Guidance III-8
- Electronic Warfare Planning Aids III-10

CHAPTER IV
COORDINATING JOINT ELECTRONIC WARFARE

- Introduction IV-1
- Joint Coordination and Control IV-1
- Component Coordination Procedures IV-8
- Electronic Warfare and Intelligence Coordination IV-10

CHAPTER V
MULTINATIONAL ASPECTS OF ELECTRONIC WARFARE

- Introduction V-1
- Multinational Force Electronic Warfare Organization and Command and Control V-1
- Multinational Electronic Warfare Coordination Cell with Allied Forces V-3
- Multinational Electronic Warfare with Australian Armies Standardization Program and Air and Space Interoperability Council Member Nations V-3
- Multinational Electronic Warfare Coordination Cell with Other Allies or Coalition Partners V-4
- Electronic Warfare Mutual Support V-4
- Releasability of Electronic Warfare Information to Allies and Multinational Forces V-5

APPENDIX

A Electronic Warfare Guidance A-1
B Electronic Warfare Frequency Deconfliction Procedures B-1
C Joint Spectrum Center Support to Joint Electronic Warfare C-1
D Electronic Warfare Reprogramming D-1
E Electronic Warfare Modeling E-1
F Service Perspectives of Electronic Warfare F-1
G References G-1
H Administrative Instructions H-1

GLOSSARY

Part I Abbreviations and Acronyms GL-1
Part II Terms and Definitions GL-5

FIGURE

I-1 The Electromagnetic Spectrum I-2
I-2 Overview of Electronic Warfare I-3
II-1 Organization of Intelligence Support to Electronic Warfare II-9
III-1 Joint Frequency Management Office Spectrum Management Process III-2
III-2 Joint Task Force Electromagnetic Spectrum Management Planning Flow III-3
III-3 Electronic Warfare Cell Actions and Outcomes as Part of Joint Planning III-9
IV-1 Executing the Spectrum Management Plan IV-2

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an Overview of Electronic Warfare**
- **Discusses Organizing for Joint Electronic Warfare**
- **Details Joint Electronic Warfare Planning**
- **Outlines the Process of Coordinating Joint Electronic Warfare**
- **Describes Multinational Aspects of Electronic Warfare**

Overview

Electronic warfare (EW) is one of the five core capabilities.

Military operations are executed in an information environment increasingly complicated by the electromagnetic (EM) spectrum. The electromagnetic spectrum portion of the information environment is referred to as the electromagnetic environment (EME). The recognized need for military forces to have unimpeded access to and use of the EME creates vulnerabilities and opportunities for electronic warfare (EW) in support of military operations.

EW includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA involves the use of EM 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. EP involves 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. ES is the subdivision 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.

EW is waged to secure and maintain the freedom of action in the electromagnetic spectrum.

The purpose of EW is to deny the opponent an advantage in the EM spectrum and ensure friendly unimpeded access to the EM spectrum portion of the information environment. EW can be applied from air, sea, land, and space by manned and unmanned systems. EW is employed to support military operations involving various levels of

detection, denial, deception, disruption, degradation, protection, and destruction.

EW's relationship to information operations (IO).

EW contributes to the success of information operations (IO) by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while protecting friendly freedom of action in that spectrum. Expanding reliance on the EM spectrum increases both the potential and the challenges of EW in IO. All of the core, supporting, and related IO capabilities either directly use EW or indirectly benefit from EW.

Principal EW activities.

The principal EW activities have been developed over time to exploit the opportunities and vulnerabilities that are inherent in the physics of EM energy. Activities used in EW include: electro-optical-infrared and radio frequency countermeasures; EM compatibility and deception; EM hardening, interference, intrusion, and jamming; electronic masking, probing, reconnaissance, and intelligence; electronics security; EW reprogramming; emission control; spectrum management; and wartime reserve modes.

Intelligence and electronic warfare support.

The distinction between intelligence and ES is determined by who tasks or controls the collection assets, what they are tasked to provide, and for what purpose they are tasked. ES is achieved by assets tasked or controlled by an operational commander. The purpose of ES tasking is immediate threat recognition, targeting, planning and conduct of future operations, and other tactical actions such as threat avoidance and homing. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements.

Organizing for Joint Electronic Warfare

How joint forces are organized to plan and execute EW is a prerogative of the joint force commander.

The planning and supervision functions supporting EW operations are divided among several directorates of a joint staff. Long-range planning of EW normally occurs under the plans directorate, while more immediate planning and the supervision of execution of EW normally falls within the purview of the operations directorate of a joint staff (J-3). The EA portions of joint EW normally must be coordinated closely with joint force components and deconflicted with the communications systems and intelligence directorates of a joint staff (J-6 and J-2). Normally, the command EW officer (EWO) is the principal EW planner on a joint staff, is part of the J-3 staff, and coordinates with the command's IO cell.

The joint force commander's (JFC's) EW staff (JCEWS) (headed by the command EWO) develops the EW portion of operation plans (OPLANs), concept plans, and operation orders, monitors EW operations and activities, and coordinates joint EW training and exercises. It also focuses its efforts on potential contingency areas within the operational area and develops the information and knowledge necessary to support contingency planning. The JCEWS should be a standing joint planning group with multi-directorate membership consisting of core membership from the combatant command/subordinate unified command headquarters' J-2, J-3, and J-6. JCEWS membership should be a long-term assignment and members should be designated spokespersons for their respective organizations. When EW is expected to play a significant role in the JFC's mission, a component EW coordination cell (EWCC) may be designated as the joint EWCC to handle the EW aspects of the operation. The joint EWCC may either be part of the JFC's staff, assigned to the J-3 directorate, or may remain within the designated component commander's structure.

Joint frequency management organization.

Each geographic combatant commander is specifically tasked to establish a frequency management structure that includes a joint frequency management organization and to establish procedures to support planned and ongoing operations. Each supported combatant commander establishes a command policy on how the spectrum is to be used in their operational area, obtains clearance (or approval) from host nations, if applicable, for use of the spectrum, and ensures that assigned military forces are authorized sufficient use of the spectrum to execute their designated missions.

Organization of intelligence support to EW.

At the national level, organizations and agencies such as the Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency are constantly seeking to identify, catalog, and update the electronic order of battle of identified or potential adversaries. At the Department of Defense (DOD) level, the DOD joint intelligence operations center (JIOC) is the lead DOD intelligence organization responsible for coordinating intelligence support to meet combatant command requirements. At the combatant command level, intelligence support to military operations is focused in the combatant command JIOC. Individual subordinate joint force J-2 organizational structures will be situation and mission dependent, as determined by the JFC. At the discretion of the JFC, a joint intelligence support element (JISE) may be established either during shape or deter phase of an operation

and/or campaign in order 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.

Planning Joint Electronic Warfare

Joint EW is centrally planned and directed, and decentrally executed.

Through careful planning, EW must be fully integrated with other aspects of joint operations in order to achieve its full potential for contributing to an operation's objectives. Since the Services provide most US EW assets available in joint operations, Service component EW planners must be integrated into the joint planning process.

Planning considerations.

EM Spectrum Management. Since EW activity takes place in the EM spectrum, joint EW planners must closely coordinate their efforts with those members of the joint staff who are concerned with managing military use of the EM spectrum.

EW Support of Suppression of Enemy Air Defenses (SEAD). 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 support, and EW planners should coordinate closely with joint and component air planners to ensure that EW support to SEAD missions is integrated into the overall EW plan.

EW Support Against a Nontraditional Threat. The global war on terrorism has shown the enemy's ability to use commercial electronic communications means in a number of nontraditional ways ranging from ad hoc cueing networks to detonation means for improvised explosive devices. EW support to counter these efforts should be integrated into the overall EW plan.

EW Reprogramming. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and target sensing system equipment. EW reprogramming includes changes to self-defense systems, offensive weapons systems, ES, and intelligence collection systems. EW reprogramming is the responsibility of each Service or organization through its respective EW reprogramming support programs.

Electronic Masking. Electronic masking is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against

enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems.

Interoperability. Interoperability is essential in order to use EW effectively as an element of joint military power.

Primary and Cascading Effects. EW planners must consider unintended consequences of EW operations. Friendly EA could potentially deny essential services to a local population, which in turn could result in loss of life and/or political ramifications. Additionally, friendly EA could disrupt signals intelligence collection efforts, possibly eliminating a critical source of information.

Meteorology and Oceanography. EW planners must consider the effects of atmospherics and space weather on available EW systems, both friendly and enemy. The various types of atmospheric conditions and phenomena can positively or negatively affect EW systems.

Joint EW planning process.

Joint EW planning is conducted through the IO cell beginning as early as possible and is coordinated with other aspects of the plan throughout the joint operation planning process. EW guidance should be included in an OPLAN as a tab to the IO guidance. This guidance should: (1) identify the desired EM profile selected by the commander for the basic concept of operations; (2) identify EW missions and tasks to Service or functional component commanders to enable them to plan resources required; and (3) evaluate enemy threats to critical friendly command and control communications, weapons control systems, target acquisition systems, surveillance systems, and computer networks and specify EP guidance necessary to ensure effective operations.

Coordinating Joint Electronic Warfare

Once a plan has been approved and an operation is commenced, the preponderance of EW staff effort shifts to the coordination necessary to ensure that EW actions are carried out as planned or modified to respond to the dynamics of the operation.

Joint EW organizational coordination.

At combatant commands and subordinate unified commands, the JCEWS should be formed as a multi-directorate joint planning group headed by the command EWO. The JCEWS should engage in the full range of EW functions to include peacetime contingency planning, the day-to-day planning and monitoring of routine theater EW activities, and crisis action planning in preparation for EW as part of emergent joint operations.

Services should begin component EW planning and activate their EWCCs per combatant command or Service guidelines. When the scope of the contingency becomes clearer, the command EWO may request that the JFC standup a joint EWCC.

Management of the electromagnetic spectrum.

Since EW is concerned with attack, protection, and monitoring of the EM spectrum, EW staff personnel have a major role to perform in the dynamic management of the spectrum during operations. Following deployment and buildup, overlaying joint force EM emissions on the existing operational area EME will create a different environment. Further, this environment will constantly change as forces redeploy and as command and control, surveillance, weapons systems, and other spectrum-use applications realign.

Coordination with IO.

One of the primary functions of the IO cell is to deconflict and coordinate the various capabilities that are associated with IO. EW activities support psychological operations (PSYOP) by, when appropriate, degrading the adversary's ability to see, report, and process information and by isolating the target audience from information. PSYOP supports EW by broadcasting PSYOP products on adversary frequencies and by developing products for broadcast on other Service EW assets. EW supports operations security (OPSEC) by degrading adversary electromagnetic intelligence, surveillance, and reconnaissance operations against protected units and activities and by creating a barrier of white noise to mask unit maneuvers. OPSEC supports EW by concealing EW units and systems to deny information on extent of EA/ES capabilities. EW supports military deception (MILDEC) by using EA/ES as deception measures; by degrading adversary capabilities to see, report, and process competing observables; and by causing enemy to misinterpret information received by his electronic means. MILDEC supports EW by influencing an adversary to underestimate friendly EA/ES capabilities. Computer network operations (CNO) may be facilitated and/or enabled through EW. The increasing prevalence of wireless internet and telephone networks in the operational environment has created a wide range of opportunities and vulnerabilities when EW and CNO tactics, techniques and

procedures are used synergistically. EW supports information assurance (IA) by using EP to protect equipment. IA supports EW by ensuring EW assets are available. EW supports physical destruction by providing target acquisition through ES and by destroying or upsetting susceptible assets with EA. Physical destruction supports EW by destroying adversary command and control targets and by destroying adversary use of electronic systems. EW supports physical security by using EP to safeguard communications used in protecting facilities. Physical security supports EW by safeguarding equipment used in EW. Counterintelligence supports EW by providing electronic countermeasures. Finally, EW deconflicts with public affairs, combat camera, civil-military operations, and defense support to public diplomacy.

Component coordination procedures.

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.

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 that are targeted against EM energy in various parts of the EM spectrum. 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 EM spectrum. It is vital that all prudent measures be taken to ensure that EA activities and other friendly EW activities are closely and continuously deconflicted with ES and intelligence collection activities.

Multinational Aspects of Electronic Warfare

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

US planners must be prepared to integrate US and allied or coalition EW capabilities into an overall EW plan, be able to provide allied or coalition nations with information concerning US EW capabilities, and provide EW support to allied or coalition nations. The planning of multinational force (MNF) EW is made more difficult because of ill-defined security issues, incompatible

crypto equipment, differences in the level of training of involved forces, and language barriers. Geographic combatant commanders should provide guidance to the US contingent force component commander and MNF commander (MNFC) (if the MNFC is a US Service member) on the release of classified material to allied and/or coalition forces. However, the MNFC must determine the need to know and release information essential to accomplishing the mission at the earliest stages of planning.

Organization and command and control.

The MNFC provides guidance for planning and conducting EW operations to the MNF through the J-3, the IO cell or, when established, the combined EWCC. The MNFC should assign responsibilities for the operations officer, who has primary responsibility for the planning and integration of EW operations with other combat disciplines, as well as the staff EW officer, whose primary responsibility should be to ensure that the MNFC is provided the same EW support that a US JFC would expect.

Allied and/or coalition commanders should assign adequately trained EW officers to the MNF EW planning cell. These officers should have an in-depth knowledge of their own forces' operational requirements and capabilities, and possess national clearances equivalent with the level of classified US military information they are eligible to receive in accordance with US national disclosure policy.

CONCLUSION

The purpose of EW is to deny the opponent an actual or perceived advantage in the EM spectrum and ensure friendly unimpeded access to the EM spectrum portion of the information environment. The JFC should integrate the capabilities and forces from all components to achieve this goal. This publication provides doctrine for EW planning, preparation, execution, and assessment in support of joint and multinational operations across the range of military operations.

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 information environment increasingly complicated by the electromagnetic spectrum (EMS). The EMS portion of the information environment is referred to as the electromagnetic environment (EME). Today, electromagnetic (EM) devices are increasingly used alone and in networks by both civilian and military organizations and individuals for **intelligence, communications, navigation, sensing, information storage, and processing**, as well as a variety of other purposes. The increasing portability and affordability of sophisticated EM equipment guarantees that the EME in which military forces operate will become **more complex in the future**. The recognized need for military forces to have unimpeded access to and use of the EME creates **vulnerabilities and opportunities for electronic warfare (EW)** in support of military operations. In joint operations, EW is one of the five information operations (IO) core capabilities.

2. Electromagnetic Environment

The term **"EMS"** refers to the range of frequencies of EM radiation from zero to infinity. The spectrum is divided into bands ranging from radio frequencies at the low end to x-ray and gamma frequencies at the high end. Figure I-1 graphically depicts the EMS. The EME refers to the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted EM emission levels that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference (EMI); EM pulse; hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static.

3. Military Operations and the Electromagnetic Environment

The impact of the EME upon the operational capability of military forces, equipment, systems, and platforms is referred to as **electromagnetic environmental effects (E3)**. E3 refers to the impact of the EME upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all EM disciplines, including EM compatibility (EMC) and EM interference; EM vulnerability; EM pulse; electronic protection (EP), hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static. Equipment and systems that operate on the principles of electromagnetism are characterized by **EM vulnerability**. Once subjected to E3, equipment and systems that operate within or as part of the EMS, may suffer degradation (incapable of performing the designated mission).

