

ARMY, MARINE CORPS, NAVY, AIR FORCE



**AIR LAND SEA
APPLICATION
CENTER**

REPROGRAMMING

MULTISERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR THE REPROGRAMMING OF ELECTRONIC WARFARE AND TARGET SENSING SYSTEMS

FM 3-51.1 (FM 34-72)

MCRP 3-40-5B

NTTP 3-13.1.15

AFTTP(I) 3-2.7

JANUARY 2003

DISTRIBUTION RESTRICTION: Distribution authorized to DOD and DOD contractors only to protect technical or operational information under the International Exchange Program or by other means. This determination was made on 15 January 2003. Other requests will be referred to HQ TRADOC, ATTN: ATDO-A, Fort Monroe, VA 23651; HQ MCCDC, ATTN: C42, Quantico, VA 22134; NWDC, ATTN: N5, Newport, RI 02841; or HQ AFDC, ATTN: DG, Langley AFB, VA 23665.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

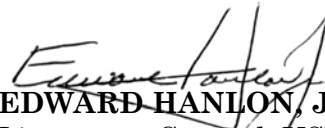
MULTISERVICE TACTICS, TECHNIQUES, AND PROCEDURES

FOREWORD

This publication has been prepared for use by respective commands and other commands as appropriate.



KEVIN P. BYRNES
General, U.S. Army
Commanding General
U.S. Army Training and Doctrine
Command



EDWARD HANLON, JR.
Lieutenant General, USMC
Commanding General
Marine Corps Combat
Development Command



R. A. ROUTE
Rear Admiral, USN
Commander
Navy Warfare Development Command



DAVID F. MacGHEE, JR.
Major General, USAF
Commander
Headquarters Air Force Doctrine
Center

**This publication is available on the
General Dennis J. Reimer Training and
Doctrine Digital Library at
www.adtdl.army.mil.**

PREFACE

1. Scope.

This publication describes multiservice tactics, techniques, and procedures (MTTP) for use during reprogramming operations to support electronic warfare (EW) and target sensing systems (TSS). The Joint Task Force (JTF) and component-level commands coordinate and integrate this activity with information operations (IO). This publication—

- a. Provides an overview of EW and TSS reprogramming.
- b. Details the requirements and procedures for coordinating and integrating reprogramming during joint/multiservice operations.
- c. Provides a detailed discussion of the reprogramming process.
- d. Provides service points of contact for reprogramming and message formats applicable to the reprogramming process.
- e. Identifies joint and service reprogramming exercise programs.

2. Purpose

a. This publication provides a single-source, consolidated reference on EW/TSS reprogramming activities to support JTF EW operations. It discusses joint operations procedures for reprogramming to facilitate coordination, synchronization, integration, and deconfliction of reprogramming actions within the JTF, when executed in exercises, contingencies, and other operations in which more than one service is involved.

b. This publication augments the authoritative doctrine published in Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations (IO)*, JP 3-13.1, *Joint Doctrine for Command and Control Warfare*; and JP 3-51, *Joint Doctrine for Electronic Warfare*.

3. Application

This publication provides JFCs, component commanders, and their operational staffs unclassified guidance for EW planning and reprogramming actions. EW planners can use this publication to gain an understanding of reprogramming actions and their impact on plans and operations. As an effective force multiplier, reprogramming operations must be properly planned and integrated across components to maximize combat effectiveness. Accordingly, this document serves as a reference for EW planners to build and execute coordinated and integrated joint operations. Enhanced mission planning and coordinated execution are the result.

This is a multiservice publication approved for use by the U.S. Army, Marine Corps, Navy, and Air Force.

4. Implementation Plan

Participating service command offices of primary responsibility (OPR) will review this publication, validate the information and references, and incorporate it in service manuals, regulations, and curricula as follows:

Army. The Army will incorporate the procedures in this publication in U.S. Army training and doctrinal publications as directed by the commander, U.S. Army Training and Doctrine Command (TRADOC). Distribution is in accordance with initial distribution number (IDN) 115744.

Marine Corps. The Marine Corps will incorporate the procedures in this publication in U.S. Marine Corps training and doctrinal publications as directed by the commanding general, U.S. Marine Corps Combat Development Command (MCCDC). Distribution is in accordance with MCPDS.

Navy. The Navy will incorporate these procedures in U.S. Navy training and doctrinal publications as directed by the commander, Navy Warfare Development Command (NWDC). Distribution is in accordance with MILSTRIP Desk Guide and NAVSOP Pub 409.

Air Force. Air Force units will validate and incorporate appropriate procedures in accordance with applicable governing directives. Distribution is in accordance with AFI 33-360.

5. User Information

a. TRADOC, MCCDC, NWDC, HQ AFDC, and the Air Land Sea Application (ALSA) Center developed this publication with the joint participation of the approving service commands. ALSA will review and update this publication as necessary.

b. This publication reflects current joint and service doctrine, command and control organizations, facilities, personnel, responsibilities, and procedures. Changes in service protocol, appropriately reflected in joint and service publications, will likewise be incorporated in revisions to this document.

c. ALSA encourages recommended changes for improving this publication. Key any comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendation directly to—

Army

Commander
U.S. Army Training and Doctrine Command
ATTN: ATDO-A
Fort Monroe, VA 23651-5000
DSN 680-3951 COMM (757) 788-3951
E-mail: doctrine@monroe.army.mil

Marine Corps

Commanding General
U.S. Marine Corps Combat Development Command
ATTN: C42
3300 Russell Road, Suite 318A
Quantico, VA 22134-5021
DSN 278-6233/6234 COMM (703) 784-6233/6234
E-mail: deputydirectordoctrine@mccdc.usmc.mil

Navy

Navy Warfare Development Command
Doctrine Development Division (Code N5)
686 Cushing Road, Sims Hall
Newport, RI 02841-1207
DSN 948-1164/4189 COMM (401) 841-1164/4189
E-mail: alsapubs@nwdc.navy.mil

Air Force

Headquarters Air Force Doctrine Center
ATTN: DJ
204 Dodd Blvd, Ste 301
Langley AFB, VA 23665-2788
DSN 574-8091 COMM (757) 764-8091
E-mail: afdc.dj@langley.af.mil

ALSA

ALSA Center
ATTN: Director
114 Andrews Street
Langley AFB, VA 23665-2785
DSN 574-0902 COMM (757) 764-0902
E-mail: alsadirector@langley.af.mil

*FM 3-51.1 (FM 34-72)
 *MCRP 3-40.5B
 *NTTP 3-13.1.15
 *AFTTP (I) 3-2.7

FM 3-51.1 (FM 34-72)	U.S. Army Training and Doctrine Command Fort Monroe, Virginia
MCRP 3-36.1B	Marine Corps Combat Development Command Quantico, Virginia
NTTP 3-13.1.15	Navy Warfare Development Command Newport, Rhode Island
AFTTP (I) 3-2.7	Headquarters Air Force Doctrine Center Maxwell Air Force Base, Alabama

6 January 2003

REPROGRAMMING

Multiservice Tactics, Techniques, and Procedures for Reprogramming of Electronic Warfare and Target Sensing Systems

TABLE OF CONTENTS

		Page
EXECUTIVE SUMMARY		vi
Chapter I	OVERVIEW OF ELECTRONIC WARFARE AND TARGET SENSING SYSTEM (EW/TSS) REPROGRAMMING	I-1
	Background	I-1
	EW/TSS.....	I-2
	Reprogramming Process.....	I-3
	Reprogramming Databases	I-4
Chapter II	REPROGRAMMING IN THE JOINT ENVIRONMENT	II-1
	Background	II-1
	JTF Battlestaff	II-1
	Component Reprogramming.....	II-3
	Coordination Between Services	II-5

*This publication supersedes FM 34-72, MCRP 3-36.1B; NWP 3-13.1.15; AFTTP(I) 3-2.7, dated 13 April 1998.

Chapter III	THE REPROGRAMMING PROCESS.....	III-1
	EW/TSS Reprogramming	III-1
	Service EW/TSS Reprogramming	III-2
	The Reprogramming Process	III-5
Appendix A	PROCEDURES FOR JOINT COORDINATION OF EW REPROGRAMMING	A-1
Appendix B	POINTS OF CONTACT (POCs)	B-1
Appendix C	REPROGRAMMING MESSAGE FORMATS.....	C-1
Appendix D	REPROGRAMMING EXERCISES	D-1
	REFERENCES.....	References-1
	GLOSSARY	Glossary-1
	INDEX	Index-1
FIGURES	II-1. Notional JTF IO Cell.....	II-2
	III-1. Reprogramming Process Current Roles	III-4
	III-2. Reprogramming Process.....	III-5
	III-3. Parametric Threat Change Validation (Crisis/Wartime).....	III-6
	III-4. Threat Change Analysis.....	III-8
	III-5. Mission Data Development and Coding	III-11
	III-6. EA Technique Reprogramming Process	III-13
	III-7. OFP Development and Coding Functional Model	III-14
	A-1. Phase I: Determine the Threat	A-2

EXECUTIVE SUMMARY

REPROGRAMMING MTTP for Reprogramming of Electronic Warfare and Target Sensing Systems

This publication—

- Provides an overview of electronic warfare and target sensing system reprogramming.
- Details the requirements and procedures for coordination and integration of reprogramming during joint/multiservice operations.
- Provides a detailed discussion of the reprogramming process.
- Provides service points of contact for reprogramming and message formats applicable to the reprogramming process.
- Identifies joint and service reprogramming exercise programs.

Electronic warfare/target sensing systems (EW/TSS) include smart weapons, munitions, sensors, and processors that rely on signature data, such as electronic intelligence (ELINT), measurement and signature intelligence (MASINT), and other signature parametrics to identify specific targets or events. With the increased fielding of EW/TSS within the services, a coordinated, integrated, and synchronized process for the reprogramming of EW/TSS during Joint Task Force (JTF) operations must be identified to maximize the effectiveness of these systems. Moreover, today's military operational planners must address the application of EW/TSS reprogramming within the framework of information operations (IO).

EW/TSS reprogramming provides the means to respond to changes in threat signature characteristics or unique theater signature environments, enhancing the capability and survivability of the joint force. Threat parametric signature changes occurring during contingency or combat operations may require operational decisions to change tactics, bypass or avoid the threat, reprogram EW/TSS against the threat, or target the threat for physical destruction. Reprogramming EW/TSS provides a timely means to respond to immediate threat changes and correct system deficiencies to mitigate the impact of the threat change.

The reprogramming process starts with collecting and processing intelligence data, proceeds with the assessment and engineering phases, and results in distributing and loading updated software and, in some instances, hardware/firmware. Reprogramming is integrated into operational plans through EW mission planning and the capabilities-analysis phase of the targetting process. While reprogramming is generally an EW function at the service component level, the JTF's commander's IO cell, specifically the Electronic Warfare Coordination Cell (EWCC), closely coordinates and deconflicts among the service components in a JTF. The staff coordination process begins with interaction between the operations and intelligence staff directorates at the JTF and

component levels, as the staffs may identify a signature parametric change as a result of the intelligence process or from operational mission reports.

The Joint Information Operations Center (JIOC) has reprogramming oversight responsibilities for the joint staff. Oversight responsibilities include requirements to organize, manage, and exercise joint aspects of EW/TSS reprogramming and facilitate the exchange of data used in joint EW/TSS reprogramming. Although actual reprogramming of equipment is a service responsibility, the coordination of reprogramming at the joint/combined level must occur because of the similarities in EW equipment. The combatant command/JTF EW officer is responsible for facilitating the exchange of reprogramming data among the components.

PROGRAM PARTICIPANTS

The following commands and agencies participated in developing and reviewing this publication:

Joint

Joint Information Operations Center (JIOC), Lackland AFB, TX

Army

Program Executive Office - Aviation, Redstone Arsenal, AL

Program Executive Office - Intelligence and Electronic Warfare, Electronic Warfare and Sensors, Fort Monmouth, NJ

U.S. Army Communications Electronics Command, Fort Monmouth, NJ

U.S. Army Intelligence and Security Command, 1st Information Operations Command (L), Fort Belvoir, VA

HQ U.S. Army Intelligence and Security Command, MASINT Division, FORT Belvoir, VA

U.S. Army Aviation Center, Fort Rucker, AL

Marine Corps

Marine Corps Combat Development Command, Joint Doctrine Branch (C427), Quantico, VA

Navy

Commanding Officer, Navy Warfare Development Command, Newport, RI

Commander, Fleet Information Warfare Center (FIWC), Little Creek Naval Amphibious Base, Norfolk, VA

Air Force

Air Force Information Warfare Center (AFIWC), 453 Electronic Warfare Squadron, Lackland AFB, TX

Headquarters Air Combat Command (ACC)/DOO, Langley AFB, VA

53 Wing, Eglin AFB, FL

WR-ALC/LN, Robins AFB, GA

HQ AFSOC ECSEF, Robins AFB, GA

National Air Intelligence Center, Wright-Patterson AFB, OH

Chapter I

OVERVIEW OF ELECTRONIC WARFARE AND TARGET SENSING SYSTEM (EW/TSS) REPROGRAMMING

1. Background

a. Reprogramming. EW/TSS include smart weapons, munitions, sensors, and processors that rely on signature data, such as electronic intelligence (ELINT), measurement and signature intelligence (MASINT), and other signature parametrics to identify specific targets or events. With the increased fielding of EW/TSS within the services, a coordinated, integrated, and synchronized process for the reprogramming of EW/TSS during Joint Task Force (JTF) operations must be identified to maximize the effectiveness of these systems.

b. This document deals with the ability to reprogram EW and TSS systems whenever the force comes across new or unexpected enemy capabilities. Moreover, today's military operational planners must address the application of EW/TSS reprogramming within the framework of information operations (IO). JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines IO as "actions taken to affect adversary information and information systems while defending one's own information and information systems." Full spectrum IO activities incorporate the disciplines, or elements, of operations security (OPSEC), psychological operations (PSYOP), military deception (MILDEC), electronic warfare (EW), computer network defense (CND), computer network attack (CNA), and physical destruction. Related areas include public affairs (PA) and civil affairs (CA). Threat parametric signature changes primarily affect the IO elements of EW and physical destruction. Threat parametric signature changes occurring during contingency or combat operations may require operational decisions to change tactics, bypass or avoid the threat, reprogram EW/TSS against the threat, or target the threat for physical destruction.

(1) EW/TSS reprogramming impacts the three elements of EW (electronic attack [EA], electronic protection [EP], and electronic support [ES]) as defined in JP 1-02, and Chairman Joint Chiefs of Staff Instruction (CJCSI) 3210.03, *Joint Electronic Warfare Policy*.

(a) EAs are typically those offensive operations using nonlethal fires (jamming) and antiradiation missiles (ARM) to degrade, neutralize, or destroy enemy combat capabilities. The reprogramming process improves the ability of EW/TSS to identify, target, and/or counter adversary systems in a dynamic electromagnetic environment.

(b) EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of EW. The reprogramming process ensures that EW/TSS perform their designed combat function by mitigating the effects of parametric signature anomalies or unknown or unidentified signatures encountered on the battlefield.

(c) ES provides information required for immediate decisions involving EW operations and other tactical actions, such as threat avoidance, targeting, and homing. ES is a continuous effort that occurs before operational deployment and

continues throughout combat operations. The reprogramming process enables target-sensing systems to identify electromagnetic emitters rapidly and accurately.

(2) **Physical Destruction.** Operational planners must weigh the impact of reprogramming efforts against operational risk and mission accomplishment. If the impact of reprogramming actions is significant, in terms of risk or resources, destroying the threat may be the most timely and effective option available to the commander. Additionally, in the case of precision munitions, reprogramming may be the key enabler of weapons accuracy.

Historical Example:

Operational commanders have a range of actions to handle changing threats. Air Force Information Warfare Center (AFIWC)/Operations Support, Reprogramming (OSR) (redesignated 453 EWS/EWP) operated on a 24-hour basis throughout operations Desert Shield and Desert Storm to provide near-real-time assessments of changing threats on CENTAF EW systems. During Desert Shield, CENTAF implemented more than 70 software reprogramming changes to its EW systems (C2 protect actions). However, when combat operations began during Desert Storm, no additional reprogramming changes were requested. CENTAF's reprogramming actions shifted to suppression of enemy air defense (SEAD) targeting. Flagging reports contributed to the targeting of threat systems for physical attack (C2 attack actions). The philosophy was that there was insufficient time to implement software changes to EW systems; "If my aircraft systems can't see it or jam it, I'm going to kill it."

c. **IO Staff Officers.** IO staff officers, as members of JTF or service component staffs, must have a thorough understanding of all facets of the reprogramming process including service-unique requirements related to reprogramming. Collecting signature data and subsequent identifying, verifying, validating, and loading software and/or firmware changes requires the coordinated efforts of many agencies. Effective interaction is necessary for efficient and rapid application of software modifications to favorably impact operations within the joint operations area (JOA).

2. EW/TSS

a. **Reprogrammable EW/TSS.** Reprogrammable EW/TSS are computer controlled or automated systems that have reprogrammable software or firmware update capabilities. Changes in the threat and/or EW system operational environment, such as threat activation of wartime reserve modes (WARM) or using camouflage, concealment, and decoy techniques to alter a threat system's signature, may affect EW/TSS performance.

b. **Reasons to Reprogram.** Reprogramming is a key enabler of force protection and precision fires within the joint force. Preparing for or during military operations, reprogramming provides operational commanders with the capability to correct EW/TSS equipment deficiencies, tailor equipment to meet unique theater or mission requirements, or to respond to changes in enemy threat systems. Reprogramming of EW/TSS provides a timely means to respond to immediate threat changes and correct system deficiencies to mitigate the impact of the threat change.

3. Reprogramming Process

a. Process Overview. The reprogramming process starts with collecting and processing intelligence data, progresses through assessment and engineering phases, and results in distributing and loading updated software and, in some instances, firmware. The services have slightly different approaches to providing reprogramming support for EW/TSS.

(1) Army Threat Change Analysis Centers. The Army Reprogramming Analysis Team Threat Analysis (ARAT-TA) Center is located at Eglin AFB to support target-sensing systems. System-oriented software support activities (SSAs) reside within the Army Material Command (AMC) and provide engineering support to develop, code, test, and distribute changes for specific systems.

(2) Navy Electronic Warfare Reprogrammable Library (EWRL). The Navy EWRL at FIWC provides the Navy/Marine Corps primary focal point for more than 20 EW systems. Reprogramming responsibilities include evaluating threat change impact on service-specific EW systems through coordination with multiple engineering centers for developing threat data, coding, testing, and disseminating validated changes to fleet users. FIWC is located in Norfolk, Virginia.

