

**ARMY, MARINE CORPS, NAVY, AIR FORCE**



**AIR LAND SEA  
APPLICATION  
CENTER**

# **REPROGRAMMING**

## **HANDBOOK FOR REPROGRAMMING OF ELECTRONIC WARFARE AND TARGET SENSING SYSTEMS**

**FM 34-72  
MCRP 3-36.1B  
NWP 3-13.1.15  
AFTTP(I) 3-2.7**

**APRIL 1998**

**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 18 October 1996.

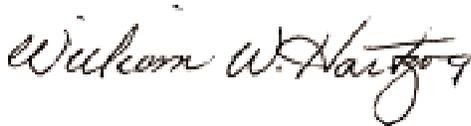
Other requests will be referred to HQ TRADOC, ATTN: ATDO-A, Ft Monroe, VA 23651; HQ MCCDC, ATTN: C42, Quantico, VA 22134; NDC, ATTN: N3, Norfolk VA 23511; or HQ AFDC, ATTN: DJ, Langley AFB VA 23665.

**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 under our direction for use by our respective commands and other commands as appropriate.



**WILLIAM W. HARTZOG**

General, USA  
Commander  
Training and Doctrine Command



**J. E. RHODES**

Lieutenant General, USMC  
Commanding General  
Marine Corps Combat  
Development Command



**G. S. HOLDER**

Rear Admiral, USN  
Commander  
Naval Doctrine Command



**RONALD E. KEYS**

Major General, USAF  
Commander  
Headquarters Air Force Doctrine Center

# PREFACE

## 1. Scope

This publication describes multiservice tactics, techniques, and procedures (MTTP) for consideration and use during reprogramming operations to support electronic warfare (EW) and target sensing systems. This activity must be coordinated and integrated with command and control warfare (C2W) operations conducted by joint task force (JTF) and component level commands. This publication—

a. Provides an overview of electronic warfare and target sensing system reprogramming.

b. Details the requirements and procedures for coordination and integration of 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 reprogramming activities to support JTF EW operations. Joint operations procedures for reprogramming are discussed to facilitate coordination, synchronization, integration, and deconfliction of reprogramming actions within the JTF when executed in exercises, contingencies, and other operations where more than one service is involved.

b. This publication augments the authoritative doctrine published in Joint

Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)* and Joint Publication 3-51, *Electronic Warfare in Joint Military Operations*.

## 3. Application

a. 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.

b. This is a multiservice publication approved for use by the United States Army, Marine Corps, Navy, and Air Force.

## 4. Implementation Plan

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

**Army.** The Army will incorporate the procedures in this publication in US Army training and doctrinal publications as directed by the commander, US Army Training and Doctrine Command (TRADOC). Distribution is in accordance with DA Form 12-11E.

**Marine Corps.** The Marine Corps will incorporate the procedures in this

publication in US Marine Corps training and doctrinal publications as directed by the commanding general, US Marine Corps Combat Development Command (MCCDC). Distribution is in accordance with MCPDS.

**Navy.** The Navy will incorporate these procedures in US Navy training and doctrinal publications as directed by the commander, Naval Doctrine Command (NDC). 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 37-160.

**5. User Information**

a. The TRADOC-MCCDC-NDC-HQ AFDC 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. We encourage recommended changes for improving this publication. Key your comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendation directly to—

<b>Army</b>	<b>Air Force</b>
<p>Commander          US Army Training and Doctrine Command          ATTN: ATDO-A          Fort Monroe VA 23651-5000          DSN 680-3153 COMM (757) 727-3153</p>	<p>Headquarters Air Force Doctrine Center          ATTN: DJ          216 Sweeney Blvd, Suite 109          Langley AFB VA 23665-2722          DSN 574-8091 COMM (757) 764-8091          E-mail: afdc.dj@langley.af.mil</p>
<b>Marine Corps</b>	<b>ALSA</b>
<p>Commanding General          US Marine Corps Combat Development Command          ATTN: C42          3300 Russell Road          Quantico VA 22134-5021          DSN 278-6234 COMM (703) 784-6234</p>	<p>ALSA Center          ATTN: Director          114 Andrews Street          Langley AFB VA 23665-2785          DSN 574-5934 COMM (757) 764-5934          E-mail : alsadirector@langley.af.mil</p>
<b>Navy</b>	
<p>Naval Doctrine Command          ATTN: N3          1540 Gilbert St          Norfolk VA 23511-2785          DSN 565-0563 COMM (757) 445-0563          E-mail: ndcjoint@nctamslant.navy.mil</p>	