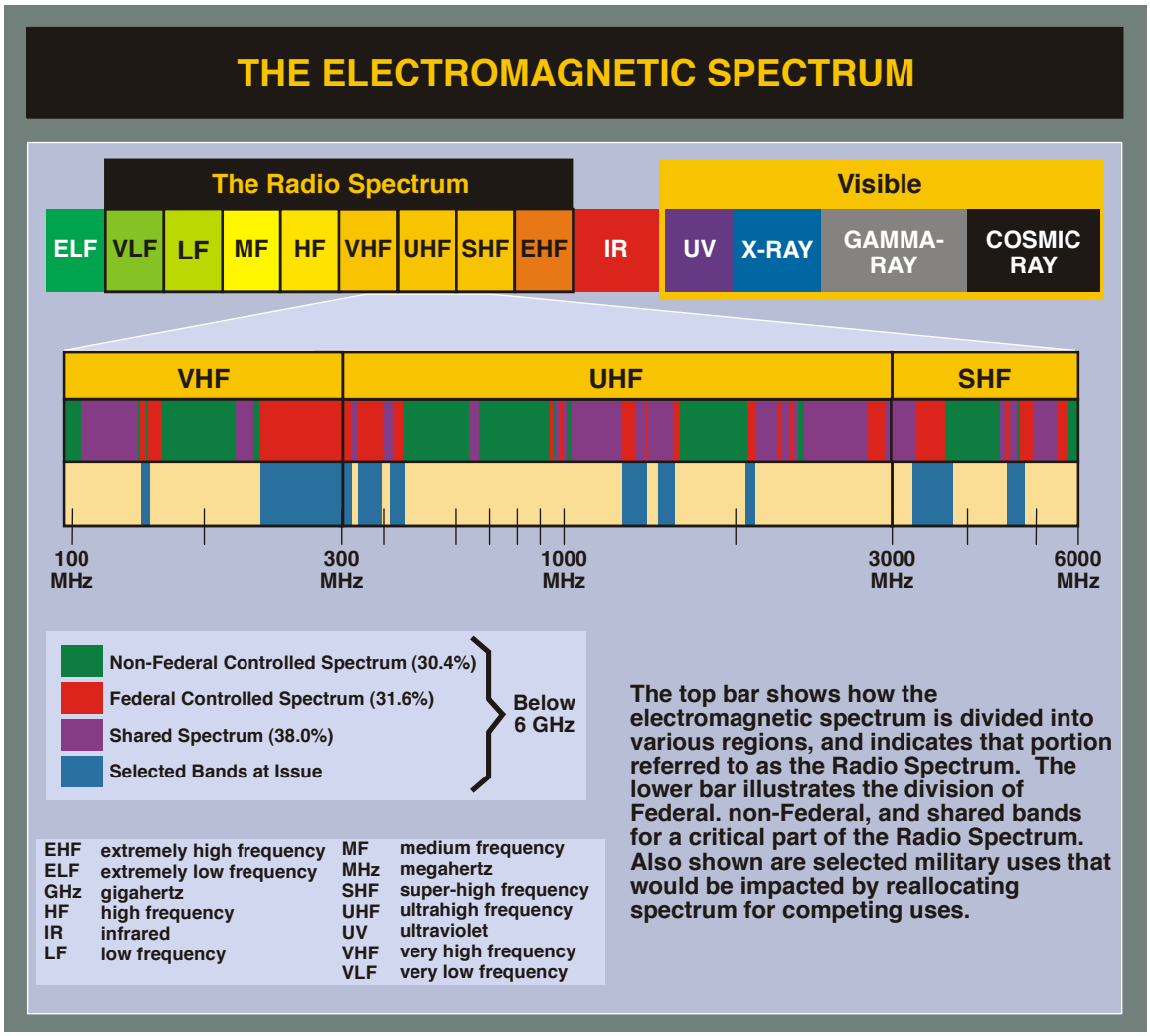


Figure I-1. The Electromagnetic Spectrum

4. Role of Electronic Warfare in Military Operations

The term EW refers to any action involving the **use of EM or directed energy (DE) to control the EMS or to attack the enemy. EW includes three major subdivisions**: electronic attack (EA), EP, and electronic warfare support (ES). Figure I-2 depicts an overview of EW, the relationships of the three subdivisions, and the relationship of the subdivisions to principal EW activities.

a. **Electronic Attack.** EA is the subdivision 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 Joint Publication [JP] 3-09, "Joint Fire Support"). EA includes:

(1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception,

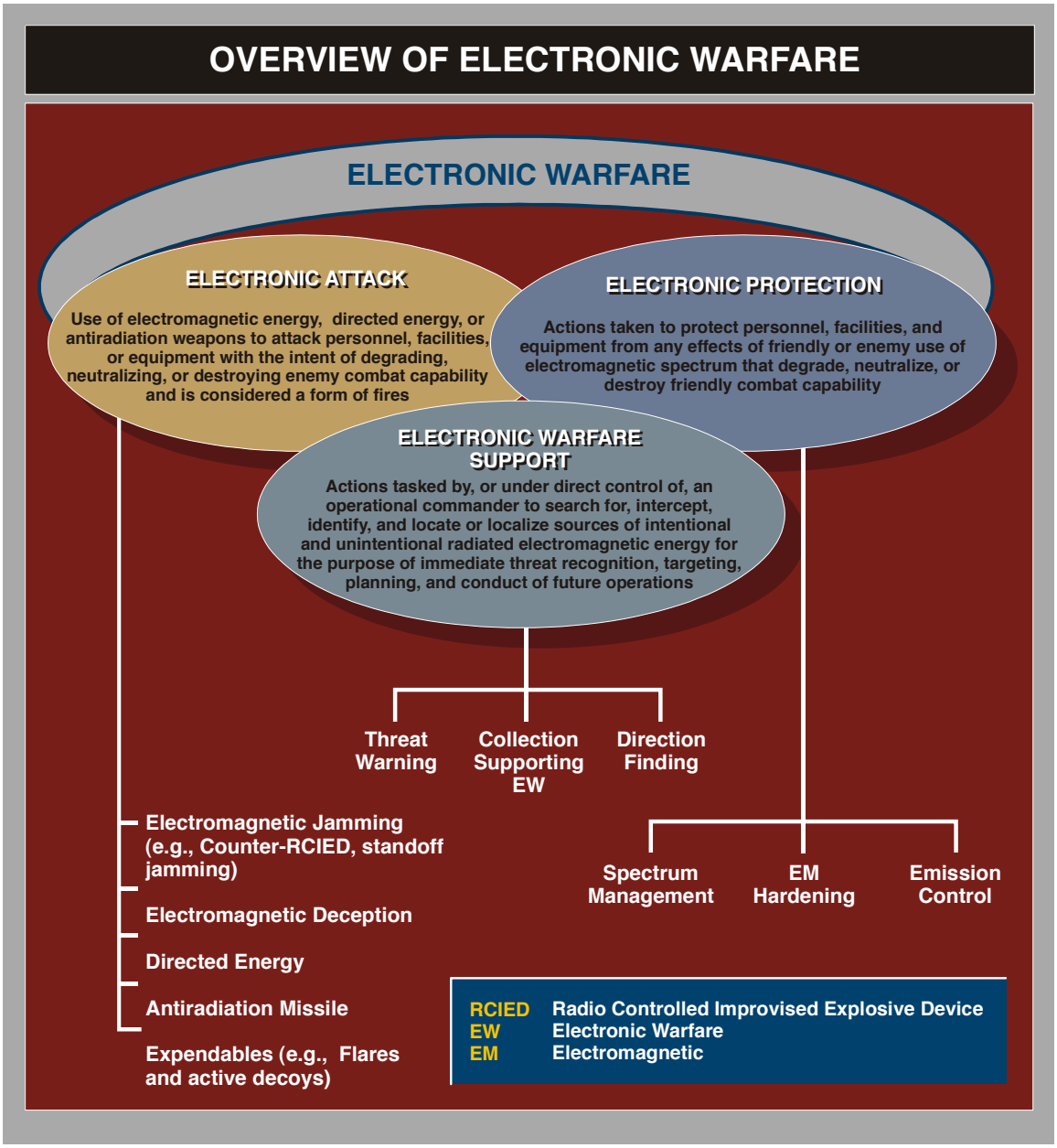


Figure I-2. Overview of Electronic Warfare

(2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams).

(3) EA includes both offensive and defensive activities to include countermeasures (CMs).

(a). Offensive EA activities are generally conducted at the initiative of friendly forces. Examples include jamming an adversary's radar or command and control (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 equipment or capability.

(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), jammers, towed decoys, DE infrared (IR) CM systems, and counter radio controlled improvised explosive device (RCIED) systems.

b. **Electronic Protection.** EP is the subdivision of EW involving actions taken **to protect personnel, facilities, and equipment** from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability. Examples include spectrum management, EM hardening, emission control (EMCON), and use of wartime reserve modes (WARM).

(1) EP includes actions taken to ensure friendly use of the EMS, such as frequency agility in a radio, or variable pulse repetition frequency in a radar.

(2) EP should not be confused with self-protection. The use of flare rejection logic on an IR missile to counter 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 self-protection/defensive EA actions (i.e., the flare) to prevent or reduce friendly use of the EMS. While defensive EA actions and EP both protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA (friendly and/or adversary), while defensive EA is primarily used to protect against lethal attacks by denying adversary use of the EMS to guide and/or trigger weapons.

c. **Electronic Warfare Support (ES).** ES refers to that 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 data can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (MASINT).

5. Effects of Electronic Warfare

EW is waged to secure and maintain the freedom of action in the EM environment for friendly forces and to deny the same for the adversary. The purpose is to deny the opponent advantage in the EMS and ensure friendly unimpeded access to the EMS portion of the information environment. EW can be applied from air, sea, land, and space by manned and unmanned systems. While control of the EMS through the application of EW is advantageous, when EW is not properly integrated and coordinated, it may adversely affect friendly forces. EW is employed to support military operations involving various levels of control, detection, denial, deception, disruption, degradation, protection, and destruction. EW can further affect the operational environment by influencing the leaders and population.

a. EW is vital throughout the shape, deter, seize initiative, dominate, stabilize, and enable civil authority phases of an operation or campaign. During the shape and deter phases, ES assets contribute

to the overall understanding of the battlefield. A judicious commander may employ EW to implement favorable intelligence preparation of the operational environment without prematurely crossing the threshold to conflict. The potential to employ nondestructive and nonlethal capabilities make EW assets vital to the preparation of the operational environment. Using EW, joint forces may set the conditions for combat when imminent, and prosecute the attack once combat is underway. The ability to achieve an objective through nondestructive means may allow a more rapid transition from seizing the initiative and the dominate phase to support operations in the stabilization phase. From stabilization to enabling civil authority, EW can foster restorative operations by offering options such as force protection through ES to monitor subversive elements, EA to counter RCIEDs, or broadcasting selected psychological operations (PSYOP) or civil defense messages to assist civil authorities.

b. EW applications in support of homeland defense are critical to deter, detect, prevent, and defeat external threats such as: ballistic missiles, aircraft (manned and unmanned), maritime vessels, land threats, hostile space systems, and cyber threats. In many cases, ES is the only method of detection and EA can dissuade or even defeat enemy attacks on the homeland.

c. In deterrence, as in other mission areas, the role of EW goes beyond simply being available to support potential combat operations. EW, as a core IO capability, supports shaping adversaries' perceptions, morale, and unit cohesion. EW applications applied toward deterrence 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.

d. **Control.** Control of the EMS is achieved by effective management/coordination of friendly systems while countering adversary systems. EA limits adversary use of the EMS; EP secures use of the EMS for friendly forces; and ES enables the commander's accurate estimate of the situation in the operational area. All three must be carefully integrated to be effective. Additionally, commanders should ensure maximum integration among EW, communications, ISR, and other IO capabilities.

e. **Detection.** Detection is the active and passive monitoring of the operational environment for radio frequency, electro-optic, laser, IR and ultraviolet EM threats. It is the essential first step in EW for effective exploitation, targeting, defensive planning, and force protection. Friendly forces must have the capability to detect and characterize interference as hostile jamming or unintentional EMI.

f. **Denial.** Denial is controlling the information an adversary receives via the EMS and preventing the acquisition of accurate information about friendly forces. Degradation can be done by traditional jamming techniques, expendable CMs, destructive measures, or network applications on a limited basis up to complete denial of usage.

g. **Deception.** Deception is confusing or misleading an adversary by using some combination of human produced, mechanical, or electronic means. Through use of the EMS, EW manipulates the adversary's decision loop, making it difficult to establish an accurate perception of objective reality.

h. **Disruption and Degradation.** Disruption and degradation techniques interfere with the enemy's use of the EMS (e.g., counter-C2) to limit their combat capabilities. This is achieved with electronic

jamming, electronic deception, and electronic 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.

i. **Protection.** Protection is the use of physical properties, operational tactics, techniques, and procedures, as well as planning and employment processes to ensure our use of the EMS. This includes ensuring that joint offensive EW activities do not electronically destroy or degrade our intelligence sensors and/or communications systems. Protection is achieved by component hardening, EMCON, frequency management/deconfliction, and employing other means to counterattack and defeat adversary attempts to control the EMS. Frequency management/deconfliction includes the capability to detect, characterize, geolocate, and mitigate EMI that affects operations. Additionally, structures like a joint force commander's (JFC's) electronic warfare staff (JCEWS) or electronic warfare coordination cell (EWCC) enhance EP through deconfliction of EW efforts.

j. **Destruction.** When used in the EW context, destruction is the elimination of targeted adversary's systems. Sensors and C2 nodes are lucrative targets because their destruction strongly influences the enemy's perceptions and ability to coordinate actions. EW, through ES, supports destruction by providing target location and/or information. Adversary systems that use the EMS can be destroyed by a variety of weapons and techniques, ranging from conventional munitions and directed energy weapons to network attacks. While destruction of adversary equipment is an effective means to deny the adversary use of the EMS, the duration of denial will depend on the adversary's ability to reconstitute.

k. **EW and the Levels of War.** EW plays a role at the tactical, operational and strategic levels of war. Jamming an early warning radar, for example, has effects on all of the 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 senior leadership from maintaining a coherent picture of the national security environment. The value of EW is fully manifested only when commanders consider and employ capabilities across the operational environment.

l**. Effects of EW in Space Control.** Space control is enabled by EW or those efforts to ensure freedom of action in space. EA may be used to deny an enemy 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 US national security interests. ES may be used to maintain awareness of the location and status of friendly and adversary space assets. Finally, EP aids in the protection of space capabilities of national interest from adversary interference.

m. **EW Delivery.** EW effects can be generated from a variety of platforms including, but not limited to:

(1) Aircraft (manned and unmanned fixed wing and rotary)

(2) Ground (fixed sites, vehicles, and troops)

(3) Ships (surface and subsurface)

(4) Space

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 battlespace may be applicable regardless of whether the target is on land, at sea, airborne, or in space.

6. Electronic Warfare's Relationship to the Global Information Grid

a. One primary consideration of EW activities should be their effect on the Global Information Grid (GIG) (including tactical communications systems) and the possibility of spectrum fratricide on friendly communications. The GIG's increasingly wireless and spaced-based communication nodes are susceptible to interference from EW. Therefore, the JCEWS or EWCC must coordinate closely with the combatant command's theater network operations control center (TNCC) and designated joint frequency management office (JFMO). The TNCC will coordinate with the Joint Task Force Global Network Operations (JTF-GNO) to deconflict the anticipated effects of EW operations on the GIG.

b. Network operations (NETOPS) and computer network defense (CND) are 24/7 operations. A secure network is a necessary prerequisite to successful operations. JTF-GNO has the United States Strategic Command (USSTRATCOM) mission to operate and defend the GIG.

c. **Network Enabled Operations.** The modern communications system allows the interconnection (networking) of geographically separated forces, which permits network enabled operations. Network enabled operations are military operations that exploit state-of-the-art information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system. Network enabled operations exploits the combat power derived from the robust networking of well informed, geographically dispersed forces. A networked force can increase combat power, achieving greater speed of command decisions and increasing the lethality, survivability, and responsiveness of the force. The JFC is responsible for ensuring radio frequency (RF) deconfliction occurs via the EWCC and frequency management offices in order to minimize EMI.

7. Electronic Warfare's Relationship to Information Operations

a. IO is the integrated employment of the core capabilities of EW, computer network operations (CNO), PSYOP, military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. The supporting capabilities of IO include information assurance (IA), physical security, physical attack, counterintelligence (CI), and combat camera (COMCAM). Related capabilities of IO include public affairs (PA), civil military operations (CMO), and defense support to public diplomacy (DSPD).

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 in that spectrum. 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 electronic vulnerabilities and a requirement to identify and protect our own from similar exploitation.

c. All EW activities conducted in joint operations should be planned and managed by personnel dedicated to EW and EM spectrum management. Typically these personnel belong to a JCEWS and joint EWCCs. These staffs must participate in and coordinate with the JFC's IO cell, which will align objective priorities and synchronize EW employment with other IO related capabilities and operations.

For more information on joint IO doctrine, refer to JP 3-13, "Information Operations." For more information on joint tactics, techniques, and procedures for conducting suppression of enemy air defenses (SEAD), refer to JP 3-01, "Countering Air and Missile Threats."

8. Directed Energy as a Part of Electronic Warfare

DE is an umbrella term covering technologies that produce a beam of concentrated EM energy or atomic or subatomic particles. A DE weapon is a system using DE primarily as a direct means to **damage or destroy adversary equipment, facilities, and personnel**. **DE warfare** is military action involving the use of DE weapons, devices, and countermeasures to either **cause direct damage or destruction** of adversary equipment, facilities, and 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**. Possible applications include lasers, radio frequency weapons, and particle beam weapons. DE applications easily fit into traditional EW roles. For example, a laser designed to blind or disrupt optical sensors is, in EW terms, EA. A laser warning receiver designed to detect and analyze a laser signal is, in EW terms, ES. A visor or goggle designed to filter out the harmful wavelength of laser light is, in EW terms, EP. The threat of an adversary's use of destructive DE weapons is also growing. Intelligence assets must be tasked to collect information about this threat, and joint planning must include the concerted development of operational procedures and courses of action (COAs) to mitigate the effects of adversaries' 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."

9. Principal Electronic Warfare Activities

The principal EW activities have been developed over time to **exploit the opportunities and vulnerabilities that are inherent in the physics of EM energy**. Although new equipment and new tactics continue to be developed, the physics of EM energy remains constant. This physical constant is the reason basic activities of EW have remained effective despite changes in hardware and tactics. The principal activities used in EW include the following.

a. **Countermeasure(s)** – CM is 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. CMs can be active or passive. They can be deployed preemptively or reactively.

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

(2) **Radio Frequency Countermeasures**. Any device or technique employing RF materials, radar absorbent materials, or technology that is intended to impair or counter the effectiveness of or counter enemy activity, particularly with respect to precision guided weapons and sensor systems.

b. **Electromagnetic Compatibility. EMC** is the ability of systems, equipment, and devices that utilize the EMS to operate in their intended operational environments **without suffering unacceptable degradation or causing unintentional degradation** because of EM radiation or response. EMC involves the application of sound EMS management: system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness.

c. **Electromagnetic Deception.** EM deception is the deliberate radiation, reradiation, 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 EM Deception.** This type of deception involves actions to eliminate revealing, or convey misleading, EM telltale indicators that may be used by hostile forces.

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

(3) Imitative **EM Deception.** This type of deception introduces EM energy into enemy systems that imitates enemy emissions.

d. **Electromagnetic Hardening.** EM hardening consists of actions taken to protect personnel, facilities, and equipment by **filtering, attenuating, grounding, bonding, and shielding** against undesirable effects of EM energy.

e. **Electromagnetic Interference. EMI** is any EM disturbance that **interrupts, obstructs, or otherwise degrades or limits the effective performance** of electronics or electrical equipment. It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, and intermodulation products.

f. **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**.

g. **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**, with the intent of degrading or neutralizing the enemy's combat capability.

h. **Electromagnetic Pulse. EM pulse** is **a strong electronic pulse,** that may couple with electrical or electronic systems to produce damaging current and voltage surges.

i. **Electronic Masking.** Electronic masking is the **controlled radiation of EM energy on friendly frequencies** so as to protect the emissions of friendly communications and electronic systems against enemy ES measures or signals intelligence (SIGINT), without significantly degrading the operation of friendly systems.

j. **Electronic Probing.** Electronic probing is the **intentional radiation into the devices or systems of potential enemies** for the purpose of learning the functions and operational capabilities of the devices or systems.