(3) Air Force Threat Change Analysis. The Air Force Information Warfare Center (453 EWS/EWF) operates an automated flagging capability to identify threat parametric signature anomalies. The 453 EWS/EWF processes worldwide ELINT and conducts a quality assessment of that data to correct for unknown or misidentified signals, collector biases, and other problems that may have created anomalies in the raw data. This data is processed through software models of Air Force EW and TSS systems to determine the impact on modeled systems. The EW Operational RCs 53 Wing, Eglin AFB, Florida, Air Force Special Operations Command (AFSOC)/Electronic Combat Support Flight(ECSF), Robins AFB, Georgia, and Warner Robins-Air Logistics Center (WR-ALC), Georgia perform further assessments of threat change impact and development of software changes.

b. Categories of Reprogramming. There are two major categories of reprogramming actions: cyclical or block updates that occur on a periodic basis and reprogramming in response to a previously unidentified or altered threat signature.

(1) Cyclical/Block Updates. Cyclical or block updates are reprogramming actions that occur on a periodic basis to update/maintain current EW/TSS libraries or to develop new EW/TSS libraries. These cyclical changes in the libraries are based on new intelligence data obtained by various intelligence collection efforts. Many EW/TSS include cyclical or block updates as part of normal life cycle improvements.

(2) Reprogramming. Reprogramming is time sensitive actions that take place as immediate responses to threat changes in the tactical environment. After validating the threat parametric signature data change, reprogramming is done as quickly as possible.

c. Reasons for Reprogramming. Reprogramming may be required for any of the following reasons:

(1) Parametric Signature Changes. Adversary use of wartime reserve modes or modification of an existing threat system may cause identification anomalies or cause the threat system to go undetected by friendly EW/TSS.

(2) New Threat System Introductions. New threat systems not previously known to exist in the theater EW environment may require reprogramming of friendly systems to ensure mission success. These threat systems include both new acquisitions and extensive modifications of existing systems.

(3) Foreign Military Sales (FMS)/ Technology Transfer. This category applies to those systems found in the EW environment that are provided by friendly and/or threat countries to third parties.

(4) Unique Theater Requirements. Specific theater missions may involve modifications, depending on unique geographical, environmental, and/or logistical concerns. Depending on theater and foreign military services participating in the coalition, reprogramming actions will occur to ensure proper identification of friendly systems and minimize the potential for fratricide.

4. Reprogramming Databases

a. Electronic Warfare Integrated Reprogramming Data Base (EWIRDB). Today's databases and flagging models are primarily based on ELINT parametric data. The EWIRDB is the primary Department of Defense (DOD) approved source for technical parametric data on noncommunications emitters. The reprogrammable systems supported include radar, radar warning receivers (RWR), combat identification, EW systems, ARM , and other targeting systems that directly enhance wartime survivability and effectiveness. The EWIRDB is the product of merged data modules from three organizational entities. These modules are—

(1) Scientific and technical intelligence (S&TI) center and service production center (SPC) assessments based on all-source intelligence from foreign emitters. SPC and S&TI are interchangeable terms. For clarity, this publication uses only the term service production center (SPC). For a definition of SPC, see paragraph b(3) below.

(2) National Security Agency (NSA) national technical ELINT database, named KILTING, on U.S. and foreign emitters.

(3) The Air Force Information Warfare Center (AFIWC) compiles U.S. and friendly-foreign emitter data from Army, Navy, and Air Force EW support agencies via the U.S. Electromagnetic Systems Database (USELMSDB).

b. Intelligence Community Support. The following intelligence agencies perform one or more of the following functions: collect, analyze, produce, assess, and validate signatures to support the reprogramming effort:

(1) NSA. The NSA maintains the KILTING database (NSA file of observed technical electronic intelligence on foreign emitters). It provides KILTING data as a component of the DOD automated EWIRDB, a digital noncommunications emitter data source the Defense Intelligence Agency (DIA) approves and validates as the baseline for ELINT data.

(2) DIA. The DIA is the focal point for joint intelligence collection and analysis. It oversees maintenance of the EWIRDB; assigns data production tasks to SPCs; and maintains the air, electronic, and ground order of battle databases.

(3) SPCs. The SPCs are intelligence production centers the DIA or another service manages. DIA tasks the SPCs to correlate, analyze, validate and produce scientific and technical intelligence based on all-source intelligence of assigned foreign emitters. SPCs support DOD and other national requirements and include—

(a) National Air Intelligence Center (NAIC). NAIC is DIA's executive agent for the EWIRDB and consolidates data from the other service SPCs, NSA's KILTING database, and AFIWC into the master EWIRDB for distribution to users. NAIC is also responsible for analyzing red and gray fixed-wing, EW/GCI, and height finder systems.

(b) Missile and Space Intelligence Center (MSIC). MSIC is responsible for analyzing red and gray ground missile systems.

(c) National Ground Intelligence Center (NGIC). NGIC is responsible for analyzing red and gray anti-aircraft artillery (AAA), rotary-wing systems, battlefield surveillance systems, ground-based, and rotary-wing mounted jammers.

(d) Office of Naval Intelligence (ONI). ONI is responsible for analyzing red and gray naval associated emitters, less those air-related signals under the purview of Air Force Intelligence Analysis Agency (AFIAA). Additionally, ONI is responsible for maintaining data on non-U.S. merchant shipping vessels.

c. MASINT Database. Emerging EW/TSS (F-22, Apache Longbow, Comanche, Advanced Threat Infrared Counter Measure, Brilliant Antitank [BAT] munitions, etc.) may require an effort parallel to the EWIRDB for MASINT data. MASINT data includes scientific and technical intelligence information obtained through quantitative and qualitative analysis of data derived from specific technical sensors, foreign material exploitation (FME) and modeling and simulation for the purpose of identifying distinctive features associated with the source, emitter, or sender to facilitate subsequent identification and/or measurement of the same. Mission data sets and programming for MASINT supported systems require new knowledge bases and interpretation skills similar to ELINT EWIR analysis. The National Target Signature Data System (NTSDS), currently under development by the DIA Central MASINT Organization, is the system that enables access to MASINT signature data.

d. Other Databases. EW/TSS systems exploit radiated signals and compare them to known threat systems characteristics. When required, communications intelligence (COMINT) databases are analyzed with ELINT/MASINT databases to assist in resolving ambiguities in identification.

Chapter II

REPROGRAMMING IN THE JOINT ENVIRONMENT

1. Background

The JTF commander should organize his battlestaff in a manner that facilitates the cross flow of reprogramming data and requirements among service components to achieve a coordinated, integrated, and synchronized process for reprogramming EW/TSS during JTF operations.

2. JTF Battlestaff

a. JTF Staff Organization. When fully formed, the JTF staff contains appropriate members in key positions of responsibility from each service or functional component having significant forces assigned to the command. Per JP 3-51 and JP 3-13, authority for planning and supervising IO and joint EW (to include EW reprogramming) is normally delegated by the JFC to the J3. An IO cell or similar organization replaces the intra-staff coordination previously accomplished through a "joint commander's electronic warfare staff." The following discussion provides one option for locating the IO cell within the operations directorate (J3).

b. J3. The J3 assists the commander in discharging assigned responsibility for the direction and control of operations, beginning with planning, and following through until specific operations are completed. In this capacity the directorate plans, coordinates, and integrates operations. The flexibility and range of modern forces require the close coordination and integration of JTF assets for effective unity of effort.

c. IO Cell. The IO cell is formed from select representatives from each staff element, component, and supporting agency responsible for integrating capabilities and related activities. The cell coordinates staff elements and/or components represented in the IO cell to facilitate the detailed support necessary to plan and coordinate IO. To assist the J3 in exercising joint IO responsibilities, the J3 normally designates an IO officer. The primary function of the IO officer is to supervise the IO cell to ensure capabilities and activities are planned, coordinated and integrated within the joint force staff and with higher headquarters, adjacent, subordinate, and multinational staffs. The IO officer ensures that IO is implemented per the planning meetings, leads the IO cell, and/or directly facilitates coordination between the components or staff organizations responsible for planning and executing IO. The IO officer serves as JTCCB (or functional equivalent) IO cell representative. The IO officer is the central point for IO and can coordinate all IO functional areas. The IO officer, or his designated representative, ensures deconfliction and unity of effort for information activities within the AOR/JOA.

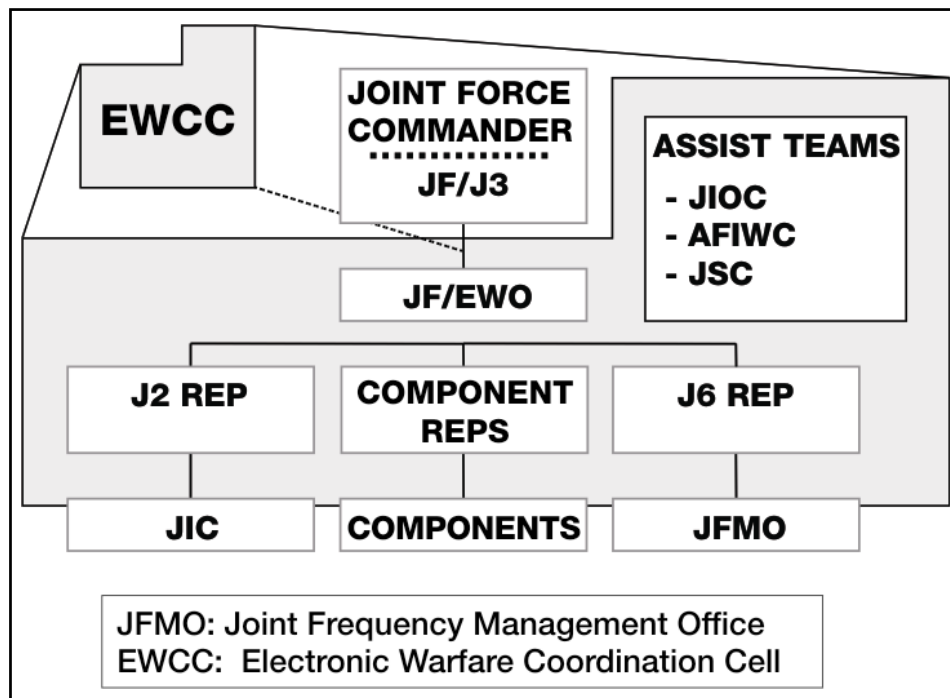


Figure II-1. Notional JTF IO Cell

d. Reprogramming. Reprogramming is integrated into operational plans through EW mission planning and the capabilities analysis phase of the targeting process for physical destruction. Specifically, electronic attack considerations include reprogramming of smart munitions to optimize weapons effects based on signature parametrics of intended targets. Electronic protect considerations include reprogramming RWRs to accurately reflect threats to friendly systems and to minimize the potential for fratricide. Specific reprogramming information should be included in the EW tab of the IO appendix of the operations annex to the JTF operations plan/order (OPLAN/ OPORD).

e. EWCC Actions. Threats to friendly forces identified during the intelligence process should cause the EW staff officer to recommend to the commander one of several options regarding these threats. These options may include bypassing or avoiding the threat, reprogramming against the threat, a change in tactics, or targeting the threat for physical destruction. The EWCC cell should monitor the development of the OPLAN/ OPORD to ensure systems with identified deficiencies against certain threats are not assigned missions into these threat areas. For example, the F-16 RWR may have problems identifying a threat based on parametric signature changes. However, because of the way threat libraries are generated, F/A-18s might not be affected. Inputs into the air tasking order (ATO) generation should be made to modify taskings based on these identified EW deficiencies.

f. Staff Coordination. While reprogramming is generally an EW function, implementing it requires close coordination and deconfliction of efforts among the IO cells in the JTF and service component staffs. The staff coordination process begins with interaction between the operations and intelligence staff directorates at the JTF and component level. A signature parametric change may be identified as a result of the

intelligence process or from operational mission reports (for example, operational change request [OCR] for the Army and Air Force; threat change analysis request [TCAR] message for the Navy/Marine Corps).

(1) The Joint Intelligence Directorate (J2) representative to the EWCC, through the intelligence collection process, might be the first to identify a possible parametric signature change. Identifying a parametric signature change could result from national-level intelligence input or analysis of theater collection efforts. Regardless of the source, the JTF intelligence fusion cell consolidates all inputs reflecting possible parametric signature changes and forwards these inputs to the theater intelligence processing center (IPC) for further assessment, collection, and verification.

Note: theater IPCs are also referred to as joint intelligence centers (JIC) and in EUCOM, a joint analysis center (JAC).

(2) Alternatively, the joint staff electronic warfare officer (EWO) may identify possible parametric signature changes through analyzing operational mission or flagging reports. Mission reports originate from operational theater or component tactical elements. Quantifying the operational impact of signature parametric changes requires close coordination between the EWO and the intelligence staff representative. The intelligence staff pursues the validation of the parametric signature change by identifying information requirements (that is, additional collection taskings) to the J2 collection manager for tasking to JTF or national intelligence assets.

(3) After receiving validation of parametric signature changes from the appropriate SPC, the operations staff develops courses of actions (COAs) recommending to the commander a tactics, techniques and procedures (TTP) change, a software/firmware change, a targeting recommendation, or any combination of the above. The commander may develop a TTP change instead of a reprogramming change or as an interim measure while waiting for development of a software/firmware change. Each service component commander makes the decision to implement a TTP or a software/firmware change. If reprogramming is impractical due to operational concerns, modified threats should receive priority as operational targets and be recommended by the IO/EW staff as high-priority targets to the JTF targeting board. If a threat is targeted and battle damage assessment (BDA) reports destruction, the EWCC ensures service-reprogramming centers receive this information via secure communications (such as DMS, SIPRNET e-mail).

3. Component Reprogramming

EW/TSS reprogramming is a service responsibility. However, during joint operations, the rapid reprogramming of EW/TSS could become critical in a rapidly evolving hostile situation. Service reprogramming efforts must include coordinating with JFCs to identify, process, and implement reprogramming requirements in a timely manner by all affected friendly forces.

a. **Joint Coordination.** The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW/TSS equipment maintained by field and fleet units. This reprogramming is the responsibility of each service through its respective EW reprogramming support program. This service responsibility remains, even when the JFC organizes his forces with functional component commands. However, joint

coordination of EW reprogramming is critical because threat signature changes and equipment reprogramming changes affect the EM environment and all three subdivisions of joint EW operations. Combatant commands must ensure that joint coordination of EW reprogramming (JCEWR) policy and procedures are exercised during all major training events and real-world operations. The Joint Staff defines this responsibility in CJCSI 3210.04 (Draft) "Joint EW Reprogramming Policy". (An excerpt of this CJCSI is in Appendix A.) This instruction tasks combatant commands, component commands, and subordinate joint force commands to establish and execute JCEWR procedures. This instruction also 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 crises.

b. U.S. Army. Operational EW mission reports may originate at the IO cell at division or corps level depending on the echelon of force designated as the Army service component commander. The division or corps EWO and G-2 representative coordinate regarding the TCAR and begin the formal process to validate the possible parametric signature change. This coordination must include EWOs at each echelon down to brigade level. The Army service component commander (ASCC) submits the TCAR to ARAT-TA, and provides information copies to appropriate theater intelligence activities. ARAT-TA coordinates validation with the appropriate SPC and alerts the appropriate SSA for the production of a software solution to the problem. The ARAT-TA coordinates any requirements for TTP production with the appropriate TRADOC proponent school.

c. U.S. Marine Corps. Fleet Marine force units can submit a TCAR during peacetime or war to report suspected emitter threat changes. A TCAR can originate at any level but is collated and reviewed at the EWCC or IO cell at the Marine Air-Ground Task Force (MAGTF). At the MAGTF level, the commanding general, via the EWCC within the IO cell, has internal management responsibility for the reprogramming effort of the deployed MARFOR, including necessary coordination with the Marine and Naval component command and joint force staff. The IO cell addresses the TCAR for ACTION to FIWC. FIWC validates the TCAR and requests via TCVR validation of the suspected threat change to the appropriate SPC. After receiving a TCAR, FIWC begins assessing the impact of the reported threat change on Marine Corps tactical air (TACAIR), rotary wing, or air cargo/transport EW equipment. If the SPC validates the threat change and determines that reprogramming is necessary, FIWC responds with a system impact message (SIM) recommending reprogramming of the affected EW system(s). The SIM is sent for ACTION to the appropriate Naval/Marine component commander and for INFO to the submitting unit and other commands requiring the information. If the MAGTF commander decides to reprogram, he sends an authorization to reprogram (ATR) message to cue TSSCs/SSAs to begin testing the parametric data. After obtaining correct system response, TSSCs/SSAs notify fleet users via the distribution notice message (DNM) that EW libraries will be forwarded via the most expeditious means.

d. U.S. Navy. Naval afloat or shore units can submit a TCAR during peacetime or war to report suspected emitter threat changes. A TCAR can originate at any level but is normally collated and reviewed by the information warfare commander (IWC) at the combined task group (CTG)/combined task force (CTF) level depending on the echelon of force designated as the Navy forces (NAVFOR) component. The NAVFOR component commander, usually via the IWC, has internal management responsibility for the reprogramming effort of the deployed force, including necessary coordination.

The TCAR will be addressed for ACTION to FIWC and INFO the appropriate SPC for threat change validation. FIWC validates the TCAR and requests via a TCVR validation of the suspected threat change to the appropriate SPC. If the SPC validates a threat change and determines that reprogramming is necessary, FIWC responds with a SIM. The SIM is sent for ACTION to the CTG/CTF commander and for INFO to the originating unit and other commands requiring the information. If the CTG/CTF commander decides to reprogram, he sends an authorization to reprogram (ATR) message to cue TSSCs/SSAs to begin testing parametric data. TSSCs/SSAs, upon completion of obtaining correct system response, will notify fleet users via the distribution notice message (DNM) that EW libraries will be forwarded via the most expeditious means.

e. U.S. Air Force. Operational mission reports (MISREPs) or TCARs may originate at any level but are collated and reviewed at the wing or numbered Air Force level depending on the echelon of force designated as the Air Force forces (AFFOR) component. The AFFOR or major command (MAJCOM) determines if further evaluation will be done on the MISREP or TCAR. Flagging reports may provide additional information in the evaluation process. The reprogramming centers respond according to the priority (routine up to 18 months, urgent-10 days [normal work shifts], emergency-24-hour work days until complete) of the TCAR. A SIM is then sent to the appropriate operational commands and cognizant organizations. A reprogramming impact message (RIM) may follow if appropriate. The AFFOR or the appropriate MAJCOM (for example, Air Combat Command (ACC) or AFSOC) sends an implementation message.

f. Special Operations Forces (SOF). SOF initiate reports according to parent service procedures. Parent service procedures will be utilized to meet reprogramming requirements with the following exception: Air Force SOF fixed-wing and MH-53 helicopters are reported through Air Force channels to the ECSF , Robins Air Force Base, Georgia.