**FM 34-72**  
**MCRP 3-36.1B**  
**NWP 3-13.1.15**  
**AFTTP(I) 3-2.7**

**FM 34-72** **US Army Training and Doctrine Command**  
**Fort Monroe, Virginia**

**MCRP 3-36.1B** **Marine Corps Combat Development Command**  
**Quantico, Virginia**

**NWP 3-13.1.15** **Naval Doctrine Command**  
**Norfolk, Virginia**

**AFTTP(I) 3-2.7** **Headquarters Air Force Doctrine Center**  
**Maxwell Air Force Base, Alabama**

**13 April 1998**

**REPROGRAMMING**  
**Handbook**  
**for**  
**Reprogramming of Electronic Warfare and**  
**Target Sensing Systems**

**TABLE OF CONTENTS**

	<b>Page</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>v</b>
<b>CHAPTER I OVERVIEW OF ELECTRONIC WARFARE AND TARGET SENSING SYSTEM (EW/TSS) REPROGRAMMING</b>	
Background .....	I-1
EW/TSS .....	I-2
Reprogramming Process .....	I-2
Reprogramming Databases .....	I-4
<b>CHAPTER II REPROGRAMMING IN THE JOINT/MULTISERVICE ENVIRONMENT</b>	
Background .....	II-1
JTF Battlestaff .....	II-1
Component Reprogramming .....	II-4
Coordination Between Services .....	II-6

<b>CHAPTER III</b>	<b>THE REPROGRAMMING PROCESS</b>	
	Joint EW/TSS Reprogramming .....	III-1
	Service EW/TSS Reprogramming .....	III-1
	The Reprogramming Process .....	III-4
<b>APPENDIX A</b>	<b>POINTS OF CONTACT (POCs)</b> .....	<b>A-1</b>
<b>APPENDIX B</b>	<b>REPROGRAMMING MESSAGE FORMATS</b> .....	<b>B-1</b>
<b>APPENDIX C</b>	<b>REPROGRAMMING EXERCISES</b> .....	<b>C-1</b>
<b>REFERENCES</b> .....		<b>References-1</b>
<b>GLOSSARY</b> .....		<b>Glossary-1</b>
<b>INDEX</b> .....		<b>Index-1</b>
 <b>FIGURES</b>		
	<b>II-1</b> Typical J-3 Organization .....	<b>II-2</b>
	<b>II-2</b> Notional JTF C2W Cell .....	<b>II-3</b>
	<b>III-1</b> Reprogramming Process Current Roles .....	<b>III-4</b>
	<b>III-2</b> Reprogramming Process .....	<b>III-5</b>
	<b>III-3</b> Parametric Threat Change Validation (Crisis/Wartime) .....	<b>III-7</b>
	<b>III-4</b> Threat Change Analysis .....	<b>III-9</b>
	<b>III-5</b> Mission Data Development and Coding .....	<b>III-11</b>
	<b>III-6</b> EA Technique Reprogramming Process .....	<b>III-12</b>
	<b>III-7</b> OPF Development and Coding Functional Model .....	<b>III-13</b>

## EXECUTIVE SUMMARY

# REPROGRAMMING

## Handbook

### 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) are those systems that 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 command and control warfare (C2W).

EW/TSS reprogramming provides the means to respond to changes in threat signature characteristics or unique theater signal 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 of EW/TSS provides a timely means to respond to immediate threat changes and correct system deficiencies or mitigate the impact of the threat change.