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

l. **Electronic Intelligence. Electronic intelligence (ELINT)** is the technical and geolocational **intelligence derived from foreign noncommunications EM radiations** emanating from other than nuclear detonations or radioactive sources.

m. **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 noncommunications EM radiations, e.g., radar.

n. **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.

o. **Emission Control. EMCON** is the selective and controlled use of EM, acoustic, or other emitters to **optimize C2 capabilities** while minimizing, for operations security:

(1) Detection by enemy sensors;

(2) Mutual interference among friendly systems; and

(3) Inhibitors to executing a military deception plan.

p. **Spectrum Management.** Spectrum management involves planning, coordinating, and managing use of the EMS through **operational, engineering, and administrative procedures**. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

q. **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.

10. Intelligence and Electronic Warfare Support

Electronic forms of intelligence gathering (SIGINT, MASINT, and other forms) comprise a significant portion of the day-to-day activities of the intelligence community. The distinction between intelligence and ES is determined by who tasks or controls the intelligence assets, what they are tasked to provide, and for what purpose they are tasked. ES that is not part of the intelligence process is often referred to as combat information (i.e., Airborne Warning and Control System passive detection system). ES is achieved by **assets** tasked or controlled by an operational commander. These assets are tasked **to search for, intercept, identify, and locate or localize** sources of intentional or unintentional radiated EM energy. 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**. However, the same assets and resources that are tasked with ES can simultaneously collect intelligence that meets other collection requirements. That is not to say that data collected for intelligence cannot meet immediate operational requirements. Intelligence collected for ES purposes is normally also processed by the appropriate parts of the intelligence community for further exploitation after the operational commander's ES requirements are met.

11. Service Perspectives of Electronic Warfare

Planning and execution of joint EW is affected by the different viewpoints on EW held by the Military Services. Although formal EW definitions are standardized in the Department of Defense (DOD), different operational environments and tactical objectives lead to variations in perspective among the Services.

Appendix F, "Service Perspectives of Electronic Warfare," gives a brief overview of the differences in EW perspective among the four Services.

Intentionally Blank

CHAPTER II
ORGANIZING FOR JOINT ELECTRONIC WARFARE

"Generally, management of the many is the same as management of the few. It is a matter of organization."

Sun Tzu

1. Introduction

How joint forces are organized to plan and execute EW is a **prerogative of the JFC**. The size of the commander's staff, the mission or missions which the joint force is tasked to accomplish, and the time allocated to accomplish the mission or missions are just some of the factors which affect the organization of the staff. This chapter discusses nominal **organizations and staff functions** to plan and execute EW in joint operations. It also summarizes EMS management functions and the joint level organization of intelligence support to EW. A brief introduction to **how each of the four Services is organized to plan and execute EW** is provided in order to give an understanding of how joint staff EW functions interact with Service components.

2. Joint Electronic Warfare Responsibility

As with other combat, combat support, and combat service support functions, EW planning and operations are divided among multiple directorates of a joint staff based on long, mid, and near term functionality. **Long-range planning** of EW normally occurs under the plans directorate of a joint staff (J-5), while more **immediate planning and the supervision** of execution of EW normally falls within the purview of the operations directorate of a joint staff (J-3). All aspects of joint EW normally must be coordinated closely with joint force components and deconflicted with the communications system directorate of the joint staff (J-6) and the intelligence directorate of a joint staff (J-2). The joint restricted frequency list (JRFL) is prepared and promulgated by the J-6 with approval by the J-3. EA, ES, and EP functions significantly affect, and conversely are affected by activities within the J-2, J-3 and J-6. Examples include ES support to collection, management, and dissemination as well as all source analysis of intelligence information (J-2), overall EW operations to include OPSEC planning and integration within the IO division (J-3), as well as day-to-day operations of the information GIG, JRFL planning and integration, and EP considerations (J-6).

a. **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 ensuring 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.

b. The IO officer is the principal IO advisor to the J-3 and acts as the J-3, IO division lead planner for the integration, coordination and execution of IO when conducting campaigns across the range of military operations. The IO officer identifies and prioritizes IO requirements on behalf of the JFC and ensures full spectrum IO is integrated into appropriate security cooperation plans.

JP 3-13, "Information Operations," provides details about the organization and procedures of the IO cell.

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 operational area of the JFC that the staff supports, and the type of mission or operation that the staff must plan. The command EWO is part of the J-3 staff and coordinates with the command's IO cell.

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), plans and monitors routine EW operations and activities, and coordinates joint EW training and exercises. It also focuses its efforts on potential contingency areas within the operational area 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) and enabling organizations such as Service and multinational EWCCs, the USSTRATCOM Joint Information Operations Warfare Command (JIOWC), E-Space portal, and the Joint Spectrum Center (JSC). These relationships are established during joint training and exercise events and are maintained via a network of collaboration throughout the planning process.

(1) Organization of the JCEWS. The JCEWS should be a standing joint planning group with multi-directorate membership. The JCEWS does not require additional billets, but rather, networks existing command billets to focus on joint EW planning and execution. At a minimum the JCEWS should consist of core membership from the combatant command/subordinate unified command headquarters' J-2, J-3, and J-6. The J-6 deconflicts all EW activity that affects the GIG with JTF-GNO through the theater NETOPS centers and theater NETOPS control centers (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. Nominal JCEWS membership may include:

(a) JCEWS chief (command EWO)

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

(c) JFMO/J-6 representative

(d) J-2 SIGINT collection manager

(e) J-2 cryptologic support group (CSG) representative

(f) Special technical operations (STO) planner

(2) Nominal JCEWS networked representation may include:

(a) EW planners from Service/functional components (e.g., joint force air component commander (JFACC), joint force special operations component commander (JFSOCC), and commander, Navy forces, distributed common ground system).

(b) EW asset liaison officers (LNOs) (e.g., EA-6B, EC-130H, US Marine Corps radio battalion, RC-135, distributed common ground system)

b. **Joint Electronic Warfare Coordination Cell.** The decision to form a joint EWCC depends on the anticipated role of EW in the operation. When EW is expected to play a significant role in the JFC's mission, a component EWCC may be designated as the joint EWCC to handle the EW aspects of the operation. The joint EWCC may either be part of the JFC's staff, assigned to the J-3 directorate, or may remain within the designated component commander's structure. The joint EWCC will plan operational level EW for the JFC.

(1) Nominal members of the joint EWCC may include:

(a) EWCC chief

(b) Deputy EWCC chief

(c) EW operations chief

(d) EW 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) JFC JFMO representative

(2) Nominal joint EWCC networked representation should include:

(a) JFC JFMO

(b) J-6 representative

(c) JFC J-2 SIGINT collection manager

(d) JFC J-2 CSG representative

(e) Service/functional components LNOs

(f) Other government agency representatives

(g) Coalition partner representatives

c. JCEWS and joint EWCC responsibilities:

(1) Specific functions and responsibilities of a JCEWS:

(a) Be familiar with EW support to current theater OPLANs and CONPLANs

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

(c) Formulate and recommend EW targets to support the JFC OPLAN

(d) Implement EW policies

(2) Functions and responsibilities common to JCEWS and joint EWCC (When a JCEWS and joint EWCC exist at the same level, the owning commander must decide command and coordination relationships between the two organizations).

(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 ISR assets and national agencies in assessing hostile EW capabilities and limitations

(f) Coordinate with ISR and national resources to weigh intelligence gain/loss of EA or the physical destruction of targets, and if necessary, coordinate the resolution of these conflicts. Resolution of intelligence gain/loss conflicts resides with the JFC.

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

(h) Maintain current assessment of the 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 the JFC's objectives, EW plan and available assets

(k) Represent EW within the IO cell to formulate and recommend to the joint targeting coordination board EW targets to support the JFC's plan

(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., EW deconfliction, EMCON, EW reprogramming)

(n) Assist JFMO in conjunction with JFC J-2, J-3, J-6, other government agencies, joint special operations center, components, and allies in resolving spectrum conflicts that JFMO or JCEWS are unable to resolve

(o) Carry out responsibilities of the jamming control authority (JCA)

(p) Coordinate and monitor joint coordination EW reprogramming (JCEWR) by identifying where EW reprogramming decisions and reprogramming actions affect joint force tactical operations and disseminating theater-wide EW plans as required

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

(r) Plan, coordinate, integrate, and deconflict EW in current and future operations taking in consideration nontraditional capabilities (e.g., IO, space, special operations, and STO) within the operational area

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

(t) Coordinate through the chain of command to resolve any component/multinational EW requests that cannot be solved at the JCEWS or joint EWCC level

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

(v) Archive EW planning and execution data and document EW lessons learned in accordance with the joint lessons learned program

(3) Joint EWCC Support Requirements**.** When activated, the EWCC should be located in or have access to a special compartmented information facility to permit thorough accomplishment of its coordinating functions. Optimal joint EWCC staffing will dictate the inclusion of STO cleared personnel in order to coordinate and deconflict STO issues. The joint EWCC will also have requirements for administrative, intelligence, logistics, legal and communications support.

(a) Administrative. Administrative support will include, but not be 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 joint EWCC will require all-source intelligence information to maintain full knowledge of an opposing force's intentions and capabilities. Intelligence support will include specific and detailed combat information, intelligence, and ES information for example: opposing force electronic systems; scheme of maneuver; communications system capabilities and deployment; electronic-dependent weapon systems capabilities and deployment; as well as EW activities, and SIGINT collection plans of friendly units. The J-2 will coordinate with theater EW units 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 joint EWCC includes, but is not limited to: storage containers for classified material; desks; maps; information display facilities; messing and billeting of assigned personnel.

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

(e) Legal. Support for the joint EWCC 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 (CCDR) is specifically tasked by joint EMS use policy (Chairman of the Joint Chiefs of Staff Instruction [CJCSI] 3320.01B, "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 CCDR authorizes

and controls use of the spectrum resources by the military forces under his or her command. Each supported CCDR establishes a command policy on how the spectrum is used in there area of responsibility (AOR), obtains clearance (or approval) from host nations for use of the spectrum (through existing coordination procedures), and ensures that assigned military forces are authorized sufficient use of the spectrum 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 control of the spectrum** for assigned forces. At the JTF level a joint spectrum management element (JSME) may be established. The combatant command JFMO or the JSME within a JTF may be assigned from the J-6 staff, from a component's staff, or from an external command such as the JSC (see Appendix C, "Joint Spectrum Center Support to Joint Electronic Warfare"). In any event, the combatant command JFMO or the JSME within a JTF must be staffed with trained spectrum managers, preferably with experience in joint spectrum use and knowledge of the spectrum requirements of the combatant command component forces. Figure III-1 diagrams the spectrum management process followed by the combatant command JFMO or JSME within a JTF. *The basic process the combatant command JFMO* or the JSME within a JTF *uses to carry out its primary responsibilities is discussed further in Chapter III, "Planning Joint Electronic Warfare," and Chapter IV, "Coordinating Joint Electronic Warfare." Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3320.01B, "Joint Operations in the Electromagnetic Battlespace," provides additional information about the JFMO and its functions and processes.*

5. Organization of Intelligence Support to Electronic Warfare

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

a. **National-Level Intelligence Organizations.** At the national level, organizations and agencies such as the Central Intelligence Agency (CIA), National Security Agency (NSA), and Defense Intelligence Agency (DIA) are constantly seeking to **identify, catalog, and update the electronic order of battle (EOB)** of identified or potential adversaries. Other intelligence agencies, such as the National Geospatial-Intelligence Agency (NGA), **support the maintenance of the EOB**. National-level organizations such as the National Air & Space Intelligence Center (NASIC), the National Ground Intelligence Center (NGIC), and the 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 that is gathered about adversary electronic 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.

JP 2-01, "Joint and National Intelligence Support to Military Operations," provides more detailed discussion on the organization of national level intelligence support.

b. **Defense Joint Intelligence Operations Center (DJIOC).** The DJIOC is the lead DOD intelligence organization for coordinating intelligence support to meet combatant command requirements.

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 organization according to established procedures. EW planners at the combatant command level work with the command J-2 staff to **satisfy EW intelligence requirements** according to command specific procedures established by each CCDR.

JP 2-0, "Intelligence Support," provides additional discussion of how theater-level intelligence support is accomplished.

d. **Subordinate Joint Force.** The J-2 is the **primary point of contact** for providing intelligence support to joint EW. Within the context of a geographic combatant command, individual subordinate joint force J-2 organizational structures will be situation and mission dependent, as determined by the JFC. The J-2 normally assigns one or more members of his/her staff to act as a liaison between the J-2 section of the staff and the IO cell (or other IO staff structure) where EW planners are normally assigned. At the discretion of the JFC, a JTF **joint intelligence support element (JISE)** may be established during crisis or the preparation stage for operations 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 purpose of this liaison is to coordinate collection requirements and analytical support for compartmented and non-compartmented IO. Because of the close interrelationship between EW (particularly ES) and activities such as SIGINT, EW planners may find it necessary to work with a wide variety of personnel in the intelligence section of the staff.

JP 2-01, "Joint and National Intelligence Support to Military Operations," discusses how the intelligence community is organized to support joint military operations.

6. Service Organization for Electronic Warfare

Each Military Service has a different approach to organizing its forces in order to plan and execute EW. Since the Services provide most US EW assets, a basic understanding of each Service's EW organization greatly facilitates the planning and coordination of EW at the joint level.

a. **Army.** Army EW assets are organized to ensure that EW operations are developed and integrated as part of the commander's overall concept of operations. At each echelon of Army organization responsible for an EW mission, the **assistant chief of staff (ACOS), information operations staff officer (G-7), in coordination with the ACOS, Army or Marine Corps component intelligence staff officer (G-2), ACOS, component operations staff officer (G-3), and ACOS, component communications systems staff officer, is responsible for planning and coordinating** EW operations into the IO plan. The **EWO** is responsible to the G-7 and coordinates directly with the

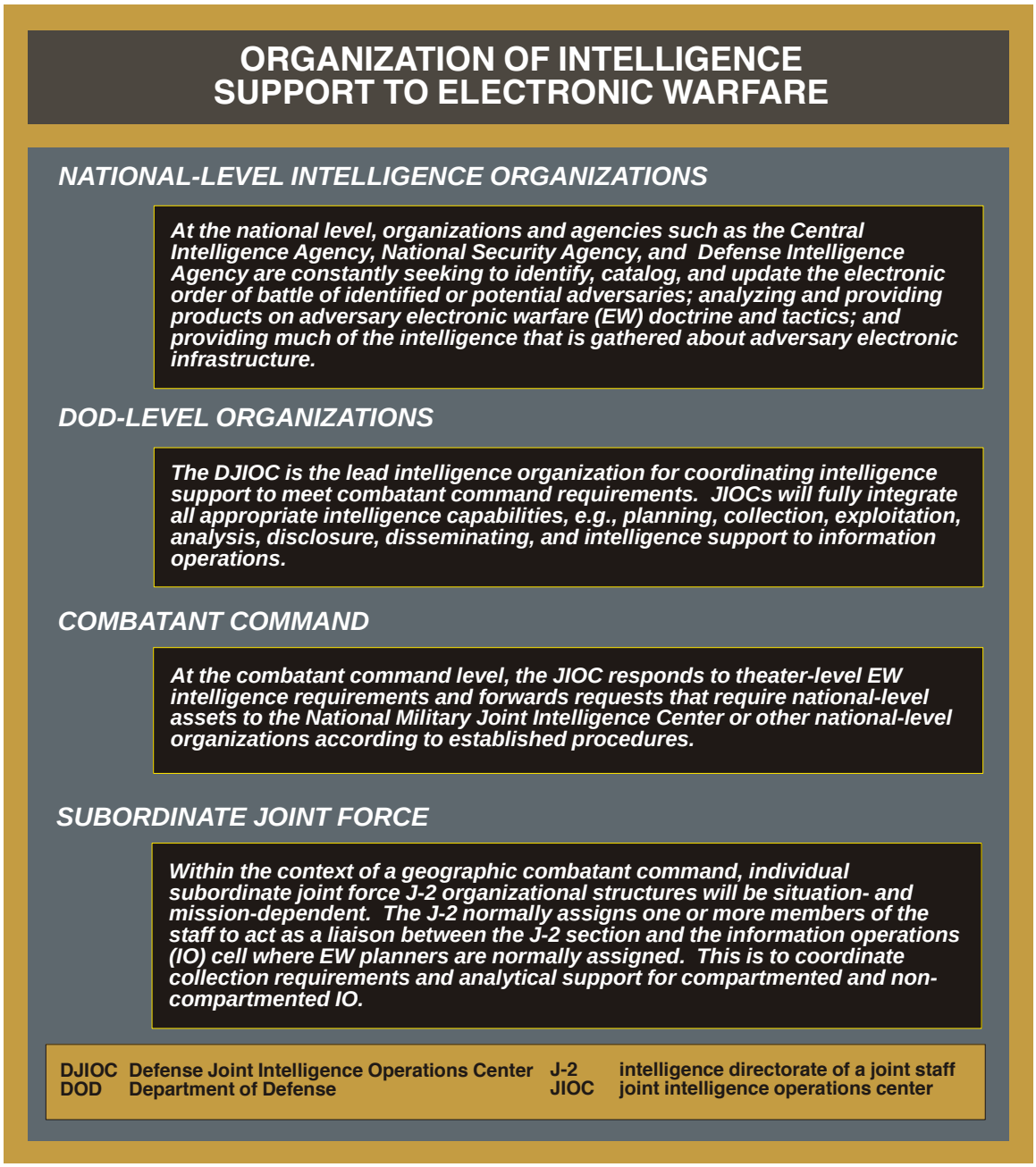


Figure II-1. Organization of Intelligence Support to Electronic Warfare

component fire support coordinator, G-2 (targeting and analysis and control element), for planning, synchronizing, coordinating, and deconflicting EW actions.

b. **Marine Corps. Marine EW assets are integral to the Marine air-ground task force (MAGTF).** 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 Marine tactical EW squadrons (VMAQs). The RADBN is organized and equipped to conduct tactical SIGINT, ground based ES, ground based EA, and communications security (COMSEC) monitoring and analysis 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 the 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. The EWCC will have a resident EWO who is responsible for ensuring that all EW plans are included in the IO annex. The MAGTF IO officer in charge of the IO cell assumes overall responsibility for the planning and coordination of EW operations.