4. Coordination Between Services

a. CJCSI 3210.04 (Draft) requires the coordination of EW reprogramming among the services. The JIOC has oversight responsibilities for the joint staff. Oversight responsibilities include requirements to organize, manage, and exercise joint aspects of EW reprogramming, and facilitate the exchange of data used in joint EW reprogramming. The EWCC and component staffs are the primary staff organizations responsible for this coordination process.

b. Although actual reprogramming of equipment is a service responsibility, the coordination of reprogramming at the joint/combined level must occur because of the similarities in EW equipment. This coordination responsibility falls on each component IO cell/EW officer. The combatant command/JTF EW officer is responsible for facilitating the exchange of reprogramming data among the components. Each component IO cell/EW officer is responsible for coordinating the EW reprogramming information among subordinate organizations. If an EWCC cell is not formed, a separate EW cell can be formed to exchange reprogramming information and provide components the required information.

c. The combatant command/JTF IO cell/EW officer receives status information from each component IO cell/EW officer during established meetings or as required. The types of information required include—

(1) Problems encountered by specific EW equipment in theater. This includes threat parametric changes that could impact the identification and/or jamming techniques used against that threat.

(2) Modifications to friendly EW operating parameters that might be misidentified by other friendly systems. For example, a change in the jamming techniques used by a system could appear to be an enemy threat, and if not coordinated, could result in fratricide.

(3) Status of existing reprogramming actions.

(4) Specific intelligence collection requirements that might assist the overall theater. An example could be a specific emitter causing a misidentification by a specific EW system, but due to other priority intelligence collection requirements, signals intelligence (SIGINT) has not been collected on this emitter. The supported combatant command/CJTF staff can input a priority intelligence collection requirement to attempt to determine the specific signals causing the misidentification.

d. The combatant command/JTF EW officer uses this information to keep the J3 and commander informed. He uses this information to modify special instructions (SPINS) on the ATO (for example, modify escort aircraft responsibilities because of a specific service problem in identifying/countering a specific threat) or provide the basis for elevating a target's priority for physical destruction during the targeting process.

Chapter III

THE REPROGRAMMING PROCESS

1. EW/TSS Reprogramming

a. Purpose. The purpose of reprogramming is to maintain and enhance the effectiveness of EW/TSS sensors and munitions resident in warfighters' field and fleet units. Preparing for or during actual hostilities, reprogramming provides operational commanders with a timely capability to correct EW/TSS equipment deficiencies, tailor equipment to meet unique theater or mission requirements, or to respond to changes in enemy threat systems.

b. Scope and Responsibility. Reprogramming impacts numerous battlefield systems including self-defense systems, offensive weapons systems, and intelligence collection systems. The reprogramming of EW/TSS is the responsibility of each service through its respective reprogramming support programs. The term reprogramming is used by the Army, Navy, and Marine Corps to refer to all (cyclic, exercise, and real-world, time-sensitive) reprogramming actions. The Air Force uses the term PACER WARE to refer to all real-world Air Force reprogramming actions. The Army uses the term JADE LANTERN to refer to all real-world Army reprogramming messages.

c. Reprogramming Changes. Several types of changes constitute reprogramming. These changes fall into three major classifications: TTP, software, and firmware/hardware. The rationale for selecting one change over another rests with the affected service commander. Generally, TTP changes are implemented as interim fixes until software changes can be made to correct identified deficiencies. Firmware/hardware changes usually require depot-level support and are usually not an option to correct an immediate problem. The operational component commander decides which reprogramming changes to implement based on the tempo of operations, the impact of the threat on mission success, and the time available to make the change. Defined reprogramming changes follow:

(1) TTP. A TTP change includes changes in tactics, equipment settings, or EW/TSS mission-planning data. These changes are usually created and implemented at the unit level using organic equipment and personnel. A change in TTP may be the operational commander's most appropriate response if the affected unit cannot afford to wait for a software or hardware change.

(2) Software. Software changes include actual changes of programmable EW and TSS equipment. This type of change requires SSA support to alter programmed look-up tables, threat libraries, or signal-sorting routines. These changes are not normally created at the unit level. However, once engineers create the required software changes, units may reprogram newer systems rapidly using electronic transmission means.

(3) Firmware/Hardware. Firmware/hardware changes and/or long-term system development is necessary when TTP or software changes cannot correct equipment deficiencies. These changes usually occur when the complex nature of a change leads to a system modification. Firmware/hardware changes normally require depot-level support.

2. Service EW/TSS Reprogramming

The Army and the Air Force have established threat change analysis centers and EW reprogramming centers to support reprogrammable EW systems/TSSs. The Navy's FIWC EWRL, in coordination with multiple TSSCs/SSAs, provides reprogramming support to Navy/USMC systems. This is in response to a constantly changing threat electromagnetic environment. The objective is to improve the overall performance of systems by incorporating hardware and software improvements that can mitigate the impact of this changing threat. The reprogramming process has evolved in complexity as the capability of fielded systems has expanded. The following paragraphs describe services' reprogramming support programs.

a. Army Target Sensing Systems Rapid Reprogramming (ATRR). Army Regulation (AR) 525-15 establishes the mission for engineering and reprogramming Army TSS. The Army's threat change analysis center is the ARAT-TA, Eglin Air Force Base, FL. The primary Army reprogramming software engineering centers are CECOM Software Engineering Center (SEC), Fort Monmouth, NJ, and MICOM Software Support Center, Huntsville, AL. The ATRR process supports the tactical commander and material developers by—

(1) Providing timely warning of reprogramming requirements created by threat changes.

(2) Providing software for reprogrammable Army TSS using the EWIRDB, approved and validated battlefield information, and/or MASINT data.

(3) Coordinating with appropriate TRADOC proponent commands for TTP issues affecting developmental and fielded systems.

b. Navy-Marine Corps EWRL Support Program. Under the direction of OPNAVINST 3430.23 (series), the tactical EWRL support program is designed to support Department of the Navy reprogrammable EW equipment used by all Navy and Marine Corps surface, air, and subsurface platforms. The naval EW reprogramming process provides operational commanders with a timely and accurate means to react effectively to changes in the threat environment and to maintain a vigilant intelligence review effort to minimize the impact of threat WARM or threat parameter changes on Navy/Marine Corps reprogrammable systems (such as RWRs, ES, EA, and EP systems, and other munitions and sensors requiring radar parametrics). Reprogramming support developed under the EWRL Support Program ensures that EW systems continue to function effectively during crisis and war. Reprogramming can be organic, involving systems capable of manipulating data either by manual manipulation of on-line data, or non-organic systems requiring extensive engineering. The reprogramming process can include changes in tactics, support operations, EW equipment software and hardware, and changes in support equipment and other support systems (for example, training devices, threat simulators).

c. The Air Force EW reprogramming process is called electronic warfare integrated reprogramming (EWIR). Air Force Instruction (AFI) 10-703 defines EWIR as the process that fully integrates operations, intelligence, communications, logistics, and other support functions to provide changes to reprogrammable EW equipment hardware and software, tactics, and equipment settings. EWIR gives the Air Force a clear and comprehensive picture of tasks, data, staffing, and the required relationships among agencies that reprogram EW equipment. This process forms the basis for

developing procedures, organizations, facilities, and expertise to ensure responsive EW reprogramming during peacetime, contingencies, and wartime.

(1) The flagging portion of threat change analysis is performed by 453d Electronic Warfare Squadron (EWS) at Lackland Air Force Base, TX. Flagging includes intelligence analysis and initial software system impact analysis. The operational EW RCs at the 53rd Electronic Warfare Group, Eglin Air Force Base, FL, and ECSF (AFSOC), Robins Air Force Base, GA perform hardware and additional software analyses. The operational RCs also identify threat change impacts/system deficiencies and develop mission data (MD) reprogramming changes, settings, and tactics to counter changes in the threat and update mission software.

(2) WR-ALC/LNE is the logistics EW RC for domestic Air Force EW programs and is responsible for overall system-level support including operational flight programs (OFPs), engineering support tools, and support equipment software. In addition, WR-ALC/LNI, Robins Air Force Base, is the threat change analysis center and operational and logistics EW RC for international programs support. The logistics and operational RCs perform test validation of data.

d. Multiservice Electronic Warfare Data Distribution System (MSEWDDS). Implementing reprogramming changes has become more timely and simple by using the MSEWDDS. Reprogramming data products and analysis are available to support operational users. The advantage of this system is its ability to provide reprogramming information to concerned users when it is available. Access to the MSEWDDS is accomplished with compatible encryption equipment, cryptographic keys, and passwords used to log into the system. Privileges are assigned based on user requirements. For example, operational units can access intelligence summaries and download mission data sets (MDS) based on the EW/TSS organic to their unit but have no privileges to load a MD set on the MSEWDDS. In contrast, software support centers (SSCs) and TSSCs/SSAs can load and update MD set information but have restricted access to intelligence summaries (to protect operational security requirements). Service threat change analysis centers and FIWC EWRL are responsible for maintaining access and privilege lists for their service. Principal products posted and maintained on the MSEWDDS are—

- (1) Threat analysis summaries.
- (2) Threat change parameters.
- (3) Draft MD set parameter recommendations.
- (4) New MD set data files.
- (5) Threat data and analysis request responses.
- (6) Draft SIMs.
- (7) RIMS.
- (8) OFPs.

e. Figure III-1 depicts the reprogramming process with the major reprogramming organizations under the current architecture.

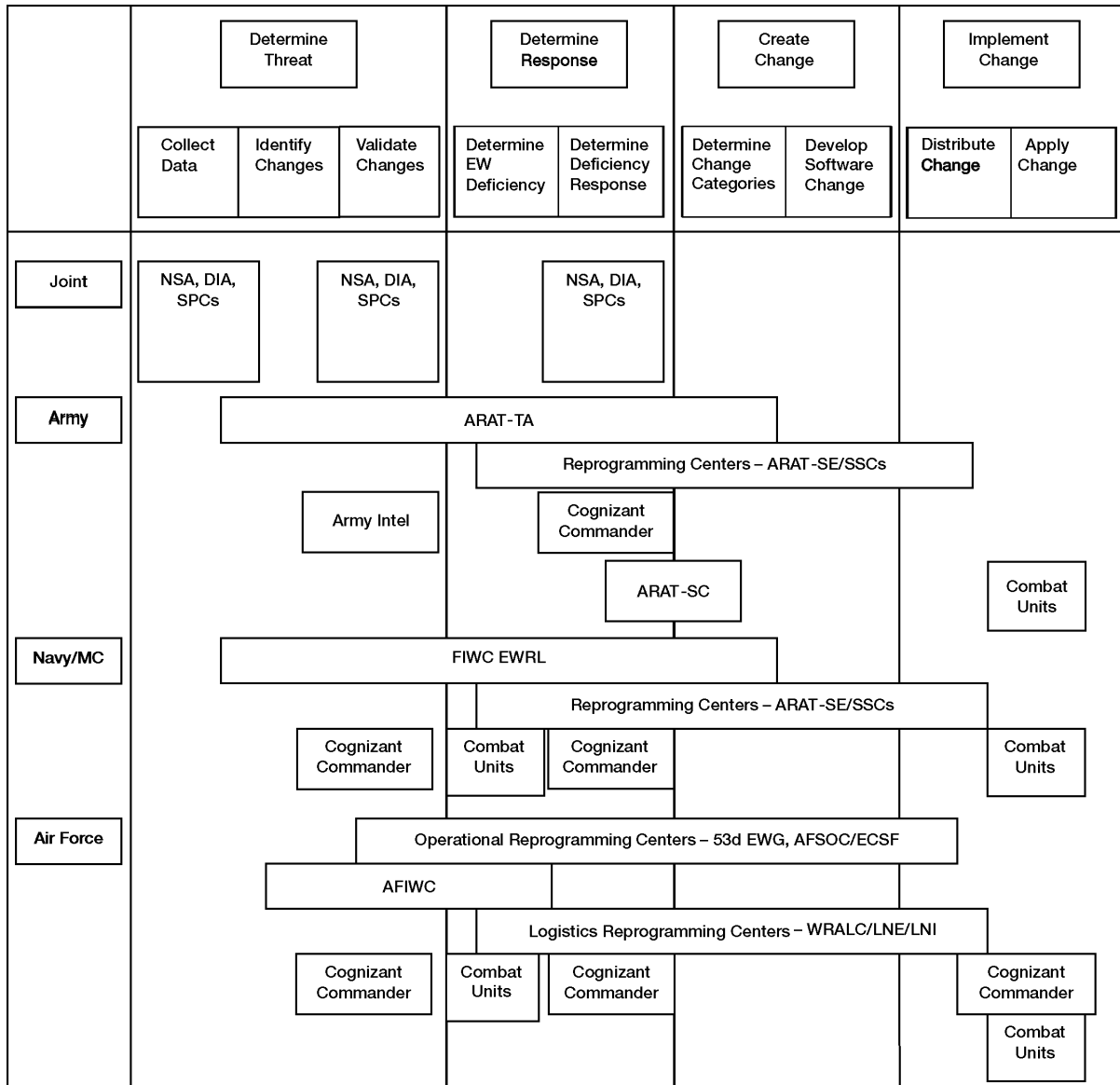


Figure III-1. Reprogramming Process Current Roles

NOTE: The MSEWDDS user’s manual can be downloaded from the home page for security requirements and detailed information can be found there on how to create an account. To create an account on the MSEWDDS using SIPRNET, input the IP address 207.84.75.01 into the address field of your browser to access the MSEWDDS home page, select connect, then signup, and follow the screen prompts to create a new account. Please refer to the MSEWDDS user’s guide for additional security information required to enable each account.

3. The Reprogramming Process

a. Process Phases. The reprogramming process is divided into four phases: determine the threat, determine the response, create the change, and implement the change. Figure III-2 provides an overview of the reprogramming process. JP 3-51 presents a more detailed top-level view of this process.

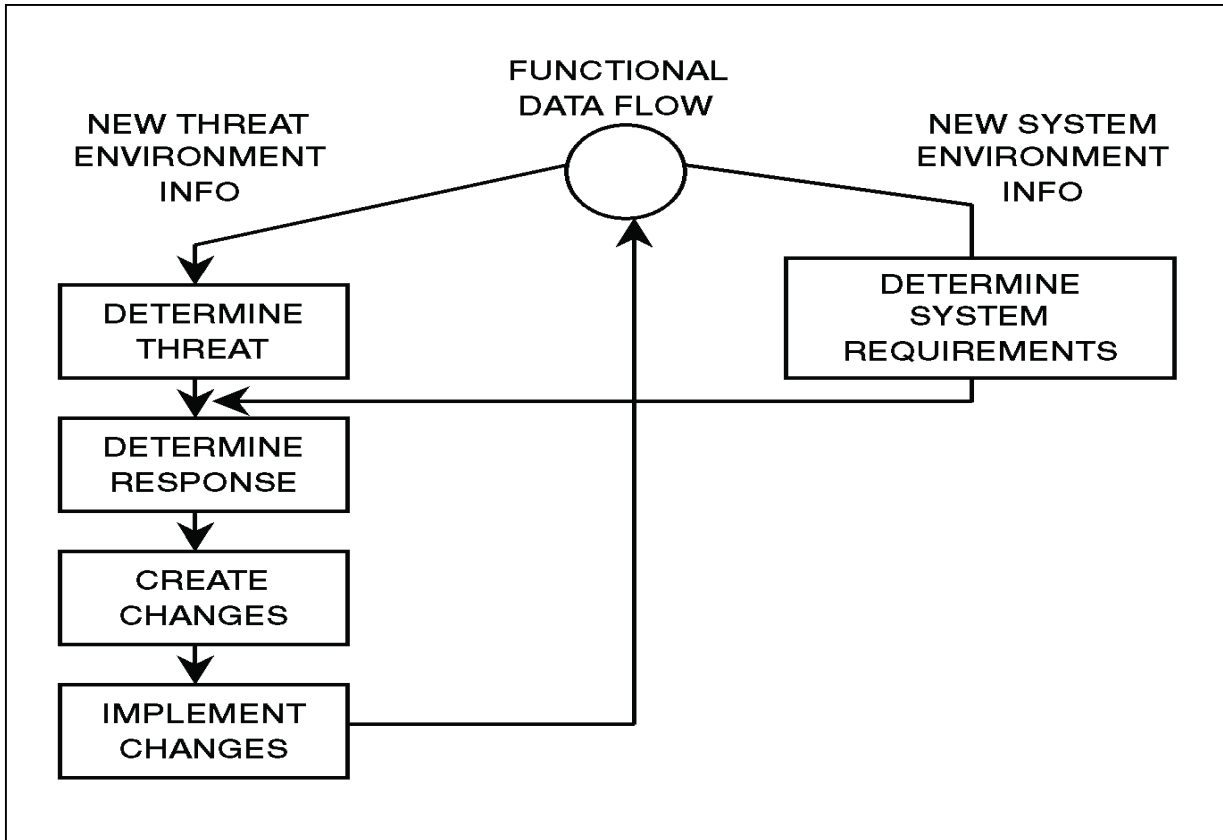


Figure III-2. Reprogramming Process

b. Determine the Threat. Determining the threat is subdivided into three steps: collect data, identify changes and validate changes.

(1) Collect Data. The first step in determining the threat involves collecting all-source threat system parametric information and reporting that data to intelligence processing centers, service EW flagging activities, and SPCs. The SPCs develop detailed parametric analyses of threat radars. The resultant assessed technical intelligence is consolidated into a combined EWIRDB product with detailed parametrics for more than 2000 radars. Besides these assessed parametric values, the EWIRDB includes the observed values provided by NSA and the values of U.S. owned and operated systems in the USELMSDB.

(2) Identify Changes. The second step in determining the threat is identifying threat changes and assessing the impact of these changes on friendly EW or TSS equipment. Flagging is a mixture of operations and intelligence functions. Threat signature data is compared with current DB holdings. Intelligence analysts at the theater SPCs and service EW flagging activities identify signal-related (parametric)

variances. Service reprogramming personnel flag or identify those threat changes affecting their EW or TSS equipment using DB information and EW flagging techniques or models. Flagging models are software simulations that account for the hardware capabilities of the TSS and its operation based on the programming of its MD sets. At AFIWC, flagging engines are connected to intelligence message systems and to raw pulse-level data that includes collected parametric information. As messages or pulse trains are received, they are filtered and run against the models. Collector bias (that is, collector contamination of the data) must be understood and considered during the identification process.

(a) Within the Air Force, 453 EWS/EWF operates automated flagging models using conventional EW system models and selectively improved flagging technique (SIFT) models. Observed ELINT data is compared to the data programmed in an EW system to determine if the threat will be correctly identified and the appropriate response elicited. AFIWC provides results of model operation to the Air Force operational EW RCs and MAJCOMs.

(b) The Army's ARAT-TA scans collect ELINT using flagging models developed for specific EW/TSS. These models sort through hundreds to thousands of daily intelligence messages. "Flagged" signals alert ARAT personnel to conduct in-depth analysis and system-impact assessments if applicable.