The reprogramming process starts with the collection and processing of intelligence data, progresses through assessment and engineering phases, and results in the distribution and loading of updated software and, in some instances, hardware/firmware. Reprogramming is integrated into operational plans through EW mission planning and the weaponizing phase of the targeting process. While reprogramming is generally an EW function on the service component level, close coordination and deconfliction among

the service components in a JTF is done through the joint commander's electronic warfare staff (JCEWS). The staff coordination process begins with interaction between the operations and intelligence staff directorates at the JTF and component level, because a signature parametric change may be identified as a result of the intelligence process or from operational mission reports.

The Joint Command and Control Warfare Center (JC2WC) has reprogramming 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. 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 CINC/JTF EW officer is responsible for facilitating the exchange of reprogramming data among the components.

## **PROGRAM PARTICIPANTS**

The following commands and agencies participated in the development and review of this publication:

### **Joint**

Joint Command and Control Warfare Center (JC2WC), Kelly AFB, TX

### **Army**

US Army Intelligence and Security Command, Land Information Warfare Activity (LIWA), Ft Belvoir, VA

HQ US Army Intelligence and Security Command, MASINT Division, Ft Belvoir, VA

TRADOC System Manager (TSM)-Commanche, US Army Aviation Center, Ft Rucker, AL

### **Marine Corps**

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

### **Navy**

Commander, Naval Doctrine Command, Norfolk Naval Base, Norfolk VA

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

Electronic Warfare Operational Programming Facility (EWOPFAC), Chesapeake, VA

### **Air Force**

Air Force Information Warfare Center (AFIWC), Kelly AFB, TX

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

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

## 1. Background

a. Reprogramming. EW/TSS are those systems that 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. This document deals with the ability to reprogram EW systems and TSS systems whenever we come across new or unexpected enemy capabilities. Moreover, today's military operational planners must address the application of EW/TSS reprogramming within the framework of command and control warfare (C2W). The essence of C2W strategy is the complementary integration of the five elements of C2W: operations security (OPSEC), military deception, psychological operations (PSYOP), EW, and physical destruction. Threat parametric signature changes primarily affect the C2W 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 Joint Publication 1-02, *DOD Dictionary of*

*Military and Associated Terms and Chairman Joint Chiefs of Staff Instruction (CJCSI) 3210.03.*

(a) EAs are typically those offensive operations using nonlethal fires (jamming) and antiradiation missiles 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 our collection systems to rapidly and accurately identify electromagnetic emitters.

(2) Physical Destruction: Operations 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.

**Historical Example:**

***Operational commanders have a range of actions to handle changing threats. Air Force Information Warfare Center (AFIWC)/Office of Scientific Research (OSR) (Flagging) 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 over 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 wait for software changes to EW systems to be implemented; "If my aircraft systems can't see it or jam it, I'm going to kill it."***

b. C2W Staff Officers. C2W 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. The collection of signature data and subsequent identification, verification, validation, and loading of 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 defined as those computer controlled or automated systems that have reprogrammable software or firmware update capabilities. Changes in the threat and/or operational environment, such as threat activation of wartime reserve modes (WARM) or use of camouflage, concealment, and decoy techniques to alter

a threat system's signature, may affect EW/TSS performance.

b. Why Reprogram? EW/TSS reprogramming provides the means to respond to changes in threat signature characteristics or unique theater signal environments, enhancing the capability and survivability of the joint force. In preparation for or during actual hostilities, 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 or mitigate the impact of the threat change.

## 3. Reprogramming Process

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

(1) Army Threat Change Analysis Centers. The Army established centralized threat change analysis centers to evaluate threat change impact and multiple system-oriented EW reprogramming centers (RCs) for engineering support to develop, code, test, and distribute changes for service specific systems. The Army's threat change analysis center is the Army Reprogramming Analysis Team - Threat Analysis (ARAT-TA) located at Eglin AFB, Florida.

(2) Navy Electronic Operational Reprogramming Facility (EWOPFAC). EWOPFAC is the Navy/Marine Corps'

primary focal point for a library of over 20 EW systems. Reprogramming responsibilities include evaluating threat change impact on service specific EW systems through coordination with multiple engineering centers for development of threat data, coding, testing, and dissemination of validated changes to fleet users. EWOPFAC, a detachment of the Fleet Information Warfare Center (FIWC), is located in Chesapeake, Virginia.