For more information about EA-6B employment, see Field Manual (FM) 90-39, Marine Corps Reference Publication (MCRP) 3-22A, Navy Warfare Publication (NWP) 3-01.4, and Air Force Tactics, Techniques, and Procedures (Instruction) (AFTTP [I]) 3-2.4, "Multi-Service Tactics, Techniques, and Procedures for EA-6B Employment in the Joint Environment

c. **Navy.** Below the joint force maritime component commander or Navy component commander, Navy forces are normally organized according to the **composite warfare commander doctrine**. Within this doctrine, the IO warfare commander (IWC) is responsible for the **integration of the various core capabilities of IO**, including EW, into naval and joint operations. An EWO is normally assigned to the IWC's staff to carry out specific staff coordination and integration functions associated with EW's role in the IO effort. EW is planned and conducted by the EWO under the direction of the IWC. The IWC oversees the execution of the coherent EW and IO plan and control of associated systems. EW execution requires continual monitoring by EW staff personnel and is delegated to the EW control ship. Embarked airborne EA assets, such as the EA-6B Prowler, are under the operational control of the strike warfare commander, who is also the carrier battle group air wing commander (CVWC) or the more traditional "carrier air group" (CAG). When executing strike operations, air wing EA assets will remain under the operational control of the CAG, and will come under the tactical control of the airborne mission commander. When participating in joint or coalition operations, the JFACC will coordinate with CAG operations for scheduling air wing assets in the air tasking order (ATO). When airborne assets are assigned ashore as part of an expeditionary force, they will be under the tactical control of the JFACC. It should also be noted that Navy airborne ES is primarily provided by shore-based aircraft such as the EP-3E Aries II. These aircraft will be assigned to the tactical control of either the battle group IWC or the JFACC as scheduled by the ATO.

d. **Air Force.** Within the Air Force component, dedicated EW support assets are under operational control of the **commander, Air Force forces (COMAFFOR)**. Within the COMAFFOR headquarters, the responsibility for EW lies within the operations directorate (A-3) and plans directorate (A-5). **Functional planning, directing, and control of Air Force EW assets, however, are normally conducted by the JFACC** through the joint air operations center's EWCC. The EWCC coordinates with the IO specialty team or the IO cell to integrate EW within other IO functions and to develop/monitor EW plans and operations in support of the JFC. The EWCC consists of an EW plans element and an EW operations element. In response to the ATO, wing and unit level staffs and individual aircrews develop the 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, whose employment the JFACC carefully rations through the ATO process.

Air Force EA and ES systems, however, are normally assigned to or integrated into Air Force wings or squadrons. 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 operational area. The defensive systems officer, EWO, and electronic combat officer also plan available EW equipment employment and oversee radar warning receiver and EW systems reprogramming. *Appendix F Service Perspectives Of Electronic Warfare provides more detailed discussion on how the services view EW.*

Intentionally Blank

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 aspect of modern military operations that must be **fully integrated** with other aspects of joint operations in order to achieve its full potential for contributing to an operation's objectives. Such integration requires **careful planning**. EW planners must coordinate **their planned activities with other aspects of military operations** which use the EMS as well as third party users of the spectrum that EW does not wish to disrupt. Coordination of military use of the spectrum is largely a matter of coordinating with other staff functions (primarily the J-2 and J-6) and components (to include allies and coalition partners) which rely on the EMS to accomplish their mission. Coordination of EW activities, in the context of third party use of the EMS, is largely a matter of EMS management and adherence to established frequency usage regimens and protocols.

b. Like other aspects of joint operations, joint EW is **centrally planned and directed and decentrally executed**. Since the Military Services provide most US EW assets available in joint operations, **Service component EW planners must be integrated into the joint planning process**. The JFC may delegate control of EW operations to a component commander or lower echelon. However, such delegation does not eliminate the requirement for joint and/or multinational coordination of EW operations. This chapter provides guidance on the joint EW planning process, discusses some of the considerations for planning EW in support of military operations, provides guidance on preparation of the EW tab to appendix 3 (Information Operations) to annex C (Operations) of the OPLAN and/or OPORD, and briefly discusses some of the automated decision aids that may be used to assist with planning joint EW.

2. Electronic Warfare Planning Considerations

a. **EMS Management.** Since EW activity takes place in the EMS, joint **EW planners must closely coordinate their efforts** with those members of the joint staff who are concerned with managing military use of the EMS. Figure III-1 shows the steps involved in JFMO spectrum management responsibilities. Figure III-2 shows a flow diagram of frequency management planning. For operations within a CCDR's AOR, the subordinate JFCs follow this guidance as amplified by the CCDR. The commander, JTF coordinates and negotiates modifications necessary for a specific JTF situation with the CCDR's staff. Joint EW planners should establish and maintain a close working relationship with the frequency management personnel. A critical management tool to ensure effective use of the EMS during military operations is 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 will be limited to the minimum number of frequencies necessary for friendly forces to accomplish JTF objectives.

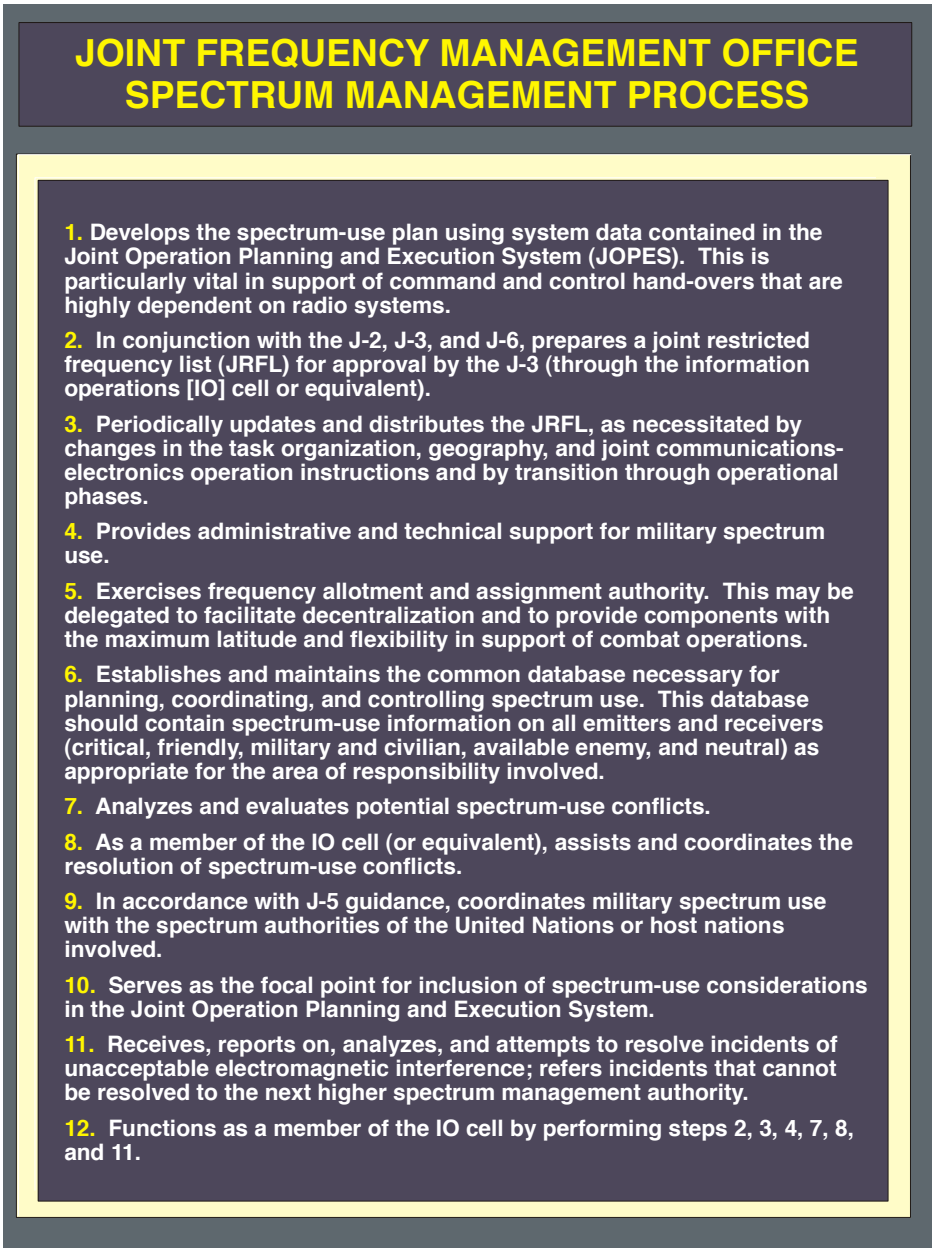


Figure III-1. Joint Frequency Management Office Spectrum Management Process

The JRFL is published, distributed and maintained by the J-6, typically through the JFMO/JSME, based upon inputs from the J-2, J-3 and J-6, with J-3 being the release authority for the coordinated listing. Upon release, the JRFL will be used to preclude listed frequencies from being interfered with during EW missions.

The JSC can support the JRFL development process by providing training on the preparation of the JRFL during exercises and onsite augmentation to assist the JFMO with JRFL preparation during the initial phases of an operation. EW planners should coordinate with the combatant command JFMO or JTF JSME to determine if JSC assistance is required early in the planning process.

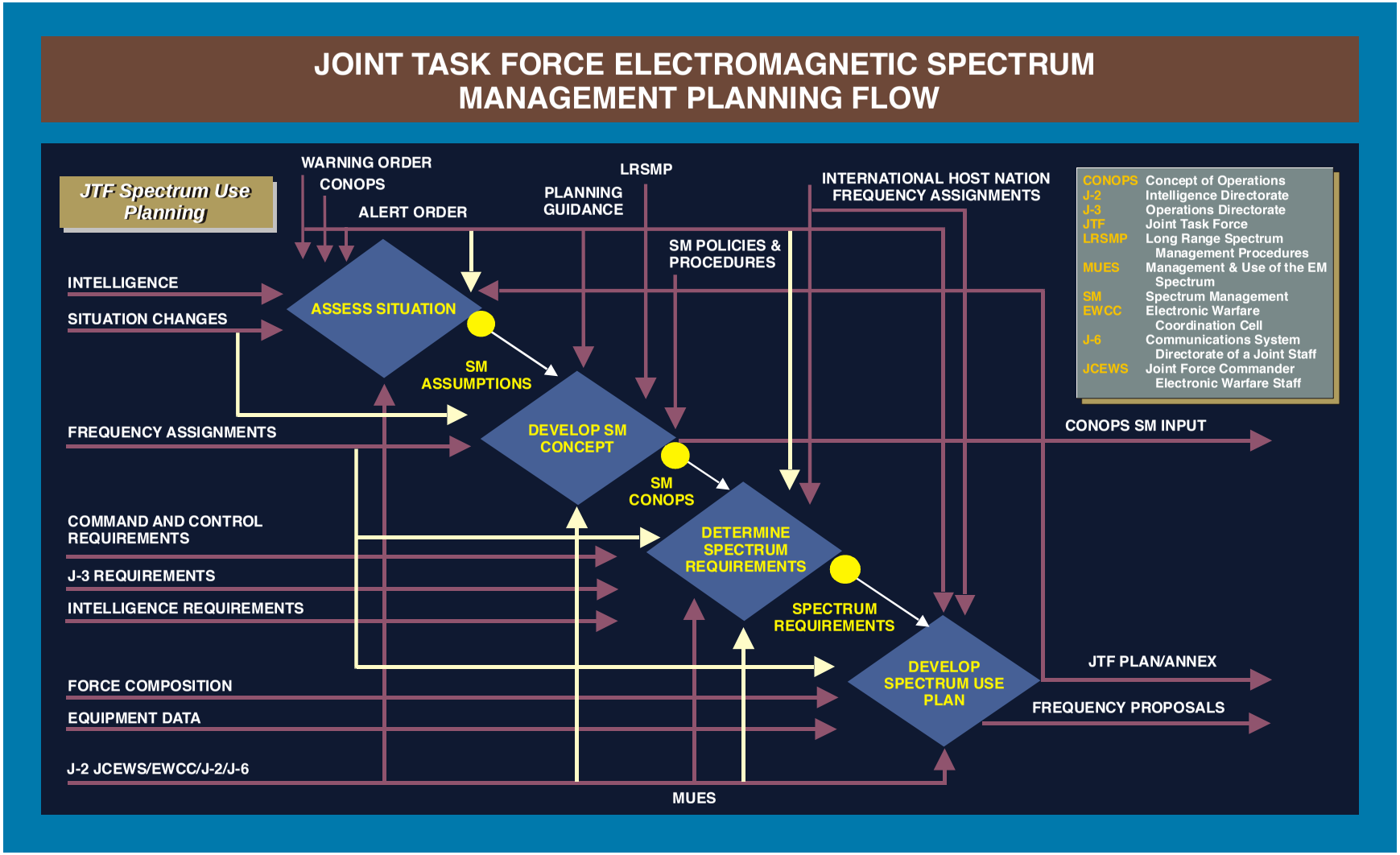


Figure III-2. Joint Task Force Electromagnetic Spectrum Management Planning Flow

See Appendix B, "Electronic Warfare Frequency Deconfliction Procedures," for frequency deconfliction procedures and information on generating the JRFL. For exercises conducted in the US or Canada, EW planners must consult CJCSM 3212.02, "Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises," for planning and guidance procedures. CJCSM 3320.01B, "Joint Operations in the Electromagnetic Battlespace," provides more detailed guidance in EMS management. For more information on the JSC, see Appendix C, "Joint Spectrum Center Support to 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 that **EW support to SEAD missions is integrated into the overall EW plan**.

For more information about SEAD, see JP 3-01, "Countering Air and Missile Threats."

c. **EW Support Against a Nontraditional Threat.** The global war on terrorism has shown the enemy's ability to use commercial electronic communications means in a number of nontraditional ways ranging from ad hoc cueing networks to detonation means for improvised explosive devices. EW support to counter these efforts should be integrated into the overall EW plan.

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 hostile EM environment. Service reprogramming efforts must include coordination with JFCs to ensure that those reprogramming requirements are identified, processed, and implemented in a timely manner by all affected friendly forces.

See Appendix D, "Electronic Warfare Reprogramming," for more information about 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 electromagnetic 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** (such as, MILDEC, OPSEC, and signals security) that are conducted, wholly or in part, within the EMS.

(2) Effective electronic masking of joint military operations involves the proactive management of all friendly radiated electronic 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 two variables:

(a) the assessed adversary ES and SIGINT collection capability (or access to third party collection); and

(b) the degree to which the electronic 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) providing adequate electronic masking guidance to component commands through OPLANs and OPORDs; and

(b) planning and implementing appropriate electronic masking measures within the joint force headquarters.

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

(a) Assess the 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 tactics, techniques, and procedures; and

(d) Alert component commands at the earliest opportunity of the need to be prepared to implement electronic masking measures. This will afford these commands with the necessary lead time to augment their own 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:

(1) to **establish standards and practice procedures** that allow for integrated planning and execution of EW operations (including joint EW); and

(2) to **exchange EW information in a timely and routine fashion.** This exchange may be conducted in either non real time or in 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 ES, EA, and EP, 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, with 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, and federal laws, LOAC, and theater ROE that may affect EW activities. These laws, rules, and guidelines are especially critical during peacetime operations when international and domestic laws, treaty provisions, and political agreements may affect mission planning and execution. Commanders must seek legal review during all levels of planning and execution of EW activities, to include planning of the theater ROE. This can best be accomplished by having a legal advisor as a member of the IO cell.

h. **Uninterrupted Consequences. EW planners must consider unintended consequences of EW operations. Friendly EA could potentially deny essential services to a local population which 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 and should coordinate military spectrum use with spectrum authorities of host nation when conducting multinational operations or exercises. The J-6 spectrum manager can provide this analysis to the JCEWS/joint EWCC to better determine the impact of EW operations and better define the consequence management value of EW missions.

i. **Meteorological and Oceanographic (METOC) Considerations.** EW planners must consider the effects of atmospherics and space weather on available EW systems, both friendly and enemy. 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 global positioning systems (GPS). Some atmospherics 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.

3. Joint Electronic Warfare Planning Process

In order to be fully integrated into other aspects of a planned operation, joint EW planning is conducted through the IO cell beginning as early as possible and is coordinated with other aspects of the plan throughout the joint operation planning process. Figure III-3 shows the integration of EW into the joint planning process. Once a planned operation has commenced, EW planners must **monitor execution of the plan** and be prepared to **assist with coordination** of the plan as well as 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 that requirements of ROE, legal authorities, and LOAC are met.

d. Review the contribution EW can make to help operate and defend the GIG with the NETOPS community. This will be done through the J-6 representative assigned to the JCEWS or EWCC staff.

e. Review the contribution which EW can make to the IO effort with other "capability level" planners (such as PSYOP, MILDEC, computer network attack and CND planners) and determine what level of EW platform support they expect to need during the operation.

f. Review with intelligence planners the type of ES platforms, capabilities, and products available to support the operation. Intelligence gain/loss analysis of EW actions should start early and be frequently reviewed throughout the planning and execution phases of an operation.

g. Consult with Service and functional components as well as multinational EW planners, wherever the most current expertise in the capabilities and employment of EW platforms resides, in order to understand the full range of capabilities that EW can contribute to IO.

h. 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 (such as those provided through the Status of Readiness and Training System for US forces) for this information. Service and functional components and multinational planners should be consulted to augment automated information.