(c) The Navy's FIWC EWRL receives ELINT data from national and tactical resources on a NRT basis and has electronic access to historic ELINT data for regression testing. NRT information, in message format, is received electronically and mechanically parsed. The ELINT data is filtered for relevancy (for example, collector bias and type ELINT notation [ELNOT]) and compared against 120 plus worldwide and geographical EW libraries used in EW equipment or systems on Navy air, surface, and subsurface platforms. Where the comparison process indicates that an ambiguity or no identification will occur, the ELINT data and the corresponding EW libraries are "flagged." The flagged data is correlated to potential platforms or weapon systems; a report is generated for an ES system DB operator to review and adjudicate. Consistent with system impact, threat assessment and priorities, and operational environment of naval forces, a reprogramming action may occur immediately or in the next EW library update.

(3) Validate Changes. The final step in determining the threat is validating threat changes. Once a signal-to-system correlation is made, the threat change must be validated to ensure an actual threat change exists. An essential part of this phase of analysis is to validate that a detected threat change is not caused by a signature anomaly, thereby voiding the need for a reprogramming action. Factors such as engineering considerations of threat system capabilities and operational considerations of threat system employment play a major role in validation.

(a) SPCs have resident foreign threat system experts and are designated as validation authorities in peacetime and contingencies. SPCs validate threat changes in peacetime and during hostilities. They forward these validated changes via secure communications (DMS, SIPRNET e-mail, etc.) to the threat change analysis centers, FIWC EWRL, and EW RCs for application.

(b) Intelligence production centers (IPC) responsibilities include verification, tracking and maintaining tactical orders of battle (OOBs) and locations of current threats.

(c) All the services acknowledge that considerations outside of the intelligence arena drive some reprogramming changes. This can include a variety of internal and external considerations that may prompt reprogramming actions, including field inputs. Operational units can impact the reprogramming process by using existing reprogramming messages. The Army and Air Force use OCR messages. The Navy and Marine Corps use the TCAR message to insert their service concerns into the reprogramming cycle. (See Appendix C for message formats. AFI 10-703 has more detailed procedures for USAF messages.)

- Parametric Threat Change Validation (Crisis and/or Wartime).

Validating threat system parametrics is a sophisticated engineering-level challenge that involves examining technical electronics intelligence (TECHELINT) and MASINT reporting considering all-source threat system capability assessments. National SPCs validate parametric entries in the national EWIR and MASINT. These centers also serve as technical advisors to the IPCs in peace and war.

- Components of a Functional Parametric Threat Change Validation (Crisis/Wartime). Figure III-3 defines the components of a functional parametric threat change validation model.

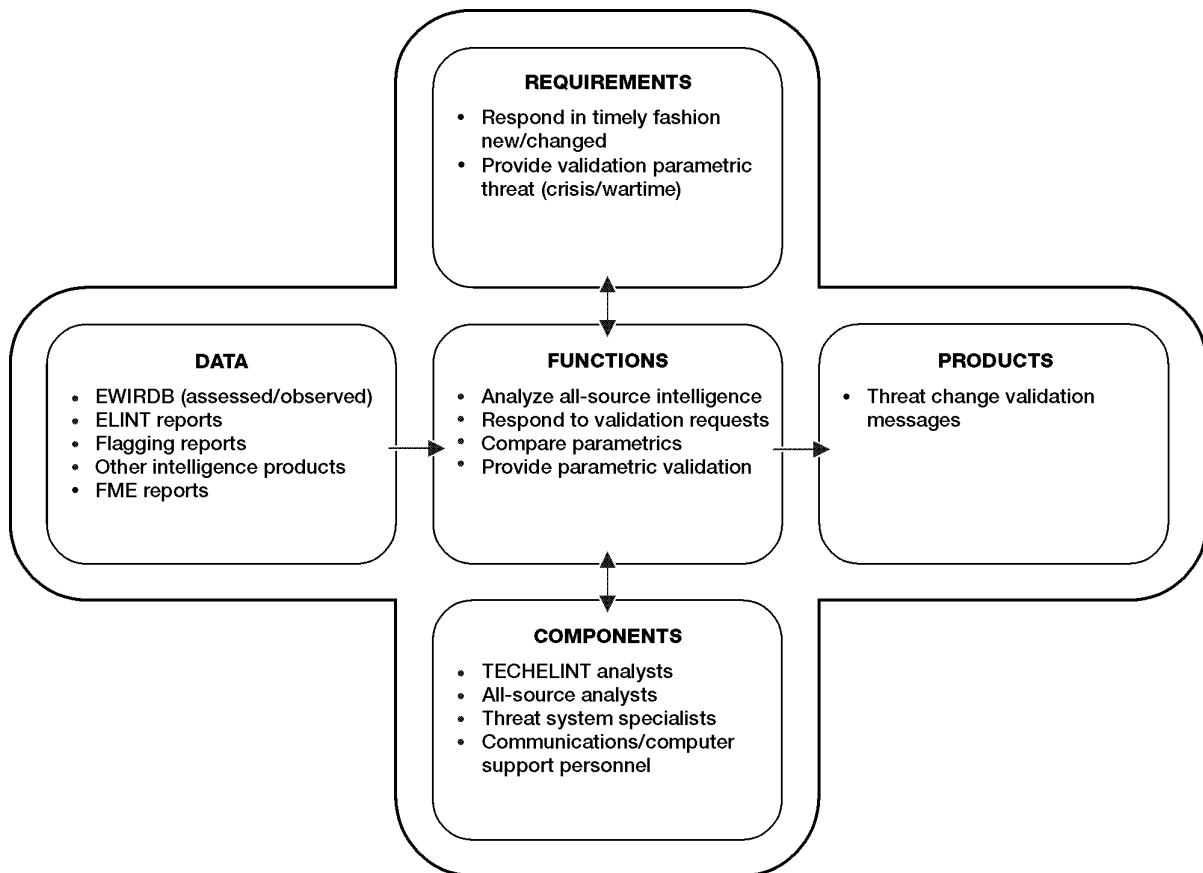


Figure III-3. Parametric Threat Change Validation (Crisis/Wartime)

(d) Requirements. Timely and accurate validation of changes in threat system parametrics is vital in providing the EW reprogramming community the

actionable data needed for responding to the changing battlefield. During crisis/wartime, signal activity levels increase as does the probability of employment of new/changed systems or modes of operation.

(e) Data. The EWIRDB remains the comprehensive baseline of current validated data during crisis/wartime. However, since the EWIRDB has a lengthy update cycle (one-three years for any emitter), more attention is given to the latest data collected from the crisis or battle area. This includes ELINT reports and tactical ELINT data. Flagging reports identify potential problems based on the latest tactical ELINT with fielded EW systems. Foreign military exploitation (FME) reports are generally not as responsive because of the time necessary to set up and exploit foreign equipment. However the quality of such data, if available, can be exceptional.

(f) Functions. All-source intelligence is analyzed for indications of variances from current holdings on threat parametrics. SIGINT is the primary discipline that reveals such variances. Parametric validation involves carefully considering the feasibility of an apparent threat change. Analysts must account for collector bias in these deliberations. They must also consider the possibility of system malfunctions.

(g) Components. Validation is a judgment requiring a detailed engineering-level understanding of the threat system and its electronic parametrics. The decisions are collective efforts with all-source analysts and threat system specialists.

(h) Products. The threat change validation message (TCVM) is the primary method used by the SPCs to communicate new validations to the reprogramming community. During peacetime most validations lead to the entry of new data in the monthly EWIRDB updates. Formal record-copy validation messages may be preceded by direct discussions via secure telephone or by other means to communicate information to those likely to be impacted.

c. Determine the Response.

(1) Validated threat change information is used to assess its impact on friendly EW and TSS equipment before a decision is made whether to initiate reprogramming. JP 3-51 specifies two parts to determine the response: determining deficiencies and determining the response to deficiencies.

(a) Determining deficiencies involves the analytic review to ascertain the reason EW/TSS equipment cannot provide appropriate indications, warning, or countermeasures. Causes for such deficiencies may include parametric variations that are not covered in the EW MD, ambiguities in signal recognition/sorting, the threat signal not being loaded in MD, or a faulty or ineffective jamming technique response.

(b) Determining the response to deficiencies requires applying considerable engineering judgment to determine a remedy for the deficiency. A response may entail a change to MD or the OFP.

(2) Threat Change Analysis Function. Threat change analysis functions exist in all the services in varied forms with varied levels of responsibilities. Figure III-4 defines the basic requirements, data, functions, components, and products of a functional threat change analysis model to evaluate proposed concepts.

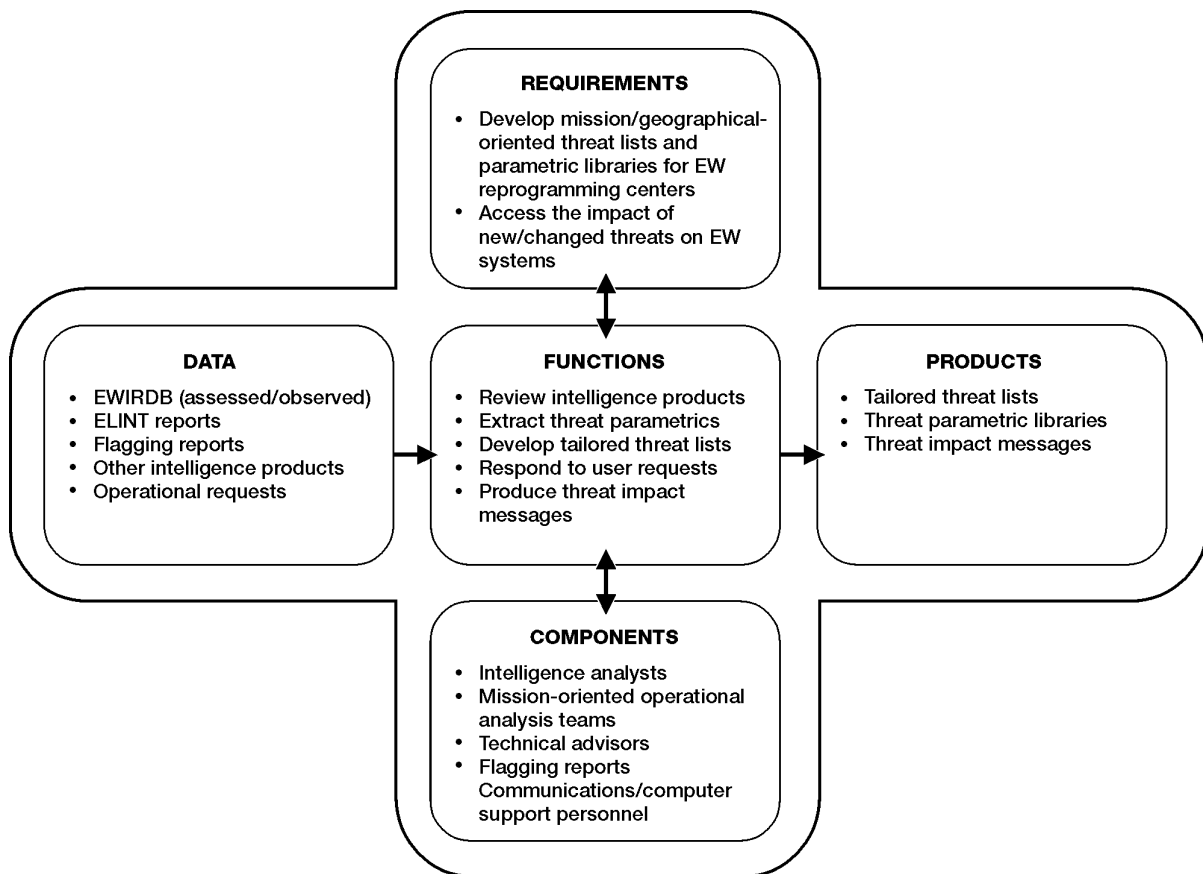


Figure III-4. Threat Change Analysis

(a) Requirements. The threat change analysis function provides an initial assessment of the impact of new/changed threats on the individual EW systems (this includes EW flagging, determining EW deficiencies, determining response to deficiencies, and determining change categories actions). In addition, developing mission/geographically-oriented threat lists and parametric libraries for individual EW systems also are included in this function.

(b) Data. National and service intelligence agencies provide observed and assessed intelligence data to support reprogramming requirements. The EWIRDB is the primary source of parametric data for reprogramming actions but there are other databases that provide additional and/or tailored information for reprogramming. Specialists directly view ELINT reports to provide a NRT assessment of the threat situation. Detailed intelligence reports are available for specific threat systems based on assessments, evaluations, and exploitation.

(c) Functions. Threat change analysis is based on a review of the intelligence products to identify and extract new/changed threat parametrics. Identification of changes includes, but is not limited to, automated flagging of ELINT reports based on EW system models to filter the signals of interest. Analysts use the new/changed data to develop tailored threat lists and parametric libraries for the individual EW systems based on specific platform mission requirements. Teams

performing the threat change analysis function are the source of technical expertise for the operational user. These teams also identify EW system deficiencies.

(d) Components. Within the threat change analysis function, intelligence personnel process intelligence information; operational personnel assess and coordinate the impact of new/change threats on the mission; a technical advisor coordinates EW system limitations with system engineers; and communications/computer support personnel maintain the computer tools and communications links.

(e) Product. Mission/geographical-oriented threat lists and parametric libraries are developed and distributed to the reprogramming centers for developing EW system MD. The SIM is sent to operational users to identify EW system deficiencies related to new/changed threat environments.

(3) Joint/IO Decision Process. The IO cell reviews the number of threat systems changing and their impacts to friendly systems, current targeting list, ATO, and operations tempo as part of the reprogramming recommendation. If only a single threat has changed parameters, yet the impact to USAF, USA, USN, and USMC systems is significant, destroying the threat should be considered. If the OPLAN does not commit friendly systems to an area where threats have changed, the IO cell should communicate this to the reprogramming centers to allow prioritization of more critical reprogramming actions. The IO cell needs to be actively involved in theater issues driving reprogramming and communicate decisions to the services and reprogramming centers.

d. Create the Change. During this phase several actions happen including developing and generating the change, testing/validating the change, and documenting the change. This document focuses on the three most common types of reprogramming: mission data development and coding, EA jamming techniques, and OFP development.

(1) Mission Data Development and Coding. MD development and coding involves converting tailored threat lists, their associated parametrics, and other intelligence data into formatted data ready for loading into an EW system. The heart of this process is parametric ambiguity analysis and resolution. This process applies to RWRs and the receiver front ends of jammers. Paragraph (2)(d) addresses the reprogramming of jamming techniques. Figure III-5 depicts the basic requirements, data, functions, components, and products of a functional MD development and coding model.

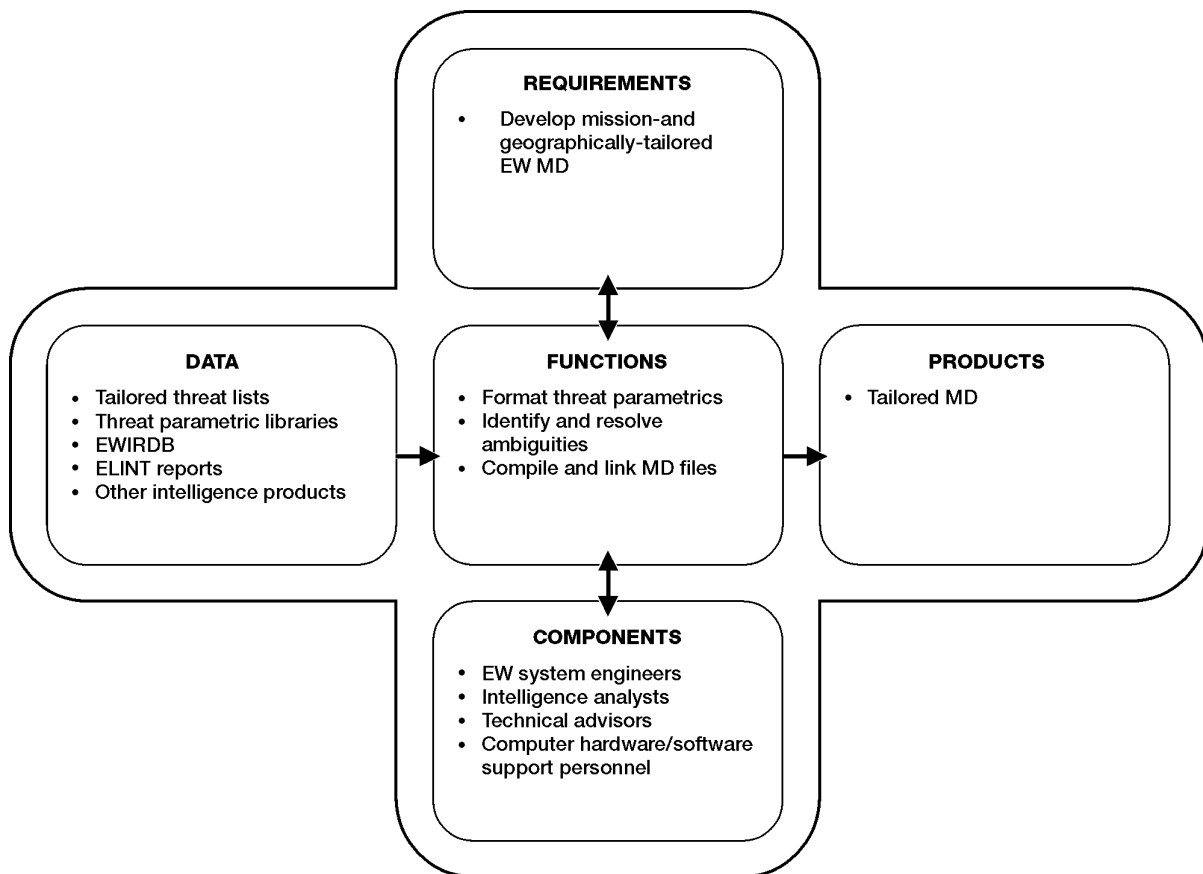


Figure III-5. Mission Data Development and Coding

(a) Requirements. The MD development function provides mission and geographically tailored MD for EW systems and includes: determining the response to deficiencies, determining the change category, and developing the software change actions defined in JP 3-51.

(b) Data. The threat change analysis function provides tailored threat lists and threat parametric libraries to support the MD development function. Supplemental data sources include the EWIRDB, ELINT reports, and numerous other intelligence products. MD support and programming, using MASINT data, requires a completely new knowledge base and set of interpretation skills when compared to EWIR analysis. Significantly greater computer resources are also required. The NGIC is the DOD executive agent for the NTSDS, which provides a common access point/method to the numerous MASINT databases held at various data centers.

(c) Functions. The key task in this process is the identification and resolution of threat ambiguities. The reprogrammer must resolve ambiguities to provide a single response to any given set of threat parameters and system settings. The reprogrammer develops and programs parametric resolve tables or trees to enable the EW system to discriminate between similar threats. In numerous cases, threats are beyond the EW systems capability to discriminate; nonetheless, the reprogrammer must select an appropriate response.

- The reprogrammer may accomplish these tasks manually or with the aid of automation tools ranging from calculators to sophisticated, state-of-the-art computer systems. However, even the most sophisticated MD tools rely heavily on the reprogrammer's expertise. At this time, ambiguity resolution is more of an art than a science.