(3) Air Force Threat Change Analysis. The Air Force Information Warfare Center (AFIWC/OSR) operates an automated flagging capability to identify threat parametric signature anomalies. AFIWC/OSR 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. Further assessments of threat change impact and development of software changes are performed by the EW Operational RCs - Eglin AFB, Florida, the 53rd Wing, Air Force Special Operations Command (AFSOC)/Electronic Combat Support Facility (ECSF), Hurlburt Field, Florida, and Warner Robins-Air Logistics Center (WR-ALC), Georgia.

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 reprogramming that takes place as an *immediate* response to threat changes in the tactical environment. After validation of the threat parametric signature data change, reprogramming is done as quickly as possible (normally taking place in 1-5 days).

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 upon 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 Database (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. It was originally conceived to support hardware design of EW systems employed by United States (US) combat forces. The reprogrammable systems supported include radar, radar warning receivers (RWR), combat identification, EW systems, antiradiation missiles (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 assessments based on all-source intelligence from foreign emitters.

(2) National Security Agency (NSA) national technical ELINT database (KILTING) on US and foreign emitters.

(3) US emitter data from Army, Naval, and Air Force EW support agencies via the US Non-Communications Systems Database (USNCSDB).

b. **Intelligence Community Support.** The following intelligence agencies perform one or more of the following functions—collect, analyze, produce, assess, and validate signatures—in support of 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 approved and

validated by Defense Intelligence Agency (DIA) 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 S&TI centers; and maintains the air, electronic, and ground order of battle databases.

(3) S&TI. The S&TI Centers are intelligence production centers managed by DIA or a service and tasked by the DIA to correlate, analyze, and produce scientific and technical intelligence based on all-source intelligence of assigned foreign emitters. S&TI centers 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 S&TI centers, NSA's KILTING database, and the AFIWC into the master EWIRDB for distribution to users. The NAIC is also responsible for analysis of red and gray fixed-wing, EW/GCI, and height finder systems.

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

(c) National Ground Intelligence Center (NGIC). NGIC is responsible for analysis of 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 the analysis of red and gray naval associated emitters, less those air related signals under the purview of NAIC. Additionally, ONI is responsible for maintaining data on non-US merchant shipping vessels.

c. MASINT Database. Emerging EW/TSS (F-22, Apache Longbow, Commanche, Advanced Threat Infrared Counter Measure, Brilliant Anti-Tank [BAT] munitions, etc.) require an effort parallel to the EWIRDB for MASINT data. MASINT data includes scientific and technical intelligence information obtained by quantitative and qualitative analysis of data derived from specific technical sensors for the purpose of identifying any 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 will require new knowledge bases and interpretation skills similar to ELINT EWIR analysis. These databases and interpretation tools are currently under development.

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.

# REPROGRAMMING IN THE JOINT/MULTISERVICE ENVIRONMENT

## 1. Background

In order to achieve a coordinated, integrated, and synchronized process for the reprogramming of EW/TSS during JTF operations, the JTF commander's battlestaff should be organized in a manner that facilitates the cross flow of reprogramming data and requirements among service components.