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

j. Recommend to the IO officer (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.

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

l. Recommend staff augmentation in accordance with staff procedures from component, supporting, and multinational forces as necessary to assemble the necessary staff to conduct EW planning.

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

n. During crisis action planning, evaluate each course of action (COA) considered with respect to EW resources required and the EW opportunities and vulnerabilities inherent in the COA.

4. Electronic Warfare Planning Guidance

Planning guidance for EW is **included as the EW tab 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 (JOPES) EW guidance as a tab to the IO guidance. CJCSM 3122.03B, "Joint Operation Planning and Execution System Vol II: (Planning Formats)" is the source documents that should be consulted for detailed information about OPLAN development.

a. **Planning Factors.** Development of the EW portion of the OPLAN requires consideration of a number of diverse factors about the proposed operations. Some of these **planning factors** include the following.

(1) 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 EM interference considerations. Once identified, these requirements should be entered into the JRFL under appropriate categories (e.g., TABOO).

(2) Identification of COMSEC and electronic security measures necessary to deny OPSEC indicators to enemy passive-EM sensors.

(3) Determination of what prior coordination and precautions will be necessary when conducting EA in order to ensure continued effective ES. Development of the JRFL is a critical preliminary step to ensuring deconfliction of EA and ES activities. Coordination and identification of specific resources required for interference deconfliction.

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

(5) Coordination and establishment of procedures to ensure timely fulfillment, including tactical real-time dissemination.

(6) Review of ROE and applicable law to determine what authorities are needed or what restrictions (if any) apply to EW operations.

b. **EW plans should:**

(1) **Identify the desired EM profile** selected by the commander for the basic concept of operations and **provide EMCON guidance** to commanders so that the desired EM profile is realized;

ELECTRONIC WARFARE CELL ACTIONS AND OUTCOMES AS PART OF JOINT PLANNING

PLANNING PROCESS STEPS	EW CELL PLANNING ACTION	EW CELL PLANNING OUTCOME
Planning Initiation	Monitor situation. Review guidance and estimates. Convene EW cell. Ensure EW representation within IO cell. Gauge initial scope of the EW role. Identify organizational coordination requirements. Initiate identification of information required for mission analysis and COA development. Validate, initiate, and revise PIRs/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 MOEs and MOPs. Analyze EW capabilities available and identify authority for deployment and employment. Identify relevant physical, informational and cognitive properties of the information environment. 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 CCIRs.	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.	N/A
Plan or Order Development	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 TPFDD refinement to ensure the EW force flow supports the CONOPS.	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.

CCIR	Commander's Critical Information Requirement	MOE	Measure of Effectiveness
COA	Course of Action	MOP	Measure of Performance
CONOPS	Concept of Operations	PIR	Priority Intelligence Requirement
EW	Electronic Warfare	RFI	Request for Information
IO	Information Operations	TPFDD	Time-Phased Force and Deployment Data

Figure III-3. Electronic Warfare Cell Actions and Outcomes as Part of Joint Planning

(2) Identify EW missions and tasks to Service or functional component commanders to enable them to plan resources required and associated 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, and computer networks. Specify EP guidance necessary to ensure effective operations during combat.

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.** Automated 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.

(1) There are a **large number of databases** available to military planners. Some of these databases are maintained by the Services, others by various intelligence community agencies or other DOD organizations, and others by allied organizations. Still other databases may be maintained by academic or private (profit or nonprofit) organizations. In general, **friendly data is maintained by Service, government contractor, and allied organizations**. **"Threat" data is compiled by intelligence organizations**. Compilation of accurate technical data into one place is 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 that data is organized into fields in a database and the level of detail (such as number of decimal places certain technical data is carried out) are functions of what the data is used for and the cost associated with compiling and maintaining each database.

(3) The sources of data being used for planning should be a topic of coordination among EW planners. The use of the E-Space portal as the common database source is recommended. If necessary, joint planners should provide guidance about what sources of **automated data should be used for specific EW planning purposes**. Planners should request that organizations that maintain important sources of EW data update their databases (or specific parts of them) more frequently than normal when planning specific operations. 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 important source of valuable information.

b. **Planning Process Aids.** There are **several automated aids** available that assist in the planning process and others under development. These include aids that **automate the JOPES planning process** or **OPLAN development, automated frequency management tools**, and others that assist with the **integration of different elements and activities of IO**. The type of automated

software used in the JOPES planning process or OPLAN development will probably be directed by some other section of the staff. Use of automated tools to integrate different elements of IO will normally be determined by the IO officer. EW planners should ensure that any EW planning input developed separately from such systems are created in a format that is compatible (electronically transferable) to designated planning tools. EW planning input from subordinate and supporting commands should specify 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 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 such energy have become widespread in EW planning. However, the accuracy, speed, and flexibility of these tools greatly depend on the accuracy of the data provided to the tool and the sophistication of the software and hardware used to manipulate the data. Reliance on the output of such tools can ultimately be a matter of life and death in combat if the tools are used to plan the location of EW assets or avoid hostile emitters. 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 must rely to judge the strengths and weaknesses of different modeling tools and determine what is and is not an appropriate use of such systems.

Appendix E, "Electronic Warfare Modeling," gives additional guidance of EW models and their use.

d. **Reachback Resources**. If EW planners don't have the automated planning tools required onsite, reachback support is available. For joint EW planners, reachback support is available from the E-Space Analysis Center at Fort Meade, Maryland, the JIOWC in San Antonio, Texas and the JSC in Annapolis, Maryland. Further information on the JSC is located in Appendix C. E-Space provides an initial capability for one-stop ELINT support to the tactical EW user, capability to query EM information across multiple databases, and collaboration through data sharing, forums and access to EW experts. E-Space has a query, analysis and collaboration tool that supports combat operations, combat and crisis action planning, indications and warning, and exercise activities. Component planners can utilize reachback support available through the Services as discussed in *Appendix F, Service Perspectives of Electronic Warfare*.

Intentionally Blank

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

A certain amount of coordination is part of the planning process. However, once a plan has been approved and an operation is commenced, the preponderance of EW staff effort shifts to the coordination necessary to ensure that EW actions are carried out as planned or modified to respond to the dynamics of the operation. Areas of concern that normally require continual monitoring on the part of EW staff personnel include **EW asset allocation, EMS management, and emerging operational issues** that require modification to plans or procedures. Normally, this monitoring is performed by **personnel on watch in the joint operations center (JOC)**. Such watch personnel, stationed at an IO (or separate 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 on which EW staff personnel should focus to accomplish such coordination.

2. Joint Coordination and Control

a. Joint EW Organizational Coordination

At combatant commands and subordinate unified commands, the J-3 IO division is primarily responsible for the EW coordination function. The EW section of the IO staff should engage in the full range of EW functions to include peacetime contingency planning, the day to day planning and monitoring of routine theater EW activities, and crisis action planning in the run-up to contingencies in preparations for EW as part of emergent joint operations. The EW section operates under the direction of J-3 IO division and coordinates closely with other appropriate staff sections and other larger 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. Services should begin component EW planning and activate their EWCCs per CCDR or Service guidelines. When the scope of the contingency becomes clearer, the command EWO may request that the JFC standup a joint EWCC. The designated joint EWCC would request additional augmentation from other JFC components to form a representative and responsive EW planning and execution organization. To avoid confusion with joint EWCC, component EWCCs are normally called EW elements.

b. Management of the Electromagnetic Spectrum

(1) The JFMO assessment of the operational area EME — conducted during the planning phase — constitutes a best guess based on information available at the time. Following deployment and

buildup, overlaying joint force EM emissions on the existing operational area EME will create a different environment. Further, this environment will constantly change as forces redeploy and as C2, surveillance, weapons systems, and other spectrum-use applications realign. Since EW is concerned with **attack (EA), EP, monitoring and exploitation** of the EMS, EW staff personnel have a major role to perform in the **dynamic management** of the spectrum during operations. Figure IV-1 shows the execution of frequency use deconfliction during an operation. A **comprehensive and well-thought-out JRFL and EMCON plan** are normally the two tools that **permit flexibility of EW actions** during an operation without compromising friendly use of the EMS. Some of the **coordination actions related to EMS** that EW staff personnel should consider include:

(a) monitoring compliance with the JRFL and EMCON plan by friendly EW assets;

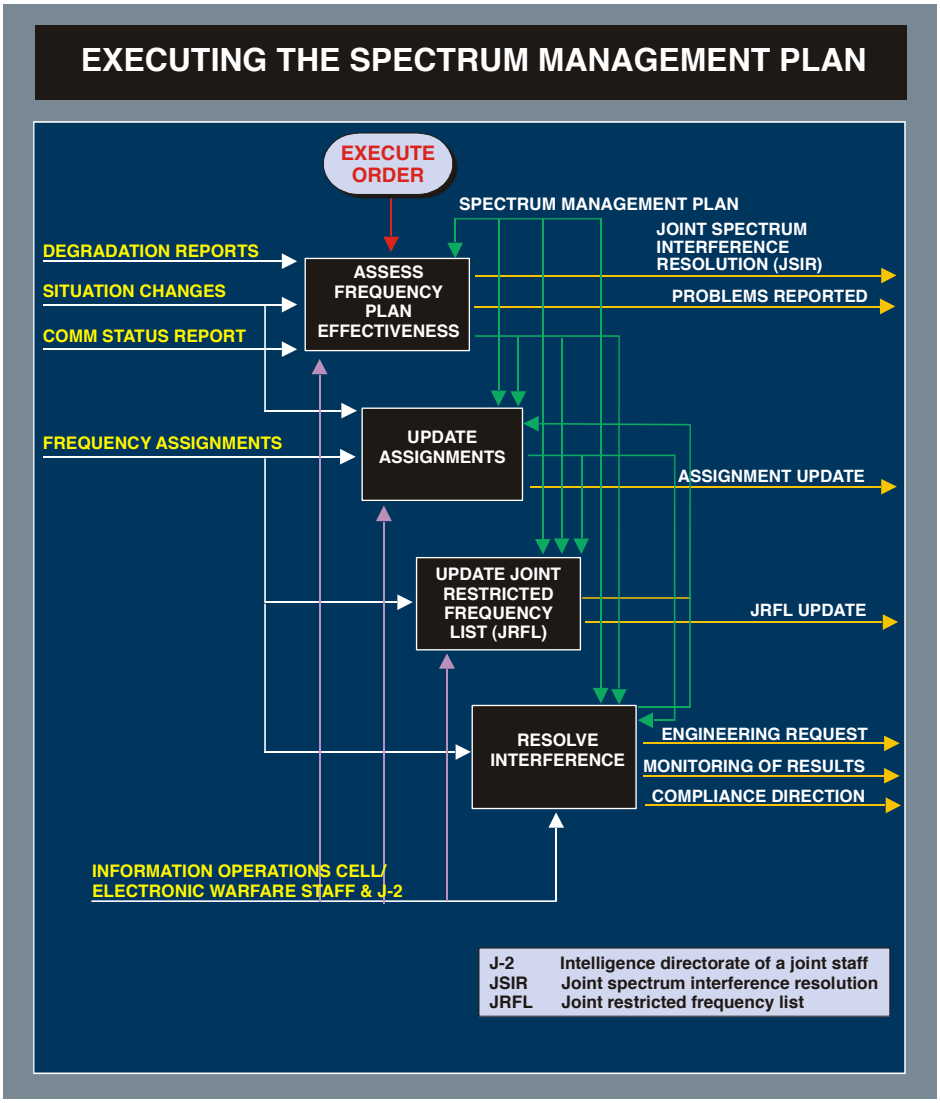


Figure IV-1. Executing the Spectrum Management Plan

(b) recommending changes to operations in the EMS based on emerging frequency deconfliction requirements;

(c) establishing employment guidance and recommending supplemental ROE for EA employment, and ensuring that the EA plan is in compliance with the standing rules of engagement, Secretary of Defense approved ROE and any existing theater specific ROE;

(d) establishing a chattermark plan to ensure communications net availability in the presence of jamming, intrusion, or interference; and

(e) establishing and designating a JCA to conduct on station coordination, employment, targeting, and deconfliction of EA and ES assets.

Appendix B, "Electronic Warfare Frequency Deconfliction Procedures," provides additional detail about EW frequency deconfliction.

(2) Jamming Control Authority. The JCA serves as the senior jamming authority in the operational area and develops guidance for jamming on behalf of the JFC. JCA responsibilities include:

(a) Participating in development of the JRFL.

(b) Ensuring compliance with the approved JRFL.

(c) Validating and approving/denying "cease buzzer" requests.

(d) Maintaining situational awareness of all jamming capable systems in the AOR.

(e) Acting as the JFC's executive agent for decisions on EW intelligence gain/loss recommendations.

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

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

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

c. **Coordination Between the Subdivisions 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:

(1) monitoring 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; and

(2) monitoring input to the reprogramming process submitted by components and coordinating urgent reprogramming actions on the basis of recommendations from Service reprogramming centers.

d. **Coordination with the Core, Supporting and Related Capabilities of IO.** EW can stand alone or enable, support, and enhance the other capabilities that are part of, support, or are related to IO. EW is viable across the full range of military operations. EW is replete with opportunities to support IO missions independent of "traditional" EW roles. Integration of EW (and the other capabilities associated with IO) is necessary if planners are to realize potential synergies between these capabilities and the effects they can generate to increase joint force effectiveness.

(1) One of the primary functions of the IO cell is to **deconflict and coordinate the various capabilities that are associated with IO**. Most of these capabilities depend on, use, or exploit the EM spectrum for at least some of their functions. The deconfliction and coordination of EW in an operation is a continuous process for the IO cell and the JCEWS/EWCC.

(2) Besides EW, the IO core capabilities include PSYOP, OPSEC, MILDEC, and CNO. Together these five capabilities, used in conjunction with supporting and related capabilities, operate within the information environment to provide the JFC an operational advantage by achieving 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. JP 3-13, "Information Operations" provides additional detail.

(a) **Electronic Warfare and PSYOP.** PSYOP activities often use the EMS to broadcast their message to target audiences using platforms such as COMMANDO SOLO. EW activities support PSYOP by, when appropriate, degrading the adversary's ability to see, report, and process information and by isolating the target audience from information. EW planners must be aware of the potential to interfere with PSYOP efforts to convey information to adversaries or foreign target audiences. PSYOP supports EW by broadcasting PSYOP products on adversary frequencies and by developing products for broadcast on other Service's EW assets. If necessary and approved, EW can prevent reception of PSYOP broadcasts. PSYOP platforms and units depend on information gathered through ES to **warn them of potential threats and provide feedback about reaction** to PSYOP broadcasts and other activities. PSYOP units rely on effective EP efforts to prevent adversary EA activities or other inadvertent EMI from disrupting their efforts. Coordination of PSYOP 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, PSYOP and EW staff personnel should deconflict their operations and frequency use on a regular basis.

JP 3-53, "Doctrine for Joint Psychological Operations," provides additional detail.

(b) **Electronic Warfare and OPSEC.** EA supports OPSEC by degrading adversary electromagnetic ISR operations against protected units and activities. ES can support the OPSEC effort by providing information about adversary capabilities and intent to collect intelligence about **essential elements of friendly information (EEFIs)** 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 EEFIs 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.

JP 3-13.3, "Operations Security," provides additional details.

(c) **Electronic Warfare and Military Deception**. EW supports MILDEC by using EA/ES as deception measures; by degrading adversary capabilities to see, report, and process competing observables; and by 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 IO 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. At the same time, coordination within the JTF staff must occur so that 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 direction finding 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/EP/ES capabilities. EW planners should ensure that EM frequencies necessary to support deception plans are accounted for in spectrum 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.

JP 3-13.4, "Military Deception," provides additional details.

(d) **Electronic Warfare and Computer Network Operations**. CNO may be facilitated and/or enabled through EW. The increasing prevalence of wireless internet and telephone networks in the operational environment has created a wide range of opportunities and vulnerabilities when EW and CNO tactics, techniques and procedures are used synergistically. While physical access to a particular computer network may be limited, electronic access may prove the key to successful computer system penetrations.

(e) **Electronic Warfare and Information Assurance**. EW supports IA by using EP to protect equipment. IA is concerned with measures that protect and defend information and information systems and the majority of the measures involve the use of the EMS. Consequently, EW is inextricably bound to IA. IA supports EW by ensuring EW assets are available. EP tactics, techniques, and procedures assist in assuring the availability, integrity, authentication, confidentiality, and nonrepudiation of measure which IA seeks to protect and defend. EA tactics, techniques, and procedures assists in compromising those same qualities which adversary IA seeks to protect and defend. EMC resolution and spectrum management procedures assist IA in overcoming the problem of electronic fratricide.

(f) **Electronic Warfare and Physical Attack**. EW supports physical destruction by providing target acquisition through ES and by destroying or degrading susceptible assets with EA. Physical destruction supports EW by destroying adversary C2 targets and by destroy adversary electronic 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 EME of the operational area for targeting and threat avoidance planning. Standoff munitions and antiradiation ordnance are major assets in any operation and may, for example, be used to selectively destroy adversary emitters in support of military deception, SEAD, OPSEC, and PSYOP efforts. The employment of antiradiation weapons must be carefully planned and deconflicted to prevent the engagement of unintended targets. Destructive DE weapons are being researched and developed and will likely come to be an important part of the physical destruction actions of joint operations. 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 electromagnetic 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 destruction 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 the physical destruction actions during combat operations.