- An additional function is to reformat, compile, and link (as applicable) parametrics (threat and other system settings) to form a MD. The MD may require special "packaging" for distribution and accommodation of loading equipment requirements. Thus, at this point, MD may or may not be "machine-ready."

(d) Components. The MD development and coding function requires EW systems engineers to develop and code MD. EW systems engineers also identify and resolve threat ambiguities. They accomplish these tasks using a variety of computer hardware and MD development and analysis tools. Intelligence analysts, technical advisors, and support personnel support them.

(e) Products. Mission and geographically tailored MD sets are developed and distributed to combat units.

(2) EA Jamming Technique Reprogramming. Figure III-6 shows a functional model depicting the EA technique reprogramming processes.

(a) Requirements. Techniques may be applied to classes of threats on a one-to-one techniques-to-threat basis or on a very specific technique-to-threat mode basis. The trend is away from the former and toward the latter.

(b) Data. The EA jamming technique reprogramming function requires data from many sources. Threat lists identify the specific threats to include in the MD and the required technique assignment. The EWIRDB plays an important role in technique reprogramming but must be heavily supplemented with other sources. For those reprogramming actions categorized as cut-and-paste and cookbook reprogramming, the single most important sources are existing versions of MD. When developing and optimizing new techniques, sources include existing MD, test reports, FME reports, and threat description documents.

(c) Functions. Key tasks in this process include programming existing techniques into EW system MD and/or OFPs; developing new/revised techniques through analysis; and optimizing techniques through testing.

(d) Components. The EA jamming technique reprogramming function requires EW systems engineers to program existing jamming techniques into MD and, in a limited number of cases, OFPs. When a jammer does not have an effective technique available to counter a threat, EW systems engineers develop new techniques through extensive threat analysis. As test assets, especially foreign material, become available, test teams engage in extensive tests to optimize techniques against the threat. Intelligence analysts, technical advisors, and support personnel support test teams and engineers.

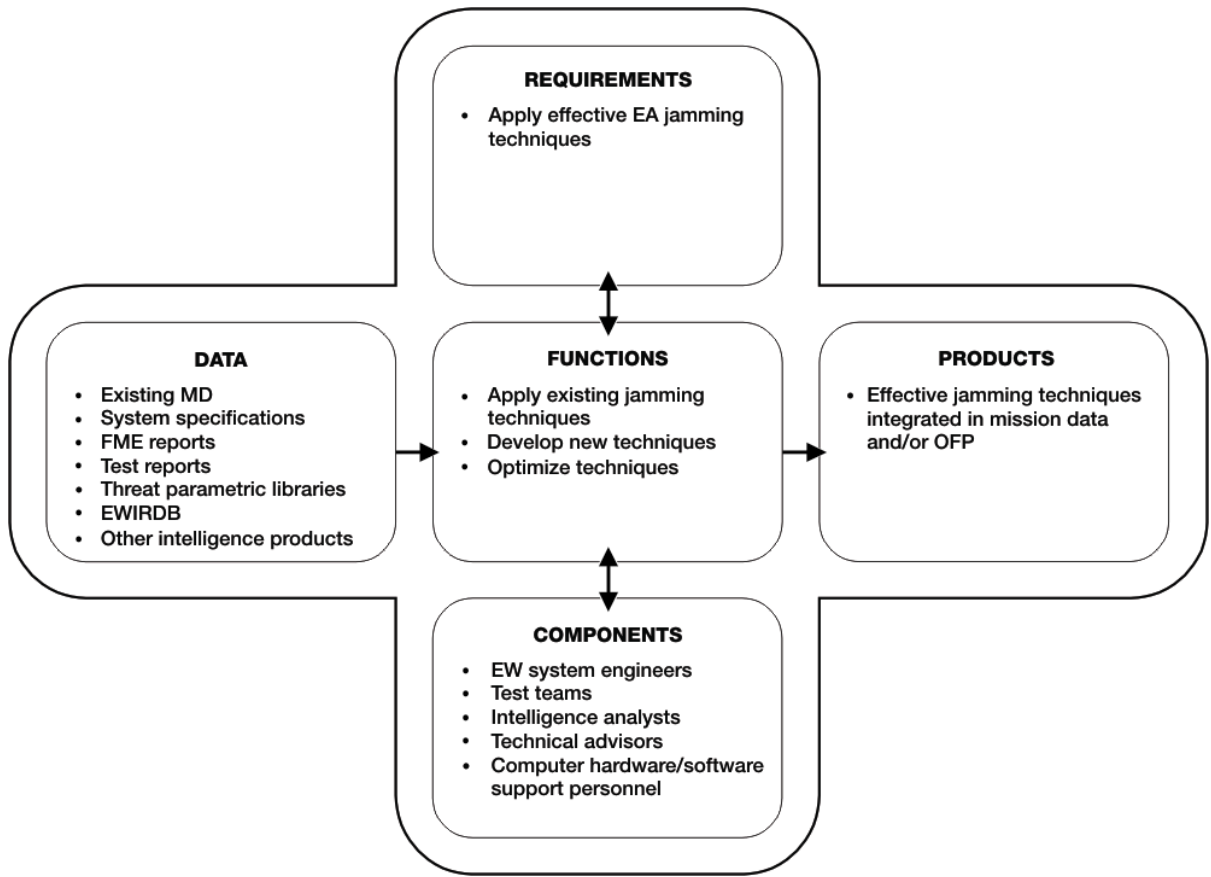


Figure III-6. EA Technique Reprogramming Process

(e) Products. The reprogramming process produces new and optimized jamming techniques for jammer MD or, in a limited number of cases, OFPs. Once developed and, when possible, optimized to counter a threat, these techniques become the standard countermeasures for given jammer/threat combinations.

(3) OFP Development. OFP development and coding involve writing/modifying software to implement the changes and testing to the level necessary to verify correct performance. Figure III-7 depicts the OFP development and coding functional model.

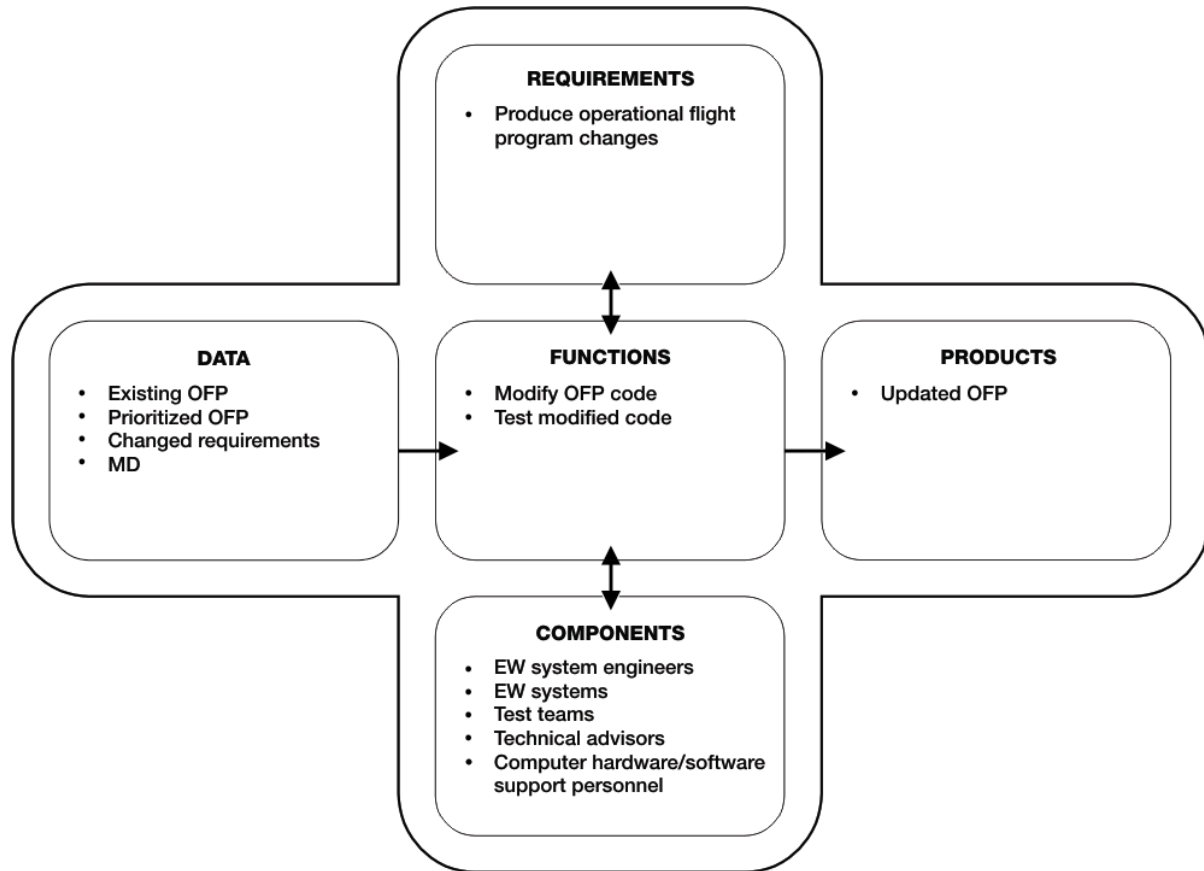


Figure III-7. OFP Development and Coding Functional Model

(a) Requirements. The OFP development and coding functions provide OFP updates for EW systems. These functions include: determine the response to deficiencies, determine the change category, and develop the software change actions defined in JP 3-51.

(b) Data. The OFP development and coding functions use the existing OFP as a baseline. Prioritized OFP change requirements guide the process. EW system MD is used in the process to test and verify correct implementation of OFP changes.

(c) Functions. The key task in this process is to modify OFP software according to established software development procedures. The process also involves laboratory and, in some cases, operational testing of software updates to verify desired performance.

(d) Components. The OFP development and coding functions require EW systems engineers to develop and code EW system OFPs. They accomplish these tasks using a variety of computer hardware, MD development, and analysis tools. Technical advisors, support personnel, and test teams support the engineers.

(e) Products. Updated OFP software is developed and prepared for distribution to combat units.

e. Implement the Change.

(1) Software changes are distributed to the users and loaded in the EW system as directed by theater component commanders. The distributing and loading reprogramming changes vary widely from system to system and among the services.

(2) Distribution of the change is accomplished through logistics channels, Defense Message System (DMS) channels, electronic media, or any other means available. Reprogramming data is archived at each service's reprogramming center. Primary storage of the data is on the MSEWDDS accessed through the Secret Internet Protocol Router Network (SIPRNET) or secure telephone unit-III (STU-III).

Appendix A

PROCEDURES FOR JOINT COORDINATION OF EW REPROGRAMMING

1. Process

The EW reprogramming process can be divided into four distinct phases: determine the threat, determine the response, create the change, and implement the change.

a. Phase I, Determine the Threat. (See Figure A-1.)

(1) During normal or contingency operations, intelligence collectors intercept, photograph, and report EW parametrics and radar specifications.

(2) Based on tasking from the national intelligence structure, they record and report this information to intelligence processing centers (IPC) and SPCs. IPCs include theater joint intelligence centers (JIC), joint analysis center (JAC), and other operational and tactical intelligence users (such as carrier task forces).

(3) When an IPC detects a change in a threat system in its area of interest, it transmits a TCAR message to all the service reprogramming centers (SRCs) and Army and Air Force flagging centers where they will evaluate if any of their systems in their areas of interest are affected. Info copies of the TCAR are sent to the agencies identified in Figure A-1. If it is found that none of the systems in their area of interest is affected, the SRC and/or flagging center will transmit a system impact message (SIM) to the originator of the TCAR stating there is no impact with info copies to the agencies identified in Figure A-1. No further action is required.

(4) If, however, an SRC or flagging center identifies one or more of their systems may be affected by the change, the affected SRC transmits a threat change validation request (TCVR) to the appropriate SPC for analysis and confirmation.

(5) The SPC analyzes the possible threat change to determine if the radar system is capable of the change, based on known system characteristics. Once analyzed, it transmits a threat change validation message (TCVM) as described above to the SRC with info copies to agencies outlined in Figure A-1.

(6) Finally, the SRCs determine how their systems are affected and issue a SIM to begin phase II. The SIM includes the system affected, how the system is affected, and suggests interim tactics, techniques, and procedures (TTPs) to defeat the threat change while implementing follow-on phases.

b. Phase II, Determine the Response. Determining the response requires significant engineering judgment and coordination. Possible options include destroying the threat, changing tactics, avoiding the threat, and/or reprogramming EW equipment through changes in mission data or operational flight programs. If the decision is made to reprogram, SRCs develop any TTPs to incorporate with the new software as part of the reprogramming impact message (RIM).

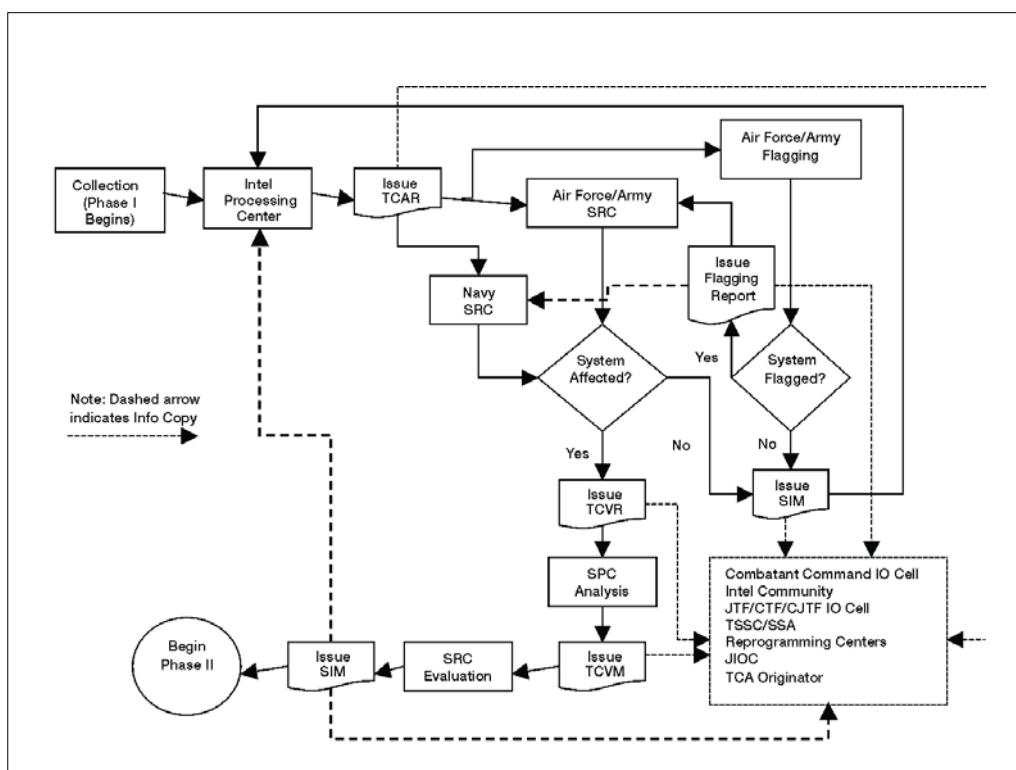


Figure A-1. Phase I: Determine the Threat

c. Phase III, Create the Change. Each service creates the required equipment or tactic changes and distributes them to its components. The SPCs provide additional technical analytical support to the reprogramming centers on request. Any proposed change, especially changes to jamming techniques, must be deconflicted with other friendly systems within the area of responsibility to ensure the reprogrammed equipment does not interfere with friendly systems. Thus, EW planners must have access to all friendly EW systems and reprogramming products. The electronic warfare coordination cell (if established) accomplishes this process.

d. Phase IV, Implement the Change. Each service component in the area of responsibility must determine the appropriate action to take to defeat the change. It can either take the suggested TTP from the SRC, or develop its TTP to defeat the change. The EWCC should be informed of the selected TTP to coordinate and deconflict with the other components and allies.

2. Identification Process

a. Intelligence collection systems, regardless of tasking authority, may collect and report electromagnetic changes of threat systems. Analysts identify suspect signals from ELINT reports, which are provided to NSA, DIA, theater and component intelligence centers, flagging centers, and SPCs. Additional reports, such as operational reports (OPREPS), mission reports (MISREPS), and in-flight reports (FLTREPS) may be reviewed to determine previously unidentified radar modes for clues to threat changes. When a threat system changes parameters, modes, or tactics, the identifying

agency transmits a TCAR to the SRCs; it also transmits the TCAR to the agencies in Figure A-1 as INFO addressees.

b. After receiving the TCVR, SPC analysts must compare the new signal parametric values to the observed and assessed values provided in the EWIRDB. The IPC assists the SPC with resident signal history files to determine if the parameters have been previously observed from that location and/or from multiple locations. Collector signal irregularities also should be compared against collector idiosyncrasies and limitations. If sufficient confidence exists in the SPC analyst's judgment of the reported signal characteristics, and especially if different collectors report the same parameters, the values may be considered to represent a valid threat mode of operation, which may or may not be intentional.

c. SPC analysts assign the validated threat change a level-of-confidence qualifier. Once completed, the SPC transmits a TCVM to the SRCs with info copies to the TCAR addressees. The TCVM will be a free text message with as much information as possible about the new operating mode and an assessment of the analyst's confidence in the new data. The TCVM includes a POC for the assessment.

3. TCVM Criteria

a. Radio frequency (RF), pulse repetition frequency (PRF), pulse repetition interval (PRI), scan period (SP), effective radiated power (ERP), pulse duration (PD), polarization changes and beam width (BW) are several of the technical parametric values to consider when validating a threat change. However, technical parametric data variation should not function as the sole criterion in TCVM. SPC engineering assessments, sound analysis, and good judgment must be used along with available all-source intelligence. SPCs should use the following guidelines and associated terminology in the TCVM process.

b. Quantity of Intercepts. More than one intercept of an unidentified or misidentified signal is desired before confirming a threat change. For instance, if several identical radars shift parameters, intentional parametric shifts can be suspected. If there is only one intercept or a concurrent lack of intercepts of parametric shifts in identical systems, the observed parametric changes may be the result of maintenance problems or operator error, which should be reported as such.

c. Collector Bias. Because collection systems differ in features, such as capability, modes of operation, mission, and look angle; analysts evaluating possible threat change candidates must be familiar with the procedures and capabilities of the collection platforms.

d. Current Situation. All-source political-military intelligence, including the most current order of battle, must be considered because it would be highly unlikely to intercept a large number of emitters operating with new parameters or modes with no other crisis indicators, such as significantly increased tensions coupled with increased military activity. This consideration is important for identifying those single system mode changes due to a maintenance malfunction, where destroying that single site would probably be a more appropriate response than reprogramming the fleet.

e. Emitter Parametric Characteristics. Intentional system parametric changes caused by either existing hardware/software functions or operational and procedural changes are the prevalent forms of WARM. Therefore, intrinsic engineering and physical limitations provided by SPCs and contained within the EWIRDB can help

bound the TCVM problem. The SPCs provide these values after lengthy analysis of all available forms of intelligence over a period of time. For each assessed value in the EWIRDB for a given threat system, the SPCs analyst provides a confidence factor associated with that assessment. These confidence factors are available in the DIA document "Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming" on page 15. This document is available at the following Joint Worldwide Intelligence Communication System (JWICS) link:
http://www.dia.ic.gov/proj/ewirdb/EWR_Procedures.html.

f. Coordination. A potential threat change exists if the new parameter values fall within the EWIRDB but outside the national technical ELINT database (KILTING). If the reported parameters are outside the EWIRDB, the SPC analysts must initiate an effort to verify the parametric values to determine if the reported parameters represent a potential threat change.

g. Level of Confidence Qualifiers

(1) Factors. A significant amount of analytical judgment comes into play when making a TCVM determination. The level of confidence that the analyst has in making a judgment is based on the following factors:

- (a) The quantity and quality of collection against the signal.
- (b) The type and fidelity of the collection platforms used.
- (c) The amount and quality of all-source intelligence reporting relative to the context of the situation.
- (d) The quality and completeness of the in-theater parametric databases.

(2) Qualifiers. Assigning level-of-confidence qualifiers is required, as a threat change in one theater may have reprogramming or tactics implications in other theaters and may cross service lines. In addition to the qualifier, additional SPC clarification may be appropriate. Such clarification is critical to the operational user who decides whether to make theater-wide (or worldwide) reprogramming changes or tactics and procedures changes. These qualifiers are available in the DIA document "Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming" on pages 15 and 16. This document is available at the following JWICS link:
http://www.dia.ic.gov/proj/ewirdb/EWR_Procedures.html.

4. U.S. System Reprogramming

In addition to the threat-driven reprogramming process described above, U.S. information will be updated in accordance with CJCSI 3210.03A, *Joint EW Policy*, Appendix B to Enclosure A, U.S. Electromagnetic Systems Database (USELMSDB) Plan.

Appendix B

POINTS OF CONTACT (POCs)

1. Joint Information Operations Center EW Branch

JIOC/J542
2 Hall Blvd, Ste 217
San Antonio, TX 78243-7008
DSN: 969-3643/4974/3256

2. U.S. Army

a. U.S. Army Land Information Warfare Activity (LIWA)

Commander Land Information Warfare Activity (LIWA)
ATTN: IAIW-DO-TA 8825 Beulah Street, Suite 211 Fort Belvoir, VA 22060-5246
Voice: DSN 235-1819 Comm: (703) 706-1819
FAX: DSN 656-1185 Comm: (703) 806-1185

b. ARAT-TA-Systems: APR-39 series; ALQ-136 series; APR-44 series; Suite of Integrated Radio Frequency Countermeasures (SIRFC); Suite of Integrated Infrared Countermeasures (SIIRCM).

ATTN: Chief ARAT-TA
203 West D Avenue, Suite 103
Eglin AFB, FL 32542
Voice: DSN 872-8899 Comm: (850) 882-8899
FAX: DSN 872-4268 Comm: (850) 882-4268

c. Army Reprogramming Analysis Team - Project Office (ARAT-PO)

Building 1210, Room 222
Fort Monmouth, NJ 07703
Voice: DSN 992-1337 Comm: (908) 532-1337
FAX: DSN 992-5238 Comm: (908) 532-5238

d. Electronic Warfare Officer Course

ATTN: ATZQ-BDE-OH
1/145 Aviation Brigade
Fort Rucker, AL 36362
Voice: DSN 558-2379/9426 Comm: (334) 255-2379/9426
FAX: DSN 558-2637 Comm: (334) 255-2637

e. Aviation Reprogramming Service Center - Fort Rucker
ATTN: ATZQ-CDC-T Building 508
Ft Rucker, AL 36362
Voice: DSN 558-9334/3500 Comm: (334) 255-9334/3500
FAX: DSN 558-1165 Comm: (334) 255-1165

f. HQ U.S. Army Intelligence and Security Command (INSCOM) MASINT
Division

Commander, INSCOM, ATTN: IAOP-OR-MAS
8825 Beulah Street
Ft Belvoir, VA 22060-5246
Voice: DSN 235-1202 Comm: (703) 706-1202
FAX: DSN 656-1176 Comm: (703) 806-1176

3. U.S. Navy/Marine Corps

Fleet Information Warfare Center (FIWC) /Electronic Warfare Reprogrammable
Library (EWRL)
2555 Amphibious Drive
Naval Amphibious Base
Norfolk, VA 23521-3225
DSN: 537-4136/4137 Comm: (757) 417-4136/4137
FAX: 537-4154 Comm: (757) 417-4154

4. U.S. Air Force

MAJCOM POCs:
ACC/DOZO Langley AFB, VA DSN 574-5905
PACAF/DOTW Hickam, HI DSN 315-449-5182
USAFE/DOTW Ramstein AB, GE DSN 314-480-6582
CENTAF Shaw AFB, SC DSN 965-4360

USAF Reprogramming Centers POCs:

53 Wing EWIR POCs
53 EWG/ERC
203 West D Ave
Suite 103
Eglin AFB, FL 32542 DSN 872-2166/Comm: (904) 882-2166

HQ AFSOC ECSF

265 Perry Street
Robins AFB, GA 31098-1607 DSN 468-2010/Comm: (478) 926-2010
Classified DMS: AFSOC ECSF-PW(S)

General Reprogramming and MSEWDDS Info

EWS/EWP (MSEWDDS Support) DSN 872-2166/Comm: (850) 882-2166
MSEWDDS IP address: 207.84.75.101
HQ AFSOC ECSF DSN 468-2010

Specific Systems POCs:

HQ AFSOC ECSF DSN 468-2010
Systems: Wide body and rotary wing (AFSOC/AMC/AFRC/ANG C-130 variants, MH-53J, HH-60, CV-22, C-5, C-17 and C-141)
36 EWS/EWC DSN 872-2052/3319/8742
Systems: ALQ-131, ALQ-184, ALR-56M, ALR-69, ALE-40, ALE-45, ALE-47
68 EWS/EWS DSN 872-2827/2325/9713
Systems: ALIC, HTS, HARM, EC-130E COMPASS CALL, EF-11/EA-6B
36 EWS/EWE DSN 872-4642/4643
Systems: B-2, F-22, ALE-50
36 EWS/EWF DSN 872-5387
Systems: U-2, F-15 TEWS
36 EWS/EWI DSN 872-4042
Systems: B-1, B-52

Other Reprogramming Centers POCs:

WR-ALC/LN Robins AFB, GA DSN 468-2261
Systems: USAF EW operational flight programs development and EW systems SILs, sustainment and support, including EW SILs, flight line and test equipment

Air Force Information Warfare Center POCs:

453 EWS/EWF DSN 969-2021
102 Hall Blvd, Suite 302
San Antonio, TX 78243

Appendix C

REPROGRAMMING MESSAGE FORMATS

The joint reprogramming community uses existing reprogramming messages formatted to convey an aspect of reprogramming that may affect the service, agency, and warfighting unit. Examples of these messages are provided to facilitate communications among the reprogramming players and inform operational users of the information required in order to affect a particular reprogramming action.

Notes: Not all service-specific message formats are presented. Refer to AFI 10-703 for most current USAF PACER WARE message formats.

Classification of all message examples is for illustration purposes only.

SAMPLE FLAGGING REPORT (FLR) (Army and USAF Only)

FROM: AFIWC (453 EWS)

TO: RCs, MAJCOM EWIR POCs

CC: as required (other agencies when requested)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE FLR ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. (area) DATA PROCESSED BETWEEN (start date) AND (end date). COLLECTIONS FROM A POLYGON DEFINED BY THE FOLLOWING COORDINATES (coordinates defining the area of interest).

3. THIS REPORT CONTAINS FINDINGS THAT MAY CAUSE PROBLEMS FOR THE SUBJECT SYSTEM. IMPORTANT: PARAMETRIC INFORMATION FOUND IN SUMMARIZED SIGINT HAS INHERENT LIMITATIONS!

4. (data concerning intercept parameters and model responses)

5. (contact instructions if other than POC of message, otherwise not required)

6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)
(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**THREAT CHANGE ANALYSIS REQUEST (TCAR) MESSAGE
(ARMY/NAVY/USMC and INTELLIGENCE CENTERS)**

1. The unit/activity that recognizes a change or potential change in the EW threat environment initiates the TCAR. The TCAR should include a brief narrative of the problem or suspected threat change. The message should also include the following information, when available:

- a. System(s) affected.
- b. Parameters of the signal(s) detected and any other parametric comments.
- c. Date, time, and location of the threat detected.
- d. Any other pertinent data (e.g., air, surface or subsurface platforms active in the area, and a brief description of current operations).

2. Use the TCAR example provided here. It contains the correct format and a sample report.

FM: ORIGINATOR

TO: FLTINFOWARCEN NORFOLK VA/N9//

Applicable Unified Command Intelligence Center (IC)

INFO: Chain of Command

APPROPRIATE CLASSIFICATION//N03430//

OPER/NORTHERN FLEX//

MSGID/GENOPS/(Originator)//

SUBJ/THREAT CHANGE ANALYSIS REQUEST 001-97 (U)//

REF/A/DOC/CNO/DDMMYY//

AMPN/OPNAVINST 3430.23 (SERIES) TACTICAL ELECTRONIC WARFARE

REPROGRAMMABLE LIBRARY (EWRL) SUPPORT PROGRAM//

POC///

RMKS/1. (S) FOL DATA MAY REPRESENT AN EW THREAT CHANGE AND IS SUBMITTED FOR ANALYSIS AND SYSTEM IMPACT ASSESSMENT PER REFA:

A. AFFECTED SYSTEM(S): SLQ-32

B. SIGNAL PARAMETERS (READ: ELNOT/RF/PRF/PRI/PW/SCAN/TYPE) A123B/1111.1/2222.2/333.33/44.4/55.5/C

C. DATE/TIME/LOCATION: 281234Z0JUL97/12340N/01234EO

D. SUPPORTING INFO: DURING KORONAN PATROL OPS, USS HONOR, IN COMPANY WITH USS COURAGE, USS COMMITMENT AND TWO HMS LONDON CLASS CRUISERS, OBSERVED ONE KOMON CLASS PTG (KNOWN TO CARRY C800B) AND ONE FAHAD CLASS PB (KNOWN TO CARRY HERO MISSILE SYSTEM). FROM TIME ON STATION (271234Z9JUL96), ALL EMISSIONS WERE EVALUATED AND IDENTIFIED. AT 281234Z0JUL96, KOMON INITIATED A MANEUVERING TACTIC INDICATIVE OF MISSILE LAUNCH SEQUENCE. AT 291300Z5JUL96, FRONT LIGHTS RADAR TRANSMISSION CEASED AND PARAMETERS NOTED PARA 1B BECAME ACTIVE. DURING NEXT HOUR USS

HONOR REPORTED ALTERNATING EMISSION PATTERN BTWN FRONT LIGHTS
AND UNIDENTIFIED RADAR.

E. CONCLUSION: BELIEVE PARAMETERS PARA 1B INDICATE NEW OR WARM
MODE OF OPERATION FOR FRONT LIGHTS RADAR.//

DECL/XX//

**THREAT CHANGE VALIDATION REQUEST (TCVR)
(ALL SERVICES)**

DTG: DDTTTTZ MMM YY

Priority: Routine, Priority, Immediate, or Flash {select one}

FROM: Analysis Center (ARAT-TA)

TO: Theater Intermediate Processing Center (IPC), Scientific & Technical Intelligence (S&TI) Centers, Service Production Centers (SPCs)

INFO: Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), others

Classification: UNCLAS EFTO, Confidential, Secret {select one}

SUBJECT: JADE LANTERN - THREAT CHANGE VALIDATION REQUEST
TCVRY# (U)

REF: [MSGID, DTG, From, Subject] {as appropriate, TACELINT, FLG, or EWAR at a minimum}

1. (U) This is a [CODEWORD] message.
2. (Classification) A [threat system name] (ELNOT [XXXXX]) WAS NOTED OPERATING WITH THE FOLLOWING PARAMETERS: {be as specific as possible}
3. (U) REQUEST VALIDATION OF THIS INTERCEPT.
4. (U) POC IS [Name], [Unit/Organization], [Phone #(s) IDSN/CML}], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**THREAT CHANGE VALIDATION MESSAGE (TCVM)
(ALL SERVICES)**

FM (APPROPRIATE SPC)
TO FLTINFOWARCEN NORFOLK VA//N9//
53WG MHS EGLIN AFB FL//ARAT/ERC/ETI//
DIRLIWA FT BELVOIR VA//DO//
INFO CTF NINE FIVE FIVE
COMSECONDFLT//J36//
TF NINE FIVE FIVE
NAVSURFWARCENDIV DAHLGREN VA//T24//
NAVAIRWARCENDWPNDIV PT MUGU CA//41130GE/454220E//
COMNAVAIRWARCENWPNDIV CHINA LAKE CA//455300D/47HHOOD//
CDRCECOM FT MONMOUTH NJ//ANSCL/RD-IW-ET//
FLTINFOWARCEN DET SAN DIEGO CA//N3//
DIRMSIC REDSTONE ARSENAL AL//MSC-1B1//
NAIC WRIGHT PATTERSON AFB OH//TAE/TAER//
CDRNGIC CHARLOTTESVILLE VA//IANG-SBR//
ONI WASHINGTON DC//241//
APPROPRIATE CLASSIFICATION//N03430//
EXER/JTFEX 02-2//
MSGID/GENADMIN/(ORIGINATOR)//
SUBJ/THREAT CHANGE VALIDATION MESSAGE 001-02 (U)//
REF/A/DOC/CNO//12JUN92//
REF/B/RMG/FIWC//DTG//
NARR/REF A IS TACTICAL EWRL SUPPORT PROGRAM AND REF B IS
FLTINFOWARCEN TCVR MESSAGE.//
POC//
RMKS/1. FOL EMITTER(S) LISTED BELOW WAS/WERE DETECTED WITH THE
FOL CHARACTERISTICS:
A. SIGNAL PARAMETERS (READ: ELNOT/RF/PRF/PRI/PD/SCAN/TYPE)
A123B/1111.1/2222.2/333.33/44.4/55.5/C/
B. DATE/TIME/LOCATION:
28JUN99/1500Z/12340N/01234E/
C. REMARKS:
PER REF (A), ORIG HAS ANALYZED PARAMETERS REPORTED REF (B) AND HAS
DETERMINED THE PULSE CONSTANT PRI VALUE OF 333.33 USEC TO BE
OPERATING 50 USEC ABOVE THE DOCUMENTED LIMITS. PARAMETERS ARE
WITHIN OBSERVED EXTREME LIMITS AND SHOULD BE TREATED AS A VALID
MODE OF OPERATION.//
DECL/XX//

**SAMPLE SYSTEM IMPACT MESSAGE (SIM) FORMAT
(ARMY and USAF)**

FROM: RC sending the message

TO: Wing/Groups who use the affected system

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE SIM ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (describe the threat change or problem, {for threat change provide the ELNOT/system name/function/parametric change} and its specific impact on the affected EW system)
3. (describe the indication, or lack of indication, the aircrew can expect and specific operational impact. Include recommended tactics, interim course of action and long term course of action to solve the problem).
4. ENSURE THIS INFORMATION IS MADE AVAILABLE TO ALL AIRCREWS WHO MAY BE AFFECTED.
5. (24hr contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE/ARMY JADE LANTERN MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SYSTEM IMPACT MESSAGE (SIM)
(NAVY AND USMC ONLY)**

(U) SYSTEM IMPACT MESSAGE
FM FLTINFOWARCEN NORFOLK VA//N9//
TO CTF/CTG//
INFO ALCON//
MSGID/GENADMIN/FLTINFOWARCEN//
SUBJ/SYSTEM IMPACT MESSAGE 01-00 (U)//
REF/A/RMG/FLTINFOWARCEN NORFOLK VA/**DTG**//
REF/B/RMG/(Respective SPC/**DTG**//
NARR/REF A IS TCAR. REF B IS TCVM VALIDATING REF A.//
POC/(NAME, COMMAND, PHONE #, E-MAIL ADDRESS)//
RMKS/1. (S) EMITTER LISTED BELOW WAS ACTIVE NUMEROUS TIMES WITHIN
THE PAST THIRTY-SIX HOURS IN THE GULF OF SABANI, INDICATING
PROBABLE WARM SHIFT BY KORONAN FORCES. A123B POSSESSES A LIMITED
SURFACE TO SURFACE AND FIRE CONTROL CAPABILITY. CURRENT SLQ-32
THREAT LIBRARY WILL NOT CORRECTLY ID THIS EMITTER. RECOMMEND
TF/COMPONENT COMMANDER DIRECT REPROGRAMMING AS FOLLOWS: READ:
ACTION/ELNOT/RF/PRI/PW/SCAN RATE/TYPE
ADD/A123B/1111.1/2222.2/333.33/44.4/55.5/C//
DECL/XX//

**SAMPLE REPROGRAMMING IMPACT MESSAGE (RIM)
(ARMY ONLY)**

FROM: ARAT-TA
TO: ASCC
INFO: USAAVNC
SSA
PEO-AVN
PM-ASE
SAFETY CENTER
(OTHER)

CLASSIFICATION

SUBJECT: JADE LANTERN - REPROGRAMMING IMPACT MESSAGE (RIMYY #)

REF:

1. () THIS IS A [CODEWORD] MESSAGE WHICH IMPACTS ALL UNITS IN [THEATER] EQUIPPED WITH [SYSTEM] OPERATIONAL FLIGHT PROFILE ### AND MISSION DATA SET ###. PASS TO ELECTRONIC WARFARE OFFICERS AND SUBORDINATE UNITS IMMEDIATELY.
2. () THE [NAME] SOFTWARE SUPPORT ACTIVITY HAS AUTHORIZED THE RELEASE OF MDS ###. FOR THE ABOVE INDICATED SYSTEM. CHANGES INCLUDE:
3. () THE NEW MDS ### IS AVAILABLE FOR DOWNLOAD FROM THE MULTI-SERVICE ELECTRONIC WARFARE DATA DISTRIBUTION SYSTEM (MSEWDDS). THE NEW FILE FOR MDS ### IS: MDS###.EXE. IT IS LOCATED IN THE [SYSTEM] LIBRARY. MDS333.EXE IS A GROUP OF FIVE INDIVIDUAL FILES, WHICH CAN BE SELF-EXTRACTED AFTER DOWNLOADING FROM THE MSEWDDS. THE FIVE FILES CONTAINED IN MD###.EXE ARE; (1) ###LIST.TXT [KNEEBOARD SHEET], (2) ###NOTES.TXT [PERTINENT NOTES], (3) ###HEX.HEX, HEXIDECIMAL FILE FOR LAPTOP UPLOAD TO [SYSTEM], (4) ###HEX.UDM, HEXADECIMAL FILE FOR MEMORY LOADER VERIFIER UPLOAD TO [SYSTEM], AND (5) 333FLAG.TXT WHICH CONTAINS THREAT CHANGE INFORMATION. DETAILED INFORMATION ON MDS DOWNLOADING AND STRUCTURE IS AVAILABLE IN THE FILE INF[SYSTEM].TXT, WHICH IS LOCATED IN THE [SYSTEM] LIBRARY. IF ELECTRONIC DISSEMINATION IS NOT AVAILABLE, PLEASE CONTACT THE POINT OF CONTACT.
4. () THE POC IS NAME, ORGANIZATION, TELEPHONE, EMAIL

**SAMPLE REPROGRAMMING IMPACT MESSAGE (RIM)
(USAF Only)**

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE RIM ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. (e.g. ALR-69 SWV 0806 replaces ALR-69 SWV 0805) ON THE (aircraft type). DO NOT LOAD THIS NEW SOFTWARE VERSION INTO ANY EW SYSTEM UNLESS SPECIFICALLY AUTHORIZED TO DO SO BY YOUR IMPLEMENTATION AUTHORITY IN AN IMPLEMENTATION MESSAGE

(IMP). THE OPERATIONAL IMPACT OF THE NEW SOFTWARE IS DESCRIBED IN PARAGRAPH 3. FOLLOW TCTO OR MAINTENANCE INSTRUCTION MESSAGE (MIM) INSTRUCTIONS, IF APPLICABLE. THE SOFTWARE CHANGE IS LOADED ON THE MSEWDDS (provide library and file name).