JP 3-09, " Joint Fire Support," provides further details.

(g) **Electronic Warfare and Physical Security**. EW supports physical security by using EP to safeguard communications used in protecting facilities. Physical security supports EW by safeguarding equipment used in EW. In an era when improvised explosive devices with radio controlled electronic detonators have become ubiquitous, EW and physical security have become closely intertwined. Operations in Iraq have provided many innovative uses of EW capabilities to preempt and disrupt threats that may be using part of the EMS to attack coalition ground forces.

(h) **Electronic Warfare and Counterintelligence**. There are many electronic aspects to CI. CI supports EW by providing intelligence information for use in electronic countermeasures. However CI personnel are normally self sufficient in carrying out the electronic tactics, techniques, and procedures associated with their duties. 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 IO and J-2 CI staff divisions must establish battle rhythm and/or tactics, techniques, and procedures to monitor and deconflict JRFL and other EW activities that either support or potentially jeopardize human intelligence activities.

(i) **Electronic Warfare and Combat Camera**. 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.

(j) **Electronic Warfare and Public Affairs**. The relationship of EW to PA is primarily one of deconfliction. News media personnel in the AOR 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.

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

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

e. **Legal Support to Electronic Warfare**. Legal review is required to ensure EW operations are in compliance with existing international law, host-nation agreements and arrangements, US policy, DOD publications, federal laws, LOACs, theater specific and ROE.

See JP 1-04, "Legal Support to Military Operations," for further details.

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 theater exploitation of captured material and interrogation of captured personnel respectively. The EW staff should establish EW exploitation and interrogation requirements through the J-2 representative of the IO cell (or via other established procedures) to take advantage of the opportunities that may be realized through the exploitation of captured equipment and the interrogation of captured personnel.

For additional information see Appendix G, JP 2-01, "Joint and National Intelligence Support to Military Operations."

3. Component Coordination Procedures

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 components to determine how they are organized and what procedures are being used by functional component forces.

a. **Army Coordination Procedures.** The Army Service component command G-3 IO division or G-7, plans, coordinates, and integrates EW requirements in support of the JFC's objectives. At corps level, coordination with both the G-7, 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 headquarters. Conversely, other components requiring Army EW support initially coordinate those support requirements with the EW officer at the Army forces headquarters or tactical operations center. This coordination is normally done in person or through operational channels in 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 corps or division level. Air Force and Army coordination will normally **flow through the battlefield coordination detachment** at the Air Forces air and space operations center. EW staffs at higher echelons monitor the EW requests and resolve conflicts when necessary. Also, the G-7:

(1) Provides an assessment of EW capabilities to other component operation centers;

(2) Coordinates preplanned EW operations with other Service components; and

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

b. **Marine Corps Coordination Procedures.** 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**. 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 service support 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; and

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

c. **Navy Coordination Procedures.** The Navy component commander is normally the numbered fleet commander for a theater. The IO cell (typically the N39 code) is responsible for all Navy EW efforts and provides coordination and tasking to task forces assigned. The IWC at the carrier strike group or expeditionary strike group 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; and

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

NOTE: Airborne EA and ES assets, such as the EA-6B Prowler, when employed in a strike support role will be the responsibility of the strike warfare commander. The strike warfare commander is the CVWC or the more traditional CAG. The CAG is responsible for coordinating integration of air wing assets into the ATO with the JFACC.

d. **Air Force Coordination Procedures.** Air Force requirements for other component EW support are established by the **COMAFFOR's A-3** (or equivalent operations directorate) **or A-5** (or equivalent plans directorate), in coordination with the director for intelligence. The A-3 or A-5 staff translates requirements for other component EW support into tasks and coordinates those tasks with the component EW agency. In addition, the A-3 or A-5 staff officer:

(1) Provides an assessment of Air Force capabilities to other component operation centers; and

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

e. **Special Operations Forces Coordination Procedures.** The JFSOCC will establish a **JOC** to serve as the task integration and planning center for joint force special operations (SO). Requirements from SO 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.

See JP 3-05, "Doctrine for Joint Special Operations," for further details.

f. **United States Coast Guard (USCG) Coordination Procedures.** The USCG operates as an independent agency in the Department of Homeland Security. Upon the declaration of war or when the President directs, the USCG will transfer to the Department of the Navy. Joint operations may include USCG assets that may 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 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 that are 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 objectives.

JP 2-01, "Joint and National Intelligence Support to Military Operations," and its classified supplement provide additional details.

CHAPTER V
MULTINATIONAL ASPECTS OF ELECTRONIC WARFARE

"The United States must. . . strengthen alliances to defeat global terrorism and work to prevent attacks against us and our friends."

The National Security Strategy of the United States of America 2006

1. Introduction

Operations IRAQI FREEDOM, ENDURING FREEDOM, and ALLIED FORCE demonstrated the requirement for US forces to be able to integrate operations with allied and coalition nations. US planners must be prepared to integrate US and allied or coalition EW capabilities into an overall EW plan, be able to provide allied or coalition nations with information concerning US EW capabilities, and provide EW support to allied or coalition nations. As in joint operations, **EW is an integral part of multinational operations**. In US-led operations, the doctrine within this publication should be used as the basis for all EW activities within the multinational force (MNF). However, the planning of MNF EW is made more difficult because of **ill-defined security issues, different crypto 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 resolved by **adherence to standard NATO 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 Standardization Program (ABCA) and the Air and Space Interoperability Council (ASIC) made up of the members of ABCA 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. **Current NATO EW doctrine is consistent with US EW doctrine.** Geographic combatant commanders should provide guidance to the MNF commander (MNFC) (if the MNFC is a US Service member) within their joint OPLANs on the release of classified material to allied and/or coalition forces. 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 Regulation 60-28, *International Military Intelligence Relationship*.

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 J-3, the IO cell or, when established, the Combined EWCC. It should be

recognized that the IO cell (or EWCC) assumes responsibilities set forth in Chapter II, "Organizing for Joint Electronic Warfare."

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 J-3 has primary responsibility for the planning and integration of EW operations with other combat disciplines.

(2) **Staff EW Officer.** The staff EWO's primary responsibility should be to ensure that 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 EW officer should be responsible for the following:

(a) Ensure that all component commanders of the MNF **provide adequately trained EW officers** to be members of the MNFC EW staff. The chain of command should be established by the J-3. The rationale for augmentee status is that the allied and/or coalition officers must be full members of the multinational EW planning cell and responsible to the chain of command. They must 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 liaison officers with allied and/or coalition commands to ensure that the MNFC's EW **plans and procedures are correctly interpreted**.

(c) **Integrate allied and/or coalition EW officer augmentees** at the 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 allied and/or coalition forces.

(e) Integrate allied and/or coalition C2 requirements into the multinational and JRFL.

(f) At the earliest possible stage, provide allied and/or coalition forces with current US EW doctrine and planning guidelines.

(3) **Allied and/or Coalition EW Officers.** Allied and/or coalition commanders should assign adequately trained EW officers to the MNF EW planning cell. These officers should:

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

(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 involved in the MNF.

3. Multinational Electronic Warfare Coordination Cell with Allied Forces

Although NATO's EW, policy contained in Military Committee (MC) 64, "NATO Electronic Warfare Policy," is largely based on 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 center (S/EWOC)," provides the operational requirement and the operational procedures for an interoperable S/EWOC 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 as well as 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 Electronic Warfare Core Staff (NEWCS)" describes the functions of the NEWCS. The primary functions of the NEWCS would be to provide a core staff to augment JFC EWCCs, serve as the primary EWCC element for the NATO response force and provide an operational planning capability for NATO operations and exercises. JFC EWCCs and primary EWCC element for the NATO response force are to be augmented by those nations contributing to the operation with assets using EW. The NEWCS must also provide 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 liaison officers. However, precedent exists; maritime forces have for many years worked multinational issues with little difficulty. Allied Tactical Publication (ATP) 8A, "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(A), "Allied Joint Operations Doctrine," includes a chapter on EW and the EWCC. NATO members invariably base their national EW doctrine on that agreed within NATO MC 64. However, there is a need to ensure that the most recent, releasable, US EW publications are provided to supporting allied and/or coalition forces. NATO has also established a NATO Emitter Database to exchange information about member countries' and nonmember countries' electronic emissions and facilitate the coordination of EW.

4. Multinational Electronic Warfare with Australian Armies Standardization Program and Air and Space Interoperability Council Member Nations

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

5. Multinational Electronic Warfare Coordination Cell with Other Allies or Coalition Partners

The principles expressed above are equally applicable to other allies and/or coalitions. The MNFC should include EW officers from supporting allied and/or coalition forces 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 allied and/or coalition units.

6. 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-51, "EW in the Land Battle," MC 101/10, "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 in place procedures within the major NATO commanders' precautionary system that can be put into effect during time 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, through the EW intelligence support organization and the theater joint analysis center or theater JIOC, should ensure maintenance of an up-to-date EOB. Allied and/or coalition staff officers should be included in turn, and should ensure that their national commands provide appropriate updates to theater joint analysis in discussions on theater EOB. They, in turn, should ensure that 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/S/EWOC, 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 officer should be aware of reprogramming efforts being conducted within the MNF. The EWCC officer 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 allied and/or coalition commands should provide the EWCC officer 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) Bilateral agreements on reprogramming support for allied and/or coalition units employing US EW equipment, to include any agreement on flagging support.

(4) Bilateral agreements 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 foreign military sales reprogramming organizations, that identify deficiencies in the allied and/or coalition country's EW equipment and their request for reprogramming support. In turn, the EWCC officer should ensure that allied and/or coalition 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 allied and/or coalition units within the MNF to **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.

d. **US EW Planning Aids.** Significant improvements have been made within the United States in the automation of EW planning aids. These improvements allow US EW planners to **extract information**, almost at will, **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 should determine what EW information would assist the MNF at the planning and unit level and ensure that they get it. To do this, the EWCC should understand security issues that preclude the release of some of the data and its source, but do not necessarily preclude the release of EW mission planning tools.

7. Releasability of Electronic Warfare Information to Allies and Multinational Forces

The integration of allied and/or multinational EW officers into US-led MNF activities is often perceived by US staff officers as too difficult due to the complexity of national disclosure policy. A clear, easily understood policy on the disclosure of EW information requested by allied and multinational partners must be developed by the commander's IO cell officer. Likewise, in peacetime exercises, the chief IO officer should work closely with the NATO EW core staff and NATO EWCCs to develop a clear, easily understood policy on the mutual disclosure of EW information.

Intentionally Blank

APPENDIX A
ELECTRONIC WARFARE GUIDANCE

The guidance in this appendix relates to the development of Tab B (Electronic Warfare) of Appendix 3 (Information Operations) to Annex C (Operations) of the format found in CJCSM 3122.03B, "*Joint Operation Planning and Execution System Vol II: Planning Formats*," for OPLANs, operation plans in concept format, OPORDs, and campaign plans.

1. Situation

a. **Enemy Forces**

(1) What are the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems?

(2) What is the enemy capability to interfere with accomplishment of the EW mission?

(3) What are the capabilities, limitations, and vulnerabilities of enemy communications, non-emitting, and EW systems resulting from third party support?

b. **Friendly Forces**

(1) What friendly EW facilities, resources, and organizations may affect EW planning by subordinate commanders?

(2) Who are the friendly foreign forces with which subordinate commanders may operate?

(3) What are the capabilities, limitations, and vulnerabilities of friendly communications, non-communications, and EW systems?

c. **Civilian and/or Neutral Facilities**

(1) What civilian and/or neutral facilities, resources, and organizations may affect EW planning by subordinates?

(2) What potential unintended and/or collateral consequences could be expected?

d. **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 the other core, related, or supporting capabilities of IO?

(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 subdivisions?

(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 emissions control guidance? Place detailed or lengthy guidance in an exhibit to this tab.

(5) What coordination with the J-6 is required to accomplish 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. **Feedback**

(1) What is the concept of operations for monitoring the effectiveness of EW operations during execution?

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

b. **After-Action Reports.** What are the requirements for after-action reporting?

c. **Signal.** What, if any, are the special or unusual EW-related communications requirements?

Intentionally Blank

APPENDIX B
ELECTRONIC WARFARE FREQUENCY DECONFLICTION PROCEDURES

1. General

Friendly, adversary, and third party operations that use or affect the EMS (communications, noncommunications, jamming) have the potential to interfere with joint force communications and other electronic systems. To counter this, the US military has established spectrum 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 spectrum use requirements while minimizing unacceptable interference. EW frequency deconfliction can be considered a subset of spectrum management and is defined as a systematic management procedure to coordinate the use of the EMS for operations, communications, and intelligence functions. This appendix provides guidance for developing joint EW frequency deconfliction procedures. To facilitate the development process, procedures and specific staff responsibilities are discussed in paragraph 5 below. To the extent possible, these procedures should be followed during joint, multinational, and single-Service operations and exercises.

2. Electronic Warfare Deconfliction Procedures

The steps involved in the EW frequency deconfliction process are as follows.

a. **Defining the Operations Concept and Critical Functions.** The J-3 defines the concept of operations to include each discrete phase of the operation. 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. 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.

b. **Developing the Intelligence Assessment.** Based on the J-3 concept of operations, the J-2 determines intelligence support requirements and identifies adversary electronic system targets for each phase of the operation (including the critical adversary functions) and associated electronic system nodes that need to be guarded. For example, during the friendly attack, adversary communication 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. An intelligence gain/loss must identify the value of the data being exploited to enable the JFC to make a decision to strike an adversary C2 despite its value to intelligence.

c. **Managing the Electromagnetic Spectrum.** JTF-GNO has overall responsibility of managing electromagnetic spectrum interference resolution to satellite communications (SATCOM) systems, satellite anomaly resolutions, and global SATCOM systems for the operation and defense of the GIG. This is done through the Global NETOPS Center. The J-6 is responsible for the administrative and technical management of the EMS in its operational area. This includes maintaining,

in conjunction with the J-2, the necessary database that contains information on all friendly, available adversary, and selected neutral or civil spectrum 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 spectrum-use conflict resolution. The assignment of frequencies is based on the J-3 concept of operations, frequency availability, unit geographic dispersion, radio wave propagation, equipment technical parameters, and criticality of unit functions. When assigning frequencies, the J-6 should advise users (using their frequency database) of possible interference from mobile systems in the operational area. Operating on assigned frequencies could spell the difference between success and failure of an operation.

d. **Defining and Prioritizing Candidate Nodes and Nets.** The joint force staff and subordinate commanders should define functions and identify specific nodes, and equipment that are critical to friendly and adversary operations. Candidate nodes and nets are submitted for EA protection to the JCEWS/EWCC (The submission should follow the standard JRFL format listed in Annex A, "Standardized JRFL Format."). In times of tension and war, certain adversary force data derived from compartmented SIGINT information should be provided by the J-2 and may be exchanged at the appropriate level of classification. Real-world EW data elements should not be exchanged in exercises except when specifically authorized.

e. **Generating 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 should compile the JRFL based on the coordinated inputs from the operations, intelligence, and communications staffs within the command and affected subordinate commands. The J-6 should ensure that the frequency assignments of unit nets designated for inclusion as PROTECTED or TABOO on the JRFL are submitted to the J-3 for final approval prior to dissemination. The restrictions imposed by the JRFL may only be removed at the direction of the J-3 if the J-3 determines that the benefit of jamming a restricted frequency surpasses the immediate criticality of exploited or required information to friendly forces. Operations and intelligence functions must be consulted before this decision. However, the self-protection of friendly forces has priority over all controls. GUARDED, PROTECTED, and TABOO frequencies are defined 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 those 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. These 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 to allow self protection by friendly forces. Specifically, during crisis or hostilities, short duration jamming may be authorized on TABOO frequencies for self protection to provide coverage from unknown threats, threats operating outside their known frequency ranges, or for other reasons.

f. **Disseminating the JRFL.** The JRFL is maintained and disseminated by the J-6.

g. **Updating 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/EWCC monitor the JRFL with respect to changes in the operations, timing, dates, and TABOO frequencies. The J-6 ensures that PROTECTED frequencies are congruent with assigned frequencies. The J-6 also amends the JRFL based on input from J-2 and J-3. Supporting EW units check the JRFL because this list is the primary source of "no jam" frequencies.

3. Joint Spectrum Interference Resolution Program

This program, coordinated and managed by the JSC, addresses those interference incidents that cannot be resolved at the unified, subordinate unified, JTF, and component levels. The joint spectrum interference resolution (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. The interference reporting procedures and format are outlined in CJCSM 3320.02A, "Joint Spectrum Interference Resolution Procedures."

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

(1) Message address: Defense Information Systems Agency (DISA) JSC-J-3 (UC) for unclassified reports and DISA JSC-J-3 (SC) for classified reports

(2) Telephone: Defense Switched Network (DSN) (312) 281-9857, DSN CONUS Area Code (312), or Commercial (410) 293-9857

(3) Sensitive compartmented information traffic is serviced directly through secure facsimile (FAX) and Intelink in the JSC sensitive compartmented information facility.

b. Upon receipt of a JSIR report 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. Resources for geolocation and direction-finding support, as well as access to databases not resident at JSC, should be coordinated with appropriate agencies as necessary. The JSC JSIR team deploys to the location of the victim organization, if necessary, in order to resolve interference problems. The organization requesting JSIR services is provided a report of the results of the JSIR analysis and appropriate information is incorporated into the JSIR database. This database supports trend analysis and future interference analysis.

c. Space system interference reporting and resolution is similar to the terrestrial reporting and resolution process except that the interference report is sent directly to the USSTRATCOM Joint Space Operations Center (JSPOC) from the space system manager affected. The space system is considered to include both the space-based and earth segments. The JSPOC forwards the incident report to the appropriate lead agency for investigation and resolution. The lead agencies are as follows: Global Satellite Communications (SATCOM) Support Center – SATCOM interference, GPS Support Center – GPS interference, and Cheyenne Mountain Operations Center – all other interference (to include Tracking, Telemetry and Control and Space Surveillance Network). Each lead agency coordinates with the JSC for analytical support.