3. (describe the software change and operational impact).

4. ENSURE ALL AIRCREWS USING THE (affected system) ARE BRIEFED ON THE SOFTWARE CHANGE.

5. (24hr contact instructions if other than POC of message, otherwise not required).

6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

SAMPLE MAINTENANCE INSTRUCTION MESSAGE (MIM)
(USAF Only, note: the Army does not currently use MIMs, but may use them and this format in the future)

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE MIM ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. (specific maintenance instructions for loading the referenced software change).

3. (describe maintenance impacts, which are caused by the software change, to include additional tests that may be required.

4. IMPLEMENTATION INSTRUCTIONS: INSTALLATION OF THIS CHANGE MUST APPROVED BY YOUR IMPLEMENTATION AUTHORITY IN AN IMPLEMENTATION MESSAGE (IMP). DO NOT LOAD THE CHANGED SOFTWARE IN TO ANY EW SYSTEM UNTIL PROPER IMPLEMENTATION INSTRUCTIONS ARE RECEIVED.

5. (contact instructions if other than POC of message, otherwise not required).

6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SAMPLE IMPLEMENTATION MESSAGE (IMP)
(ARMY Only)**

FROM: ARMY SERVICE COMPONENT COMMANDER
TO: SUBORDINATE UNIT COMMANDERS
INFO: ARAT-TA
SSA

PEO - AVN
(OTHER)

CLASSIFICATION: as appropriate

SUBJECT: JADE LANTERN - IMPLEMENTATION MESSAGE FOR RIMYY### FOR [SYSTEM].

REF;

1. (U) THIS IS A [CODEWORD] MESSAGE WHICH IMPACTS THE READINESS AND/OR EFFECTIVENESS OF AIRCRAFT SURVIVABILITY EQUIPMENT. PASS TO ELECTRONIC WARFARE OFFICERS/APPROPRIATE STAFF IMMEDIATELY.
2. (U) RIMYY### AUTHORIZES INSTALLATION OF MDS ### TO REPLACE MDS ### IN ALL AFFECTED {SYSTEM}; USING OPERATIONAL FLIGHT PROFILE ### IN [THEATER].
3. (U) ACTION ADDRESSEES WILL REPLY TO THIS HEADQUARTERS VIA UNIT LOAD MESSAGE AND [ANY THEATER SUPPLEMENTAL REPORTING REQUIREMENTS] WHEN INSTALLATION HAS BEEN COMPLETED.
4. (U) POC IS NAME, ORGANIZATION, PHONE NUMBER, EMAIL

**SAMPLE IMPLEMENTATION MESSAGE (IMP)
(USAF Only)**

FROM: MAJCOM or JFACC/CFACC/AOC

TO: Wing/Groups in area of responsibility who use the affected system

CC: as required (Appropriate RCs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE IMP ALQ-161
PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC
WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE
(RIM)

ALQ-161)

APPLICABLE PACER WARE INFORMATION CAN BE FOUND ON THE MULTI-
SERVICE ELECTRONIC WARFARE DATA DISTRIBUTION SYSTEM (MSEWDDS) AS
FOLLOWS: LIBRARY----FILE NAME----ADDED----COMMENTS

B) 161MSG, 1897RIM.RTF, 02/06/01, PACER WARE RIM ALQ-161 PW 01 AWF1

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. THIS MESSAGE IS HQ ACC/DO AUTHORIZATION TO INSTALL REFERENCED
SOFTWARE CHANGE TO B-1 AIRCRAFT SPECIFIED IN THE RIM. TRAINING/TEST
UNITS WILL UPLOAD THE SOFTWARE CHANGE ON A NON-INTERFERENCE BASIS
WITH PROGRAMMED TRAINING AND TESTING.
3. ENSURE THAT THIS MESSAGE IS MADE AVAILABLE TO YOUR DEPLOYED
UNITS, IF APPLICABLE. DEPLOYED UNITS ASSIGNED TO OPERATION NORTHERN
WATCH (ONW) MUST WAIT FOR IMPLEMENTATION FROM USAFE/DOTW.
4. THIS MESSAGE CAN BE FOUND ON THE MSEWDDS EITHER BY SECURE STU-III
MODEM OR THROUGH SIPRNET AT [HTTP://WWW.WG53.EPLIN.AF.SMIL.MIL](http://www.wg53.eplin.af.smil.mil) OR
([HTTP://207.84.75.101](http://207.84.75.101)). MSEWDDS ASSISTANCE CAN BE OBTAINED BY CALLING
DSN 872-2166. THE REFERENCES ABOVE INDICATE THE APPROPRIATE BBS
LIBRARY AND FILE NAME FOR SUBJECT MESSAGES.
5. IMPORTANT: PER REFERENCE A, UNITS ARE REQUIRED TO PROVIDE A UNIT
LOADING MESSAGE (ULM) NLT 1 MAR 01 OR AS SOON AS LOADING IS COMPLETE.
THIS CAN BE DONE BY REPLYING TO THE DMS IMP MESSAGE OR E-MAIL mail to:
ACCDOZO@LANGLEY.AF.MIL. COURTESY COPY (CC) THE 53WG PW ACCOUNT FOR
DMS MESSAGES OR INFO mail to: 53WGERCPW@EGLIN.AF.MIL IF E-MAIL.
A. DEPLOYED UNITS ASSIGNED TO ONW ARE REQUIRED TO PROVIDE A ULM TO
USAFE

**SAMPLE UNIT LOAD MESSAGE (ULM)
(ARMY Only)**

FROM: SUBORDINATE UNITS
TO: ARMY SERVICE COMPONENT COMMAND
INFO: ARAT
PEO-AVN
SSA
(OTHER)

CLASSIFICATION

SUBJECT: JADE LANTERN - UNIT LOAD MESSAGE FOR MDS ### FOR [SYSTEM]

REF:

1. (U) THIS IS A [CODEWORD] MESSAGE.
- 2.(U) THE FOLLOWING UNIT(S) HAS/HAVE COMPLETED INSTALLATION OF MDS ### INTO ITS/THEIR OPERATIONAL FLIGHT PROFILE ## EQUIPPED [SYSTEM] IN [THEATER].
3. (U) PROBLEMS ENCOUNTERED:
4. (U) POC IS NAME, ORGANIZATION, TELEPHONE, EMAIL

**SAMPLE UNIT LOADING MESSAGE (ULM)
(USAF Only)**

FROM: Wing/Group sending the message

TO: MAJCOMs or JFACC/CFACC/AOC IMP Authority

CC: as required (RCs and Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE ULM ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. THE (wing/group i.e. 1FW) HAS COMPLETED LOADING REFERENCE SOFTWARE CHANGE. LOADING WAS COMPLETED ON (DTG in ZULU i.e. 12 2345 DEC 01).

3. (any pertinent information concerning delays in loading, problems in lading etc. otherwise not require).

4. CONTACT INSTRUCTIONS:

A. WING/GROUP EW POC: (name, rank, phone number and unclassified e-mail address).

B. WING/GROUP AVIONICS/POD SHOP POC: (name, rank, phone number and unclassified e-mail address).

5. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SAMPLE AUTHORIZATION TO REPROGRAM MESSAGE (ATR)
(NAVY AND USMC ONLY)**

(U) AUTHORIZATION TO REPROGRAM (ATR) MESSAGE:

FM CTF/CTG

TO FLTINFOWARCEN NORFOLK VA//N9//

INFO ALCON

MSGID/GENADMIN/CTF/CTF//

SUBJ/AUTHORIZATION TO REPROGRAM EW SYSTEMS 01-00 (U)//

REF/A/RMG/FIWC/DTG//

AMPN/REF A IS SIM 01-00//

POC/Name, Command/DSN/Email address//

RMKS/1. (C) IAW REF A, ORIG CONCURS WITH RECOMMENDATION TO
REPROGRAM ALL AFFECTED EW SYSTEMS.//

DECL/XX//

**SAMPLE DISTRIBUTION NOTICE MESSAGE (DNM)
(NAVY/USMC ONLY)**

FM NAVAIRWARCENWPNDIV PT MUGU CA//41130GE/454220E// (AIR
REPROGRAMMING TSSC)
NAVSURWARCENDIV DAHLGREN VA//T24// (SURFACE REPROGRAMMING TSSC)
TO CTF NINE FIVE FIVE
INFO TF NINE FIVE FIVE
COMSECONDFLT/J36//
DIRMSIC REDSTONE ARSENAL AL//MSC-1B1//
NAIC WRIGHT PATTERSON AFB OH//TAE//TAER//
CDRNGIC CHARLOTTESVILLE VA//IANG-SBR//
ONI WASHINGTON DC//241//
COMNAVAIRWARCENWPNDIV CHINA LAKE CA//455300D/47HHOOD//
FLTINFOWARCEN DET SAN DIEGO CA//N3//
APPROPRIATE CLASSIFICATION//N03430//
EXER/JTFEX 02-2//
MSGID/GENADMIN/(Originator)//
SUBJ/DISTRIBUTION NOTICE MESSAGE 001-02 (U)//
REF/A/RMG/FLTINFOWARCEN/DTG//
REF/B/RMG/CTF NINE FIVE FIVE/DTG//
REF/C/RMG/NSWC DAHLGREN/DTG//
NARR/REF A IS SIM 001-02, RECOMMENDING REPROGRAMMING, REF B IS ATR
001-02, AUTHORIZING REPROGRAMMING AND REF C IS AN/SLQ-32 ONLINE
ADVISORY MESSAGE.//POC//
THE FOLLOWING IS A SAMPLE PARAGRAPH FOR REPROGRAMMING AIR EW
SYSTEMS:
RMKS/1. PER REFS (A) AND (B), ORIG WILL POST UPDATED THREAT LIBRARY
TO SECURE BULLETIN BOARD SYSTEM BTWN 07 - 10 JUL XX. TO DOWNLOAD,
CALL (TSSC)
THE FOLLOWING IS A SAMPLE PARAGRAPH FOR REPROGRAMMING SURFACE
EW SYSTEMS:
RMKS/1. PARAMETERS REPORTED REF (A) HAVE BEEN ENGINEERED FOR THE
AN/SLQ-32. FLEET UNITS HAVE BEEN DIRECTED TO TAKE REF (C) FOR
ACTION.
DECL/XX//

**SAMPLE OPERATIONAL CHANGE REQUEST (OCR)
(ARMY Only)**

FROM: ASE EQUIPPED UNIT
TO: ARMY SERVICE COMPONENT COMMANDER
SSA
PEO-AVN
ARAT

INFO: USAAVNC

CLASSIFICATION

SUBJECT: JADE LANTERN - OPERATIONAL CHANGE REQUEST

1. () DESCRIBE THE SPECIFIC CONDITIONS THAT MAY WARRANT A REPROGRAMMING ACTION TO INCLUDE SYSTEM, OPERATIONAL FLIGHT PROFILE NUMBER, MDS NUMBER AND THEATER.
2. () UNIT POC NAME, TELEPHONE, AND EMAIL.

**SAMPLE OPERATIONAL CHANGE REQUEST (OCR) FORMAT
(USAF Only)**

FROM: Organization sending the message

TO: MAJCOM EWIR POCs

CC: as required (Appropriate RCs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE OCR ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

APPLICABLE PACER WARE INFORMATION CAN BE FOUND ON THE MULTI-SERVICE ELECTRONIC WARFARE DATA DISTRIBUTION SYSTEM (MSEWDDS) AS FOLLOWS:

LIBRARY----FILE NAME----ADDED----COMMENTS

B) 161MSG, 1897RIM.RTF, 02/06/01, PACER WARE RIM ALQ-161 PW 01 AWF1

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. (provide description of the specific problem).

A. PRIORITY: (select EMERGENCY, URGENT or ROUTINE)

B. SYSTEM: (complete nomenclature of the system and software version, e.g. ALR-69 SWV 0805).

3. REQUEST MACOM APPROVAL OF THE REQUESTED CHANGE AND DIRECT TO THE APPROPRIATE REPROGRAMMING CENTER TO BEING WORK (based on the priority).

4. (contact instructions if other than POC of message, otherwise not required).

5. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SAMPLE SOFTWARE CHANGE MESSAGE (SCM) FORMAT
(ARMY and USAF)**

FROM: RC sending the message

TO: RC performing the coding of the software change

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE SCM ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE/ARMY JADE LANTERN MESSAGE.
2. (RC providing the coding) IS AUTHORIZED TO ENCODE THE (system and SWV) MISSION DATA LISTED IN PARAGRAPH 3. THE NEW SOFTWARE WILL REPLACE (system and SWV). THIS SOFTWARE SHOULD BE ENCODED AT (select EMERGENCY, PRIORITY or ROUTINE) PRECEDENCE. PLEASE PROVIDE THIS OFFICE WITH AN ESTIMATED COMPLETION DATE TIME GROUP.
3. (discussion of what the MD reprogramming engineer is trying to accomplish with the MD, test desired and how the resultant MD is to released).
4. (mission data to be encoded).
5. (contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE/ ARMY JADE LANTERN MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SAMPLE TIME COMPLIANCE TECHNICAL ORDER MESSAGE (TCTO) FOR
(USAF Only)**

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE TCTO ALQ-161 PW 01

ACC001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (describe the difference the Block Cycle or OFP change implemented over the superseded software).
3. (describe any changes to system Handbooks and or Mission Guides).
4. (describe any changes to Mission Data).
5. IMPLEMENTATION INSTRUCTIONS: YOUR IMPLEMENTATION AUTHORITY HAS APPROVED INSTALLATION OF THIS CHANGE. AT RECEIPT OF REFERENCED TCTO, INSTALL THE SOFTWARE CHANGE AFTER PROPER COORDINATION WITH THE WING/GROUP EW POC IAW AFI 10-703.
6. (contact instructions if other than POC of message, otherwise not required).
7. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

**SAMPLE STATUS MESSAGE (STM) FORMAT
(USAF Only)**

FROM: RC sending the message

TO: MAJCOMs or JFACC/CFACC/AOC IMP Authority

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE STM 53
EWG/ERC PW

01 AWF001 (U)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC
WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE
(RIM)

ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. (provide the time frame covered by this STM).

3. STATUS OF: (the following paragraphs will be provided for each system the
reprogramming center is responsible for).

C. SYSTEM NAME:

D. DTG OF SCM's OR TASKING RECEIVED:

E. TESTING COMPLETE: (estimated or actual time).

F. ENGINEERING COMPLETE: (estimated or actual time).

G. KIT PROOF: (estimated or actual time).

H. DISTRIBUTE: (estimated or actual time).

I. MESSAGE SERIAL NUMBER: (i.e. MIM ALR-69 SWV 0806 PW 00 AWF001).

J. SYSTEM POC's: (engineers and or equipment specialists).

K. COMMENTS: (list any known problems or any field confirmations received or
distributed reprogramming data packages).

4. STATUS OF: (paragraph 3 is repeated again for each system).

5. (contact instructions if other than POC of message, otherwise not required).

6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Appendix D

REPROGRAMMING EXERCISES

1. Joint EW Reprogramming Exercises

PROUD BYTE exercises focus on the joint coordination of EW reprogramming. This annual exercise is normally conducted as part of a larger exercise (for example, USPACOM ULCHI-FOCUS LENS, USJFCOM UNIFIED ENDEAVOR, etc.) to exercise the combatant command/JTF IO staff and the SPC. On a rotating basis, each combatant command/JTF staff exercises to increase the awareness and coordination of EW reprogramming actions at the joint and combined levels. The transfer of threat change validation authority from the S&TI centers to the SPC is also exercised. Additionally, support of the SPCs to the EW reprogramming process is evaluated. The services are encouraged to conduct their own EW reprogramming exercises (USA - BRAVE BYTE, USN/USMC - NEPTUNE BYTE, USAF - SERENE BYTE) as part of the PROUD BYTE exercises.

2. ARAT Involvement in Army and Joint Service MDS Programming Exercises

a. The threat analysis and software engineering components of the ARAT support Army service component commanders in planning, coordinating, and executing objectives during joint or service reprogramming exercises.

b. BRAVE BYTE is the Army component of the JIOC PROUD BYTE exercise. Army component commands participating in joint exercises are encouraged to incorporate reprogramming objectives. A list of recommended exercise objectives includes but is not limited to—

(1) Assess the ability of the ARAT-TA, software support activities (SSA) and SPCs to sustain operations on a 24 hr/day, 7 days/week basis.

(2) Assess the timely and accurate flow of information between elements of the reprogramming community.

(3) Assess the intelligence and reprogramming communities' response to threat change validation requests (TCVRs).

(4) Evaluate the capability of the MSEWDDS and communications architecture to exchange information and software changes from across the Army reprogramming community to the unit's capability to conduct internal reprogramming objectives.

(5) Determine the effectiveness of signature libraries and software flagging models to detect parametric changes and anomalies.

(6) Evaluate the decision process that creates and implements a tactics, techniques and procedures (TTP) change.

(7) Evaluate the readiness of reprogramming organizations.

(8) Determine if TACELINT simulators, signal generators, and exercise intelligence collection are adequate to replicate new or changed emitters for exercising the reprogramming process.

c. Additionally, Army units undergoing National Training Center (NTC) rotations should consider reprogramming operations.

3. Naval Exercises

a. The Navy supports the joint EW communities PROUD BYTE exercises through the NEPTUNE BYTE exercise program. NEPTUNE BYTE exercises come under the purview of the joint coordination of electronic warfare reprogramming (JCEWR) process that examines the ability of the EWRL community to quickly provide TF/TG commanders with updated EW libraries to correct deficiencies in battle group ES/EA/EP systems. The EWRL process evaluates administrative, equipment, communications and personnel used in Navy, Marine Corps and joint EWRL efforts. Managed by FIWC, NEPTUNE BYTE meets the joint reprogramming objectives of threat change recognition and validating and directing service reprogramming responses. Supplemental objectives of NEPTUNE BYTE exercises include the following:

- (1) Determine and document capabilities and limitations of the EWRL process.
- (2) Train in and evaluate the administrative notification and approval process and information flow for EW reprogramming.
- (3) Provide for realistic scenario-driven training.
- (4) Train on and evaluate reprogramming equipment.
- (5) Train in and evaluate communications paths.
- (6) Evaluate and validate new hardware, software, and equipment.

b. Exercise objectives are accomplished in three phases by determining the threat change, developing the appropriate parametric data, and implementing reprogramming procedures as necessary. The reprogramming process begins when any unit (that is, Fleet Unit, Fleet Marine Force [FMF], or any other element with EW interests) can confirm or reasonably suspect a change in the EW threat environment. The process is completed with the system reprogramming action or determination that reprogramming is not required. In addition, reprogramming at sea training has been directed by the Commander, Second Fleet and Commander, Third Fleet as part of the battle groups' inter-deployment training cycle (IDTC). FIWC conducts training with each deploying BG as part of JTFEX for deployment certification.

4. Air Force Exercises

SERENE BYTE Exercises. SERENE BYTE exercises will be held with joint exercises to the maximum extent possible. The purpose of SERENE BYTE exercises is to familiarize operators with the real-world limitations of tactical communications systems. Joint exercises will expose all levels of the EWIR process to communications limitations inherent in large-scale exercises and allow joint coordination and cooperation between the services. These exercises may include FMS participants. There are two types of SERENE BYTE exercises: annual and quarterly.

a. Annual Exercises. Annual SERENE BYTE exercises cover the entire EWIR process. They document the capabilities and limitations of all major components of reprogramming, including—

- (1) Collect, validate, and distribute intelligence information.

- (2) Evaluate signals.
- (3) Distribute changes.
- (4) Implement changes.
- (5) Validate equipment changes in combat units.

b. Quarterly Exercises. These exercises focus on validating the procedures for distributing emergency reprogramming data to units. They identify shortcomings in communications and support equipment and allow the units to practice mission data loading procedures. Quarterly exercises will not be held within one month of the annual exercise or within the same quarter. (The annual exercise serves as a quarterly exercise.) Unit commanders and appropriate MAJCOM normally decide which units and systems participate in the quarterly exercises.

References

Joint

- JP 1-02, *DOD Dictionary of Military and Associated Terms*, 7 May 2002
- JP 3-0, *Doctrine for Joint Operations*, 10 Sep 2001
- JP 3-13, *Joint Doctrine for Information Operations (IO)*, 9 Oct 1998
- JP 3-13.1, *Joint Doctrine for Command and Control Warfare*, 7 Feb 1996
- JP 3-51, *Joint Doctrine for Electronic Warfare*, 7 Apr 2000
- JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, 13 Jan 1999
- CJCSI 3210.04 (draft), *Joint Coordination of EW Reprogramming*
- CJCSM 3500.04B, *Universal Joint Task List*, 1 Oct 1999

Army

- FM 3-0, *Operations*, 14 Jun 2001
- FM 3-13, *Information Operations*, 24 Jan 2002
- FM 100-15, *Corps Operations*, 29 Oct 1996
- AR 525-15, *Software Reprogramming Policy for Target Sensing Systems*, 1 Feb 1993
- AR 525-22, *Electronic Warfare Policy*, chg 1, 1 Nov 1999
- TRADOC Pam 525-5, *Force XXI Operations*, Headquarters U.S. Army Training and Doctrine Command, Fort Monroe, VA 23651-5000, 1 Aug 1994

Marine Corps

- MCDP 6, *Command and Control*, Oct 1996
- MCWP 5-1, *Marine Corps Planning Process*, 24 Sep 2001
- FMFM 6-1, Marine Division
- MCRP 5-12C, *Marine Corps Supplement to the DOD Directory of Military and Associated Terms*, Jul 1998

Navy

- OPNAV Instruction 3430.2313, *Tactical Electronic Warfare Reprogrammable Library Program*, 12 Jun 1992
- OPNAV Instruction 5450.231, *Mission, Functions, and Tasks of the Fleet Information Warfare Center*, 5 May 1995
- Fleet Information Warfare Center N9 Reprogramming at Sea Training Plan

Air Force

- AFI 10-703, *Electronic Warfare Integrated Reprogramming*, 31 Oct 2001
- AFDD 2-5.1, *Electronic Warfare Operations*, 19 Nov 1999

Glossary

Section I—ABBREVIATIONS AND ACRONYMS

A

AAA	anti-aircraft artillery
ACC	Air Combat Command
AFDC	Air Force Doctrine Center
AFFOR	Air Force forces
AFI	Air Force instruction
AFIAA	Air Force Intelligence Analysis Agency
AFIWC	Air Force Information Warfare Center
AFSOC	Air Force Special Operations Command
AR	Army regulation
ARAT	Army reprogramming analysis team
ARAT-SE	Army Reprogramming Analysis Team- Software Engineering
ARAT-TA	Army Reprogramming Analysis Team-Threat Analysis
ARFOR	Army forces
ARM	antiradiation missiles
ATO	air tasking order
ATRR	Army Target Sensing Systems Rapid Reprogramming

B

BAT	brilliant antitank
BDA	battle damage assessment
BG	battle group

C

C2	command and control
CECOM	U.S. Army Communications - Electronics Command
CECOM SEC	U.S. Army Communications - Electronics Command Software Engineering Center
CENTAF	Central Command air forces
CF	confidence factor
CINC	commander in chief
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Memorandum

CJTF	combined joint task force
COMINT	communications intelligence
CSS	central security service
CTF	combined task force
CTG	combined task group
D	
DB	database
DCI	Director of Central Intelligence Agency
DIA	Defense Intelligence Agency
DNM	distribution notice message (USN)
DOD	Department of Defense
DSCS	Defense Satellite Communications System
E	
EA	electronic attack
ECG	electronic combat group
ECSF	electronic combat support flight
ELINT	electronic intelligence
ELNOT	electronic intelligence notation
EP	electronic protection
EPL	electronic intelligence parameters list
ES	electronic warfare support
EW	electronic warfare
EWASIF	electronic warfare avionics integration support facility
EWCC	electronic warfare coordination cell
EWIR	electronic warfare integrated reprogramming
EWO	electronic warfare officer
EWIRDB	Electronic Warfare Integrated Reprogramming Data Base
ELMSDB	electromagnetic systems database
EWRL	electronic warfare reprogrammable library (USN)
EW/TSS	electronic warfare and target sensing systems
F	
FIWC	fleet information warfare center
FME	foreign military exploitation
FMF	Fleet Marine Force
FMS	foreign military sales

G	
G-2	Army or Marine Corps component intelligence staff officer
GCI	ground control intercept
I	
Info	information
INSCOM	U. S. Army Intelligence and Security Command
Intel	intelligence
IO	information operations
IPC	intelligence production center
IW	information warfare
J	
J2	intelligence directorate of a joint staff
J3	operations directorate of a joint staff
J5	plans directorate of a joint staff
J6	command, control, communications, and computer systems directorate of a joint staff
JAC (EUCOM)	joint analysis center, European Command
JCEWR	joint coordination of electronic warfare reprogramming
JCS	Joint Chiefs of Staff
JIOC	Joint Information Operations Center
JF	joint force
JFC	joint force commander
JIC	joint intelligence center
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JOA	joint operations area
JOC	joint operations center
JPOTF	joint psychological operations task force
JSC	Joint Spectrum Center
JTF	joint task force
JTCB	joint targeting coordination board
K	
KILTING	National Technical ELINT Database
L	
LIWA	land information warfare activity

M	
MAGTF	Marine air-ground task force
MAJCOM	major command (USAF)
MARFOR	Marine Corps forces
MASINT	measurement and signature intelligence
MCCDC	Marine Corps Combat Development Command
MD	
MDS	mission data set
MEF	Marine expeditionary force
MHz	megahertz
MISREP	mission report
MSEWDDS	multiservice electronic warfare data distribution System
Msg	
MSIC	Missile and Space Intelligence Center
N	
NAIC	National Air Intelligence Center
NAVFOR	Navy forces
NERF	Navy emitter reference file
NGIC	National Ground Intelligence Center
NRT	near real time
NSA	National Security Agency
NTSDS	national target signature data system
NWDC	Navy Warfare Development Command
O	
OB	order of battle
OCR	operational change request
OFP	operational flight program
ONI	Office of Naval Intelligence
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security
OSR	Office of Scientific Research
P	
PAO	Public Affairs Office; public affairs officer
POC	point of contact
PRF	pulse repetition frequency

PSYOP	psychological operations
R	
RAPADS	radar parametrics data set
RC	reprogramming centers
Rep	representative
RIM	reprogramming impact message
RWR	radar warning receiver
S	
S&TI	scientific and technical intelligence
SC	support cells
SE	shielding effectiveness
SED	software engineering directorate
SEAD	suppression of enemy air defenses
SIFT	selectively improved flagging technique
SIGINT	signals intelligence
SIM	system impact message
SIPRNET	Secret Internet Protocol Router Network
SOF	special operations forces
SPC	service production center
SPINS	special instructions
SRC	service reprogramming center
SSA	software support activity
SSC	software support center
Ste	suite
STU-III	secure telephone unit-III
T	
TACAIR	tactical air
TACELINT	tactical electronics intelligence
TCAR	threat change analysis request
TCVM	threat change validation message
TCVR	threat change validation request
TECHELINT	technical electronics intelligence
TF	task force
TG	task group
TIM	threat impact message
TLAM	Tomahawk land attack missile
TRADOC	U.S. Army Training and Doctrine Command

TSS	target sensing system
TSSC	tactical system support center
TTP	tactics, techniques, and procedures
U	
U.S.	United States
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy
W	
WARM	wartime reserve mode
WR-ALC	Warner Robins-Air Logistics Center

PART II-TERMS AND DEFINITIONS

Electronics Intelligence. Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT (JP 1-02).

ELINT Parameter Limits List. A technical electronic intelligence reference document, which describes the basic operating parameters (e.g. RF, PRF, scan) of non-communications signals. Its purpose is to aid collectors and electronic warfare (EW) operators in rapid signal identification and determining new or unusual operating characteristics. Information may be derived from a combination of actual collection, "book" values, or other sources. The parameters given are subject to averaging and generalizations and are not intended for applications such as EW reprogramming. The EPL is also available on Secret Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System (JWICS). Also called EPL.

Electronic Warfare Integrated Reprogramming Data Base. A Defense Intelligence Agency-managed database, maintained and distributed by the National Air Intelligence Center (NAIC) as the executive agent. It is the primary Department of Defense (DOD) approved source for technical parametric and performance data on non-communications emitters and associated systems. It directly supports electronic warfare (EW) reprogramming by all U.S. military services. The EWIRDB combines assessed, all-source intelligence data from the service production centers (SPCs) on foreign systems with observed electronic intelligence (ELINT) (KILTING) data from the National Security Agency (NSA) on foreign emitters. Additionally, engineering-value/measured data on U.S. emitters (gathered data), provided by the services to the Air Force Information Warfare Center, is included. Also called EWIRDB.

KILTING Database. The National technical electronic intelligence (ELINT) database containing comprehensive technical data (as observed through SIGINT) on non-communications emitters. Information in KILTING is maintained in an extensive hierarchical tree structure which links related parametric measurements. The inputs to KILTING are provided mainly by signals analysts from National Security Agency (NSA) and the Electronic Warfare Integrated Reprogramming Data Base (EWIRDB) production centers subsequent to their in-depth technical analyses. Unlike the ELINT Parameter Limits List (EPL), one of the primary objectives of KILTING is (when merged with assessed and gathered information in the EWIRDB product) to support the services' electronic warfare (EW) reprogramming needs.

Measurement and Signature Intelligence. Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT. (JP 1-02).

Reprogramming. To counter the effects of signature changes and given the authority by an appropriate field commander, reprogramming is the ability to reconfigure/alter the collection spectrum, current databases, mission data/software, or

other operational characteristics of electronic warfare/target sensing systems (EW/TSS) to maintain a greater level of effectiveness.

Service Electronic Warfare Reprogramming Centers. Identifying electronic warfare (EW) system deficiencies, determining operational responses, and developing reprogramming changes, settings, and tactics to counter changes in the threat, is an individual service responsibility. Also called SRCs.

Service Production Centers. Responsible for updating and maintaining assigned emitters in the Electronic Warfare Integrated Reprogramming Data Base (EWIRDB). Emitter assignments are primarily based on their areas of expertise. They provide system-specific technical information to the theater intelligence centers and the service electronic warfare reprogramming centers (SRCs). The Missile and Space Intelligence Center (MSIC) is the overall manager of the EWIRDB as a component of Defense Intelligence Agency (DIA) and is still considered to be a scientific and technical intelligence (S&TI) center. Also called SPCs.

System Impact Message. Issued by a service electronic warfare reprogramming centers (SRC) to describe to users the impact of a given threat change to a friendly electronic warfare (EW) system. The SIM may indicate that the new mode of operation is already covered by friendly EW systems without need for reprogramming. Also called SIM.

Threat Change Analysis Request. Issued by an intelligence collector or user to initiate the electronic warfare (EW) reprogramming process when they suspect a potential threat change. Also called TCAR.

Threat Change Validation Message. Issued by service production centers (SPC) in response to a threat change validation request (TCVR). Carries the analyst's judgment about the validity of a suspected threat change mode. Also called TCVM.

Threat Change Validation Request. Issued by service electronic warfare reprogramming centers (SRC) to the appropriate service production center (SPC) to request validation of a suspected change in a threat system. Also called TCVR.

Wartime Reserve Modes (WARM). Characteristics and operating procedures of sensors, communications, navigation aids, threat recognition weapons, and countermeasure 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).

Index

A

Air Force Information Warfare Center (AFIWC), I-5, III-6
Air Force Intelligence Analysis Agency (AFIAA), I-5
Air Force Special Operations Command (AFSOC), I-3, II-5, III-3, B-2
ambiguity resolution, III-13
antiradiation missiles (ARM), I-1, I-4
Army Reprogramming Analysis Team Threat Analysis (ARAT-TA), I-3, II-4, III-2, III-6, B-1, D-1
Army Target Sensing Systems Rapid Reprogramming (ATRR), III-2

B

battle damage assessment (BDA), II-3
block updates, I-3

C

collection and analysis, I-5
collector bias, I-3, III-6, III-9, A-3
combat identification, I-4
communications intelligence (COMINT), I-6

D

Defense Intelligence Agency (DIA), I-5, A-2, A-4

E

electronic attack (EA), I-1, III-2, III-11, III-13, III-14
Electronic Combat Support Flight (ECSF), I-3, II-5, III-3, B-2
electronic intelligence (ELINT), vi, I-1, I-3, I-4, I-5, I-6, III-6, III-7, III-8, III-10, III-12, A-2, A-4
electronic protection (EP), I-1
electronic support (ES), I-1, I-2, III-2, III-6
electronic warfare (EW), i
Electronic Warfare Coordination Cell (EWCC), vii, II-2, II-3, II-5, A-2
Electronic Warfare Integrated Reprogramming Database (EWIRDB), I-4, III-2, III-5, III-8, III-9, III-10, III-12, III-13, A-3, A-4
Electronic Warfare Reprogrammable Library (EWRL), I-3, III-2, III-6, III-7, D-2

F

firmware/hardware, vi, III-1, III-2, III-3, III-13, III-15, A-4, D-2
Fleet Information Warfare Center (FIWC), I-3, II-4, III-2, III-3, III-6, III-7, B-2, D-2
foreign emitters, I-4, I-5

Foreign Military Sales (FMS), I-4, D-3

I

intelligence data, vi, I-3, I-4, III-10, III-11, 6

J

jamming, I-1, II-6

jamming technique, III-9, III-11, III-13, III-14, A-2

Joint Force Commander (JFC), II-1, II-3

Joint Information Operations Center (JIOC), vii, II-5, B-1, D-1

joint operations area (JOA), I-2, II-1

Joint Task Force (JTF), i, vi, I-1, II-1, D-1

K

KILTING database, I-5, 7

M

measurement and signature intelligence (MASINT), vi, I-1, I-5, III-2, III-12, B-2

message format, III-6, C-1

military deception (MILDEC), I-1

Missile and Space Intelligence Center (MSIC), I-5

missing report (MISREP), II-5, A-2

mission data sets (MDS), III-3, D-1

mission planning, i, vi, II-2

Multiservice Electronic Warfare Data Distribution System (MSEWDDS), III-3, III-16, B-3, D-1

N

National Air Intelligence Center (NAIC), I-5, 6

National Ground Intelligence Center (NGIC), I-5, III-12

National Security Agency (NSA), I-5, III-5, A-2

National Target Signature Data System (NTSDS), I-6, III-12

O

Office of Naval Intelligence (ONI), I-5

operational change request (OCR), II-3, III-7, C-17

operational flight program (OFP), III-3, III-4, III-9, III-11, III-13, III-14, III-15

operations security (OPSEC), I-1

P

parametric variations, III-9

physical destruction, vi, I-1, I-2, II-2

psychological operations (PSYOP), I-1

R

radar, I-4, III-5, A-1, A-3

radar warning receivers (RWR), I-4, II-2, III-2, III-11

S

Secret Internet Protocol Router Network (SIPRNET), III-16

selectively improved flagging technique (SIFT), III-6

service production center (SPC), I-4, II-4, III-5, III-7, III-9, A-1, D-1

signature data, vi, I-1, I-2, I-6

signature, parametric, I-1, I-2, I-3, I-4, II-2, II-3, II-4

signature, threat, vi, I-3, II-4, III-6

system impact message (SIM), II-4, II-5, III-11, A-1

T

target sensing systems (TSS), i, vi, I-1, II-1, II-3, II-4, III-1

threat change analysis request (TCAR), II-3, II-4, III-7, A-1, A-3, C-2

V

validation, II-3, II-5, III-3, III-7, III-8, III-9, A-1, C-4, D-1

W

Warner Robins-Air Logistics Center (WR-ALC), I-3, III-3, B-3

wartime reserve modes (WARM), I-2, III-2

FM 3-51.1 (FM 34-72)
MCRP 3-40.5B
NTTP 3-13.1.15
AFTTP(I) 3-2.7

6 JANUARY 2003

By Order of the Secretary of the Army:

Official:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
XXXXX

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: Distribute in accordance with the initial distribution number (IDN) 115744 requirements for FM 3-51.1

By Order of the Secretary of the Air Force:

DAVID F. MacGHEE, JR.
Major General, USAF
Commander
Headquarters Air Force Doctrine Center

Air Force Distribution: F