4. Responsibilities

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

a. **J-3 Responsibilities**

(1) Determine and define critical friendly functions (TABOO and PROTECTED) to be protected from jamming and electronic deception based on the joint force concept of operations and in coordination with components.

(2) Approve the initial JRFL and subsequent changes.

(3) Provide guidance in OPLANs as to when jamming takes precedence over intelligence collection and vice versa.

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

(5) Continually weigh the operational advantages of employing EW against the advantages of intelligence collection.

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

b. **J-2 Responsibilities**

(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/EWCC) for approval.

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

(3) Develop and maintain map of nonmilitary entities operations on 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.

c. **J-6 Responsibilities**

(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, using SPECTRUM XXI, 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/EWCC 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 based on the changing of assigned operational frequencies among friendly force units.

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

d. **JCEWS/EWCC Responsibilities**

(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 through the IO cell.

(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.

e. 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/EWCC 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) Submits 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 Annex A, "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 spectrum protection. Normally, candidate nodes and nets should be submitted either through intelligence channels and consolidated by J-2 or through operations channels and consolidated by J-3.

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

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

(4) Keeps the JCEWS/EWCC apprised of issues that potentially impact EW planning and operational activities.

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

5. Frequency Deconfliction Analysis

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

a. **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 with jamming operations. The JRFL limits the frequencies that require immediate review by the JCEWS/EWCC. Where possible, automated decision aids should be used to conduct this comparison.

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

c. **Time.** Time analysis attempts to protect critical network equipment from friendly interference during friendly jamming missions. This subjective judgment is one that should be made by the J-3 or JTF commander, who must weigh the trade-off between critical jamming 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.** SPECTRUM XXI is the DOD standard automated spectrum management tool that supports operational planning, as well as near real-time management of radio frequency spectrum, with emphasis on assigning compatible frequencies and performing spectrum engineering tasks. During peacetime, SPECTRUM XXI is used by a joint staff at its permanent headquarters to facilitate the complex task of managing the spectrum during the planning and execution phases of exercises, as well as performing routine spectrum management functions. In the combat environment, SPECTRUM XXI 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 operational area, frequency assignments, terrain data, equipment characteristics, and tactical constraints.

Intentionally Blank

ANNEX A TO APPENDIX B
STANDARDIZED JOINT RESTRICTED FREQUENCY LIST FORMAT

The following JRFL format is an attempt to give the planner a standardized listing of information for developing a JRFL. This format is used by the joint automated communications-electronics operations instruction (CEOI) system (JACS). JACS is the joint standard for CEOI and JRFL

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 CEOI). 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.	PERIOD:	Two characters (represents CEOI time period 01-10), if known.
7.	START DATE:	Eight characters (MM/DD/YY) indicate start date when protection is required, if known.
8.	END DATE:	Eight characters (MM/DD/YY) indicate end date when protection is no longer required, if known.
9.	START HOUR:	Four characters 24 hour format (HHMM) indicate start time when protection is required, if known.
10.	END HOUR	Four characters 24 hour format (HHMM) indicate end time when protection is no longer required, if known.
11.	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
12.	RECEIVER COORDINATES:	Fifteen characters (latitude [dd(N or S)mmss] and longitude [ddd(E or W)mmss]) provides the location of the receiver or system to be protected, if known.
13.	AGENCY SERIAL NUMBER:	Ten characters (the agency serial number is a unique identifier for each frequency assignment), if known.
14.	POWER:	Nine characters (W=watts, K=kilowatts, M=megawatts, G=gigawatts) and a maximum of five decimal places, (e.g., W10.01234), if known.
15.	EMISSION:	Eleven characters (the emission designator contains the necessary bandwidth and the emission classification symbols [e.g., 3KOOJ3E]), if known.
16.	EQUIPMENT NOMENCLATURE:	Eighteen characters (e.g., AN/GRC-103), if known.
17.	COMMENTS:	Forty characters (provided for user remarks), optional entry.
18.	CEOI NAME:	Ten characters (a short title provided by the user to help identify the entry could use the actual title identified on the CEOI), optional entry.

production for the warfighter. This JRFL format is unclassified but, when actually accomplished, should show the proper classification of each paragraph.

APPENDIX C
JOINT SPECTRUM CENTER SUPPORT TO JOINT ELECTRONIC WARFARE

1. General

The DOD JSC was activated on 28 September 1994. The JSC has assumed all the missions and responsibilities previously performed by the Electromagnetic Compatibility Analysis Center, as well as additional functions. The JSC is a field activity of the DISA.

2. Mission

The mission of the JSC is to ensure the 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. The JSC Support to EW

a. The JSC maintains databases and provides data about friendly force C2 system locational and technical characteristics for use in planning electronic protect measures. Databases maintained by the JSC provide EW planners with information covering communications, radar, navigation aids, broadcast, identification, and EW systems operated by the DOD, other United States 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 JSC assists spectrum managers, the JCEWS/EWCC, 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, a spectrum management tool that has the capability to create, edit, and manage the JRFL. The JSC also has combatant command support teams that can be deployed to assist combatant commands, subordinate unified commands, JTFs, or their components when requested. These teams are trained to prepare JRFLs or provide training and assistance in JRFL preparation. The teams can also serve as on-site advisors and assistants in spectrum management matters and EW deconfliction as required.

c. The JSC 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 in order to request assistance in resolving suspected spectrum interference problems.

d. The JSC provides data about foreign communications frequency and location data. Databases containing this data are developed primarily from open sources.

e. The JSC also provides unclassified communications area studies about the communications infrastructure of over 150 countries. These area studies are developed entirely from open source material. Information provided in these studies includes: physical and cultural characteristics (geography, climate, and population); overview of telecommunications systems; and EM frequencies registered for use within the geographic boundaries of each country. Data in these studies includes 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 the widely-used SPECTRUM XXI.

4. Mailing Address:

JSC/J3
2004 Turbot Landing
Annapolis, MD 21402-5064

5. Defense Message System (DMS) Address:
DISA JSC-J3 (UC) or (SC)

6. Telephone Numbers:

DSN: (312) 281-9815 (UNCLASSIFIED)
COMMERCIAL: (410) 293-9815
FAX: DSN (312) 281-3763 (UNCLASSIFIED)
FAX: DSN (312) 281-5309 (CLASSIFIED)
Duty Officer: DSN (312) 281-9857,
Commercial (410) 293-9857

APPENDIX D
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 changes.

(1) **Tactics.** A tactics change includes 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. These changes are not normally created organically, although newer systems may be reprogrammed rapidly at the unit level using electronic transmission means.

(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 planning or actual hostilities, EW reprogramming provides operational commanders with a timely capability to correct EW and/or TSS equipment deficiencies, tailor equipment to meet unique theater or mission requirements, or to respond to changes in adversary threat systems.

(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, resulting 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 3-51.1, Marine Corps Reference Publication (MCRP) 3-40.5B, Navy Tactics, Techniques, and Procedures (NTTP) 3-13.1.15, AFTTP (I) 3-2.7, Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare and Target Sensing Systems.

(1) **Determine Threat.** The first phase of reprogramming is to develop and maintain an accurate description of the equipment's operational environment, 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 that an accurate description of the EM environment 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 the 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 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 EM environment. 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 is identified 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 by 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 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 generates 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 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 changes) 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 that unit combat effectiveness is regained or enhanced by the tactic, software, or hardware change. To accomplish this task, component commands ensure that 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 EM environment and all three subdivisions of joint EW operations. Combatant commands must ensure that 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 in accordance with the following joint policy. CJCSI 3210.04, "Joint Electronic Warfare Reprogramming Policy," outlines the responsibilities of the Joint Staff, Military 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. This instruction describes the purpose of threat change validation and directs combatant commands to develop and exercise a timely threat change validation process to support the needs of component commands and Service reprogramming support activities during times of crisis.

Intentionally Blank

APPENDIX E
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/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 tradeoff analyses, and develop tactics, doctrine, and procedures.

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

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.

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

b. **Army.** Aviation and Missile Command, National Ground Intelligence Center, 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.

c. **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 Analysis, Naval Space Command, and Naval Surface Warfare Center.

d. **Air Force.** Air Force Agency for Modeling and Simulation, Air Force Research Laboratory, NASIC, Air Force Information Warfare Center (AFIWC), Air Force Operational Test and Evaluation Center, Air Force Studies and Analysis Agency, Aeronautical Systems Center, Survivability and Vulnerability Information Analysis Center, Air Armaments Center, Air and Space C2 Agency, C2 Battle Lab, and Air Force Wargaming Centers.

e. **Marine Corps**. Commandant's Warfighting Lab, Wargaming and Combat Simulated Division of Marine Corps Combat Development Command, and MAGTF Staff Training Program, 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 & 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), a research (data gathering) phase, 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 which can be used to aggregate realistic effects at higher order simulation levels, e.g., mission/campaign level war gaming. In such cases, audit trails should be available in analyst manuals or other documentation to document data sources, 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 upon 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: radio frequency and IR wavelength propagation, radio 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-ER), clutter (land/sea/atmospheric), satellite coverage (polar/geosynchronous), link analysis, missile guidance and flyout, evasive maneuvers, communications processes, communications targeting, EP, 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 2167A, Open Software Foundation, and National Security Agency and Central Security Service. 2167A 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 on 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 on the battlefield 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 that 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. More "crystal-balling" becomes necessary, but such efforts tend be less reliable the farther out one tries to project into the future. Benchmarking against widely accepted simulations provides a straightforward and less biased method of validation. However, there are problems caused by differences in input data structures, assumptions, and output formats between the models. To the extent possible, careful review, analysis, and manipulation of data must be applied to minimize the potential of creating apparent discrepancies which 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 Forces Command, Joint Training and Simulation Center, Combined Arms Center, NGIC, NASIC, AFIWC, Naval Air Warfare Center Weapons Division, and Air Force Air Warfare Center.

b. **Parametric, Signature, and Antenna Pattern.** NSA, DIA, NGIC, Missile and Space Intelligence Center, Office of Naval Intelligence, nuclear weapons reconnaissance list, Navy Information Operation Commands, NASIC, JSC, and AFIWC.

c. **Topographic.** NGA, US Geological Survey, Army Engineer Topographic Laboratories, CIA, and Waterways Experiment Station.

APPENDIX F
SERVICE PERSPECTIVES OF ELECTRONIC WARFARE

1. Army

The focus of Army EW operations is based on the need to synchronize lethal and nonlethal attacks against adversary targets in support of operational and tactical ground, air, and space operations. Army EW disrupts, delays, diverts, and denies the adversary's ability to wage war while protecting friendly use of communications and noncommunications systems. The perspective of Army forces is directly associated with the combined arms structure of adversary forces and the manner in which both friendly and adversary combatants conduct combat operations. The high mobility of opposing combat forces and the speed, range, precision accuracy, and lethality of their weapons systems place stringent demands on the C2 systems of both friendly and adversary ground force commanders. Synchronization is achieved by integrating EW into both the IO plan and fire support operations in support of the ground scheme of maneuver, using centralized control and decentralized execution functions performed by parallel communications systems and procedures at all echelons. Organic (air and ground-based) EW resources available to support Army operations are limited, but improving. Mission requirements usually exceed operational and tactical capability. Cross-Service EW support, synchronized with Army combat operations, is essential to the success of joint military operations. Joint planning and continuous, effective coordination are critical to synchronizing joint EW capabilities and generating joint combat power at the critical time and place in battle. The Army provides and requires cross-Service EW support when and where needed to achieve the combat objectives and operational goals of the JFC.

2. Marine Corps

a. 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 enemy's decision cycle. This ability enhances friendly capabilities while shattering the moral, mental, and physical cohesion of the adversary, rendering the adversary incapable of effectively resisting. Marine EW units, found within both the command and aviation combat elements of a MAGTF, are task organized to meet the needs of the MAGTF commander, subordinate commanders, and ultimately the operational goals of the JFC.

b. EW units are integrated into the commander's concept of operations and scheme of maneuver in order 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 the short-term effects of EW, conducting active operations of EA, ES, and EP in order to support the operational requirements of the MAGTF commander as well as those of the JFC with provision of cross-Service support in the joint arena.

3. Navy

Naval task forces use all aspects of EW in performing their naval warfare tasks. Emphasis is given to surveillance, the neutralization or destruction of adversary targets, and the enhancement of friendly force battle management through the integrated employment and exploitation of the EMS and the medium of space. Naval battle groups employ a variety of organic shipboard EW systems, primarily for

self protection. Naval aviation forces are the primary means by which naval forces take the EW fight to the adversary at extended ranges. Carrier and land-based EA-6B Prowlers use a variety of onboard systems to conduct EA (including both standoff and close-in jamming), ES, and EP in support of SEAD and IO tasking. Naval task force use of the EMS and space encompasses measures that are employed to:

a. Coordinate, correlate, fuse, and employ aggregate communication, surveillance, reconnaissance, data correlation, classification, targeting, and electromagnetic attack capabilities;

b. Deny, deceive, disrupt, destroy, or exploit the adversary's capability to communicate, monitor, reconnoiter, classify, target, and attack;

c. Facilitate antiship missile defense; and

d. Direct and control employment of friendly forces.

See NTTP 3-51.1, Navy Electronic Warfare and NTTP 3-13.2, Information Operations Warfare Commander's Manual for additional details.

4. Air Force

a. The COMAFFOR conducts a variety of EW operations, including EA, EP, and ES.

b. In addition, EW supports SEAD and other IO mission areas (e.g., delivery of PSYOP messages, actions taken to support a MILDEC operation). The object of these operations is to increase aircraft survivability, enhance the effectiveness of military operations, and increase the probability of mission success. Air Force EW system development and employment focus on this task. The Air Force uses an integrated mix of disruptive and destructive EW systems to defeat hostile integrated air defenses. Disruptive EW systems, (e.g., self-protection jamming) provide an immediate but temporary solution. The EC-130H Compass Call conducts a variety of EW missions and is Air Force's primary nonlethal SEAD asset. It performs C2 systems countermeasures throughout the C2 spectrum, supporting air, land, sea, and SO across the range of military operations. Destructive systems provide a more permanent solution, but may take longer to fully achieve the desired results. The integrated use of destructive and disruptive systems offsets their individual disadvantages and results in a synergistic effect. Successful EW operations emphasize risk reduction while still maintaining mission effectiveness. 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. Aggressive employment of EW can have a profound impact on the JFC's IO. The Air Force employs a variety of ground-, air-, and space-based assets to accomplish these tasks.

APPENDIX G
REFERENCES

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

1. Department of Defense

a. DOD Directive 3000.3, *Policy for Nonlethal Weapons*.

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

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 3150.25B, *Joint Lessons Learned Program*.

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

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

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

f. CJCSI 3320.02B-1, *Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)*.

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

h. CJCSM 3122.03B, *Joint Operation Planning and Execution System Vol II: Planning Formats*.

i. CJCSM 3212.02B, *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 3320.02A, *Joint Spectrum Interference Resolution (JSIR) Procedures*.

l. CJCSM 3500.04D, *Universal Joint Task List*.

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

n. JP 2-0, *Intelligence Support*.

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

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

q. JP 3-01.4, *Joint Tactics, Techniques, and Procedures for Joint Suppression of Enemy Air Defenses (J-SEAD)*.

r. JP 3-05, *Doctrine for Joint Special Operations*.

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

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

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

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

w. JP 3-53, *Joint Doctrine for Psychological Operations*.

x. JP 3-57, *Joint Doctrine for Civil-Military Operations*.

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

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

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

3. Multinational and Multi-Service

a. MC 64/9 NATO, *Electronic Warfare Policy*.

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

c. MC 486 NATO, *Electronic Warfare Core Staff (NEWCS)*.

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

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

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

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

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

i. AJP-2, *Allied Joint Intelligence Doctrine*.

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

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

l. ATP-44, *Electronic Warfare in Air Operations*.

m. ATP-51, *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*.

p. FM 3-51.1, MCRP 3-40.5B, NTTP 3-13.1.15, AFTTP(I) 3-2.7, *Multi-Service Tactics, Techniques, and Procedures for the Reprogramming of Electronic Warfare and Target Sensing Systems*.

q. FM 90-39, MCRP 3-22A, NWP 3-01.4, AFTTP(I) 3-2.4, *Multi-Service Tactics, Techniques, and Procedures for EA-6B Employment in the Joint Environment*.

4. Navy Publications

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

b. NTTP 3-13.2, *Information Operations Warfare Commander's Manual*

Intentionally Blank

APPENDIX H
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center, ATTN: Doctrine and Education Group, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3). The lead agent for this publication is USSTRATCOM Director of Plans and Policy (J-5).

3. Supersession

This publication supersedes JP 3-51, 7 April 2000, *Joint Doctrine for Electronic Warfare*.

4. Change Recommendations

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

TO: JOINT STAFF WASHINGTON DC//J3-DDGO//
CDRUSSTRATCOM OMAHA NE//J512//
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
CDRUSJFCOM SUFFOLK VA//DOC GP//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info the Lead Agent and the Director for Operational Plans and Joint Force Development J-7/JEDD via the Chairman of the Joint Chiefs of Staff (CJCS) Joint Electronic Library at http://www.dtic.mil/doctrine.

b. 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 Military Services and other organizations are requested to notify the Joint Staff/J-7 when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution of Printed Publications

a. Additional copies of this publication can be obtained through the Service publication centers listed below (initial contact) or US Joint Forces Command (USJFCOM) in the event that the joint publication is not available from the Service.

b. Individuals and agencies outside the combatant commands, Services, Joint Staff, and combat support agencies are authorized to receive only approved joint publications and joint test publications. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

c. Additional copies should be obtained from the Military Service assigned administrative support responsibility by DOD Directive 5100.3, 15 November 1999, *Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands*.

By Military Services:

Army: US Army AG Publication Center SL
1655 Woodson Road
Attn: Joint Publications
St. Louis, MO 63114-6181

Air Force: Air Force Publications Distribution Center
2800 Eastern Boulevard
Baltimore, MD 21220-2896

Navy: CO, Naval Inventory Control Point
700 Robbins Avenue
Bldg 1, Customer Service
Philadelphia, PA 19111-5099

Marine Corps: Commander (Attn: Publications)
814 Radford Blvd, Suite 20321
Albany, GA 31704-0321

Coast Guard: Commandant (G-OPD)
US Coast Guard
2100 2nd Street, SW
Washington, DC 20593-0001

Commander
USJFCOM JWFC Code JW2102
Doctrine and Education Group (Publication Distribution)

116 Lake View Parkway
Suffolk, VA 23435-2697

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

6. Distribution of Electronic Publications

a. The Joint Staff will not print copies of electronic joint publications for distribution. Electronic versions are available at www.dtic.mil/doctrine Non-Secure Internet Protocol Router Network (NIPRNET), or http://nmcc20a.nmcc.smil.mil/dj9j7ead/doctrine/ SECRET Internet Protocol Router Network (SIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Defense Pentagon, Washington, DC 20301-7400.

Intentionally Blank

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

A-3	Operations Directorate (COMAFFOR)
A-5	Plans Directorate (COMAFFOR)
ABCA	American, British, Canadian, Australian Armies Standardization Program
ACOS	assistant chief of staff
AFIWC	Air Force Information Warfare Center
AFTTP (I)	Air Force tactics, techniques, and procedures (instruction)
AJP	Allied joint publication
AOR	area of responsibility
ASIC	Air and Space Interoperability Council
ATO	air tasking order
ATP	allied tactical publication
C2	command and control
CAG	carrier air group
CCDR	combatant commander
CCIR	commander's critical information requirement
CEOI	communications-electronics operating instructions
CI	counterintelligence
CIA	Central Intelligence Agency
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CM	countermeasure
CMO	civil-military operations
CND	computer network defense
CNO	computer network operations
COA	course of action
COMAFFOR	commander, Air Force forces
COMCAM	combat camera
COMSEC	communications security
CONPLAN	concept plan
CSG	Cryptologic Support Group
CVWC	carrier strike group air wing commander
DCCC	defense collection coordination center
DE	directed energy
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DJIOC	Defense Joint Intelligence Operations Center
DOD	Department of Defense
DSN	Defense Switched Network

DSPD	defense support to public diplomacy
E3	electromagnetic environmental effects
EA	electronic attack
EEFI	essential elements of friendly information
ELINT	electronic intelligence
EM	electromagnetic
EMC	electromagnetic compatibility
EMCON	emissions control
EME	electromagnetic environment
EMI	electromagnetic interference
EMS	electromagnetic spectrum
EOB	electronic order of battle
EO-ER	electro-optical-infrared
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWCC	electronic warfare coordination cell
EWO	electronic warfare officer
FAX	facsimile
FM	field manual
FSE	fire support element
G-2	Army or Marine Corps component intelligence staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-3	component operations staff officer
G-7	information operations staff officer (ARFOR)
GCCS	Global Command and Control System
GCCS – A	Global Command and Control System – Army
GIG	Global Information Grid
GPS	global positioning system
IA	information assurance
IEEE	Institute of Electrical and Electronics Engineers
IO	information operations
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
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
JCA	jamming control authority
JCEWR	joint coordination of electronic warfare reprogramming
JCEWS	joint force commander's electronic warfare staff
JFACC	joint force air component commander
JFC	joint force commander
JFMO	Joint Frequency Management Office
JFSOCC	joint force special operations component commander
JIOC	joint intelligence operations center
JIOWC	Joint Information Operations Warfare Command
JISE	joint intelligence support element
JOC	joint operations center
JOPES	Joint Operation Planning and Execution System
JP	joint publication
JRFL	joint restricted frequency list
JSC	Joint Spectrum Center
JSIR	joint spectrum interference resolution
JSME	joint spectrum management element
JSPOC	Joint Space Operations Center
JTF	joint task force
JTF-GNO	Joint Task Force-Global Network Operations
LNO	liaison officer
LOAC	law of armed conflict
MAGTF	Marine air-ground task force
MASINT	measurement and signature intelligence
MC	Military Committee (NATO)
MCRP	Marine Corps reference publication
METOC	meteorological and oceanographic
MILDEC	military deception
MNF	multinational force
MNFC	multinational force commander
NASIC	National Air and Space Intelligence Center
NATO	North Atlantic Treaty Organization
NEWCS	NATO electronic warfare core staff
NETOPS	network operations
NGA	National Geospatial-Intelligence Agency
NGIC	National Ground Intelligence Center
NSA	National Security Agency
NTTP	Navy tactics, techniques, and procedures
NWP	Navy warfare publication

OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
PA	public affairs
PSYOP	psychological operations
QSTAG	quadripartite standardization agreement
RADBN	radio battalion
RCIED	radio-controlled improvised explosive device
RF	radio frequency
ROE	rules of engagement
SATCOM	satellite communications
SEAD	suppression of enemy air defenses
S/EWOC	signals intelligence/electronic warfare operations center
SIGINT	signals intelligence
SIM	system impact message
SIPRNET	SECRET Internet Protocol Router Network
SO	special operations
STO	special technical operations
TNCC	theater network operations (NETOPS) control center
TSS	target sensing system
USCG	United States Coast Guard
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
VMAQ	Marine tactical electronic warfare squadron
WARM	wartime reserve mode
WP	Working Party (NATO)

PART II — TERMS AND DEFINITIONS

CEASE BUZZER. An unclassified term to terminate electronic attack activities, including the use of electronic warfare expendables. (This term and its definition are applicable only in the context of this publication and cannot be referenced outside this publication.) (Approved for removal from the next edition of JP 1-02.)

chattermark. Directive communications call to begin using briefed radio procedures to counter communications jamming. (This term and its definition are applicable only in the context of this publication and cannot be referenced outside this publication.) (Approved for removal from the next edition of JP 1-02.)

civil-military operations. The activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate military operations, to consolidate and achieve operational US objectives. Civil-military operations may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. Civil-military operations may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces. Also called CMO**.** (JP 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combat camera. The acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, special force, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services. Also called COMCAM**.** (JP 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2**.** (JP 1-02)

communications intelligence. Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 1-02)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (JP 1-02)

communications system. Communications networks and information services that enable joint and multinational warfighting capabilities. (JP 1-02)

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. (JP 1-02)

computer network defense. Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. Also called CND. (JP 1-02)

computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE. (JP 1-02)

computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO. (JP 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (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. (JP 1-02)

defense support to public diplomacy. Those activities and measures taken by the Department of Defense components to support and facilitate public diplomacy efforts of the United States Government. Also called DSPD. (JP 1-02)

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. (JP 1-02)

directed-energy device. A system using directed energy primarily for a purpose other than as a weapon. Directed-energy devices may produce effects that could allow the device to be used as a weapon against certain threats; for example, laser rangefinders and designators used against sensors that are sensitive to light. (JP 1-02)

directed-energy warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. (JP 1-02)

directed-energy weapon. A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. (JP 1-02)

electromagnetic compatibility. The ability of systems, equipment, and devices that utilize the electromagnetic spectrum to operate in their intended operational environments without suffering unacceptable degradation or causing unintentional degradation because of electromagnetic radiation or response. It involves the application of sound electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation; and clear concepts and doctrines that maximize operational effectiveness. Also called EMC. (JP 1-02)

electromagnetic deception. The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. (JP 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 that may be encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. It is the sum of electromagnetic interference; electromagnetic pulse; hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static. Also called EME**.** (JP 1-02)

electromagnetic environmental effects. The impact of the electromagnetic environment upon the operational capability of military forces, equipment, systems, and platforms. It encompasses all electromagnetic disciplines, including electromagnetic compatibility and electromagnetic interference; electromagnetic vulnerability; electromagnetic pulse; electronic protection, hazards of electromagnetic radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of lightning and precipitation static. Also called E3**.** (JP 1-02)

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

electromagnetic interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. It can be induced intentionally, as in some forms of electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like. Also called EMI**.** (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)

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)

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)

electromagnetic radiation. Radiation made up of oscillating electric and magnetic fields and propagated with the speed of light. Includes gamma radiation, X-rays, ultraviolet, visible, and infrared radiation, and radar and radio waves. (JP 1-02)

electromagnetic radiation hazards. Hazards caused by transmitter or antenna installation that generates electromagnetic radiation in the vicinity of ordnance, personnel, or fueling operations in excess of established safe levels or increases the existing levels to a hazardous level; or a personnel, fueling, or ordnance installation located in an area that is illuminated by electromagnetic radiation at a level that is hazardous to the planned operations or occupancy. Also called EMR hazards or RADHAZ. (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)

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)

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. (Approved for inclusion in the next edition of JP 1-02.)

electronic intelligence. Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT**.** (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

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)

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)

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. (Approved for inclusion in the next edition of JP 1-02.)

electronic reconnaissance. The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 1-02)

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)

electronic warfare. Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. Also called EW**.** (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of 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)

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. These changes may be the result of deliberate actions on the part of friendly, adversary or third parties; or may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of electronic warfare reprogramming is to maintain or enhance the effectiveness of electronic warfare and target sensing system equipment. Electronic warfare reprogramming includes changes to self defense systems, offensive weapons systems, and intelligence collection systems. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of 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. (Approved for inclusion in the next edition of JP 1-02.)

electro-optical countermeasure. See **countermeasure.**

electro-optical-infrared countermeasure. Any 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. Electro-optical-infrared is the part of the electromagnetic spectrum between the high end of the far infrared and the low end of ultraviolet. Electro-optical-infrared countermeasure may use laser and broadband jammers, smokes/aerosols, signature suppressants, decoys, pyrotechnics/pyrophorics, high-energy lasers, or directed infrared energy countermeasures. Also called EO-IR CM. (Approved for inclusion in the next edition of 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)

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)

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. Also called GIG. (JP 1-02)

guarded frequencies. Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the guarded frequency list changes as the enemy 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. (JP 1-02)

imitative communications deception. That division of deception involving the introduction of false or misleading but plausible communications into target systems that mimics or imitates the targeted communications. (JP 1-02)

imitative electromagnetic deception. See **electromagnetic deception.**

improvised explosive device. A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components. Also called IED. (JP 1-02)

information assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (JP 1-02)

information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02)

information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp

adversarial human and automated decision making while protecting our own. Also called IO. (JP 1-02)

joint restricted frequency list. A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Also called JRFL. (JP 1-02)

joint suppression of enemy air defenses. A broad term that includes all suppression of enemy air defense activities provided by one component of the joint force in support of another. Also called J-SEAD**.** (JP 1-02)

manipulative electromagnetic deception. See **electromagnetic deception.**

meaconing. A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (JP 1-02)

measurement and signature intelligence. Technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Measurement and signature intelligence capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems as well as gas, liquid, and solid materials sampling and analysis. Also called MASINT**.** (JP 1-02)

military deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called MILDEC. (JP 1-02)

Modernized Integrated Database. The national level repository for the general military intelligence available to the entire Department of Defense Intelligence Information System community and, through Global Command and Control System integrated imagery and intelligence, to tactical units. This data is maintained and updated by the Defense Intelligence Agency. Commands and Services are delegated responsibility to maintain their portion of the database. Also called MIDB**.** (JP 1-02)

nondestructive electronic warfare. None. (Approved for removal from the next edition of JP 1-02.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called **OPSEC.** (JP 1-02)

Intentionally BlankIntentionally Blank**physical security.** 1. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. 2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (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)

protected frequencies. Those friendly 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. 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 must be updated periodically. (JP 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP**.** (JP 1-02)

public affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA**.** (JP 1-02)

public diplomacy. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad. (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. (Approved for inclusion in the next edition of JP 1-02.)

reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 1-02)

rules of engagement. Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. (JP 1-02)

signal security. A generic term that includes both communications security and electronics security. (JP 1-02)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT**.** (JP 1-02)

simulative electromagnetic deception. See **electromagnetic deception.**

space control. Combat, combat support, and combat service support operations to ensure freedom of action in space for the United States and its allies and, when directed, deny an adversary freedom of action in space. The space control mission area includes: surveillance of space; protection of US and friendly space systems; prevention of an adversary's ability to use space systems and services for purposes hostile to US national security interests; negation of space systems and services used for purposes hostile to US national security interests; and directly supporting battle management, command, control, communications, and intelligence. (JP 1-02)

spectrum management. Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (Approved for inclusion in the next edition of JP 1-02.)

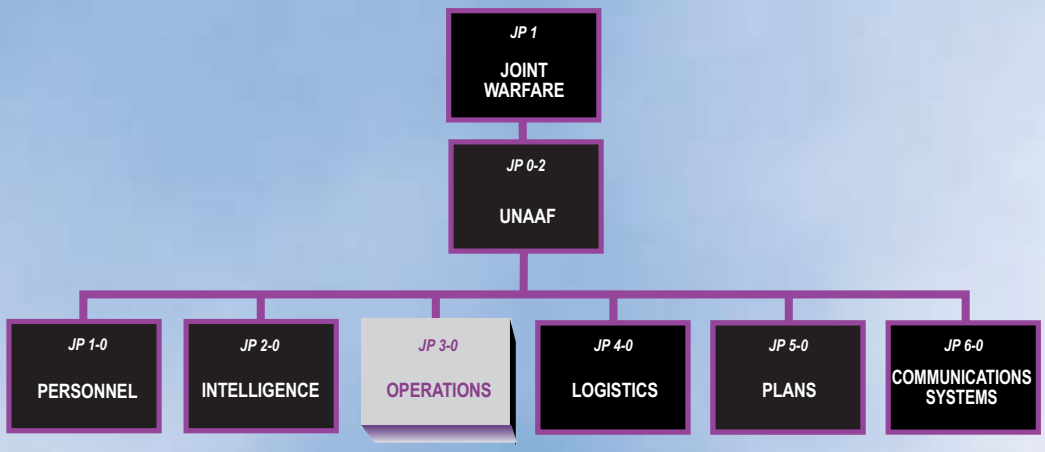
suppression of enemy air defenses. That activity that neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by destructive and/or disruptive means. Also called SEAD**.** (JP 1-02)

TABOO frequencies. Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces. Normally, these frequencies include international distress, CEASE BUZZER, safety, and controller frequencies. These frequencies are generally long standing. However, they may be time-oriented in that, as the combat or exercise situation changes, the restrictions may be removed. (JP 1-02)

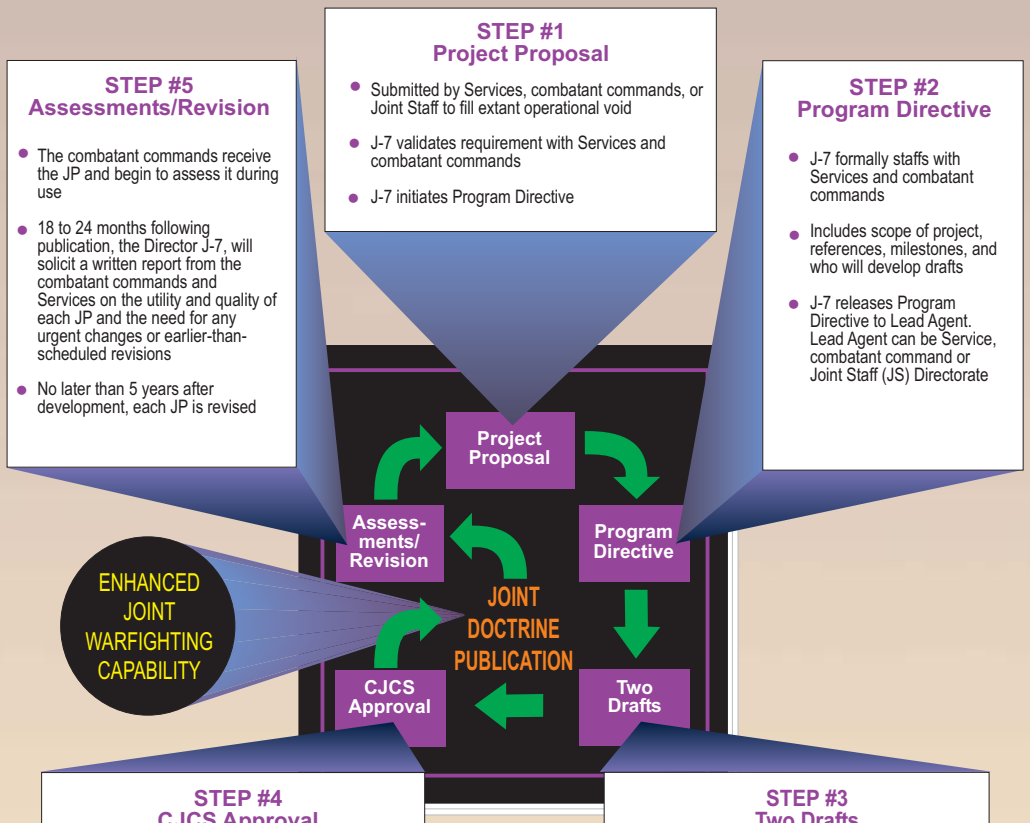
wartime reserve modes. Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. Also called WARM**.** (JP 1-02)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint doctrine is 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