## 2. JTF Battlestaff

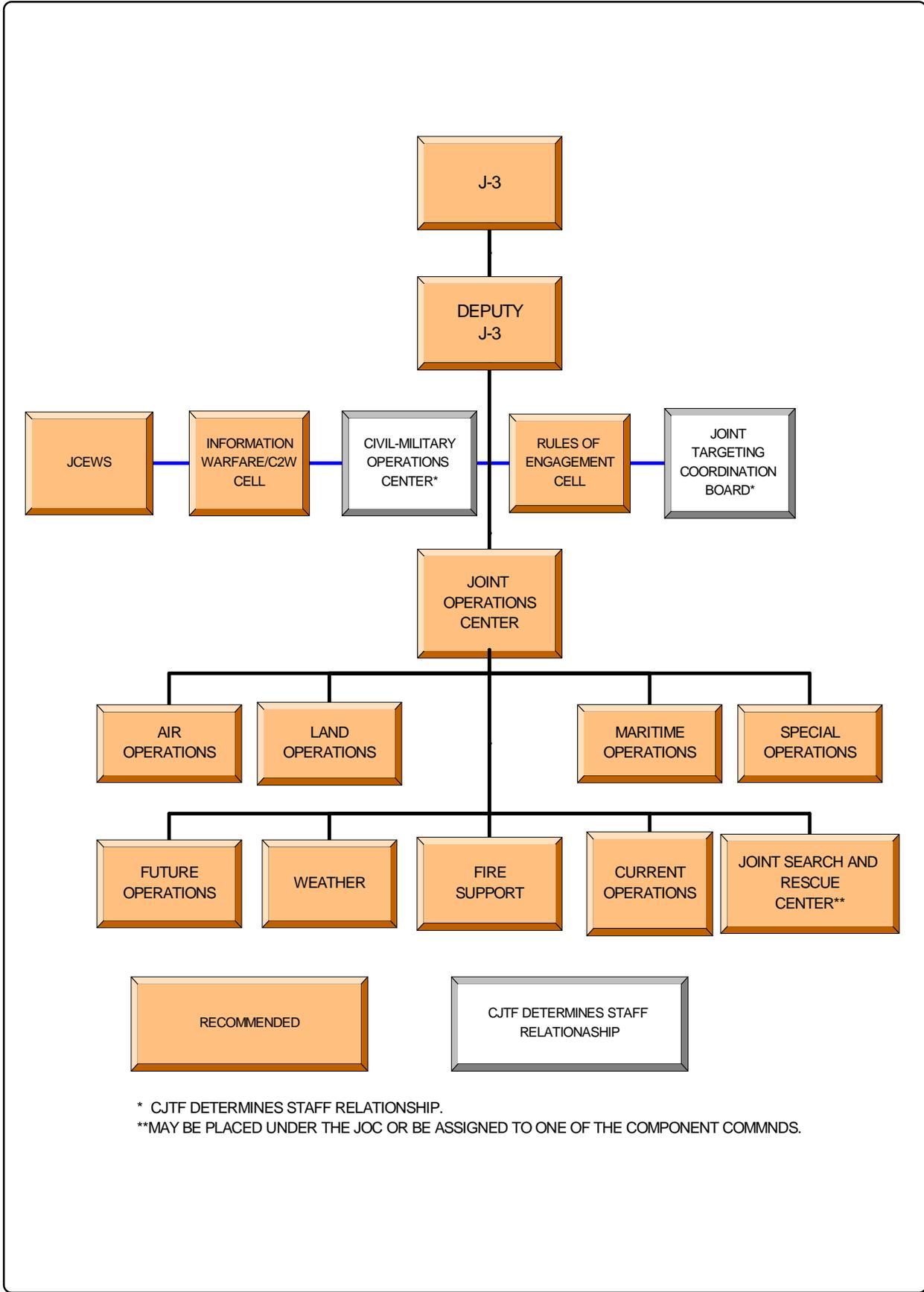
a. JTF Staff Organization. Normally, the nucleus of a JTF staff is formed from the host CINC staff and through augmentation from across DOD, usually not below the level of Army corps, Marine expeditionary force, numbered fleet, or numbered Air Force. When fully formed, the JTF staff will be composed of appropriate members in key positions of responsibility from each service or functional component having significant forces assigned to the command. The following discussion of the JTF staff focuses on the Operations Directorate (J-3).

b. J-3. The J-3 assists the commander in the discharge of 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. Figure II-1 depicts a typical J-3 organization.

c. Joint Commanders Electronic Warfare Staff (JCEWS). The JCEWS

provides a joint focus for denying the enemy the use of the electromagnetic spectrum while maintaining its availability for friendly exploitation. The JCEWS plans, coordinates, and integrates joint force EW operations. Through detailed, centralized, joint EW planning and standardized joint procedures, the JCEWS ensures the full use of joint EW capabilities as well as aggressive, decentralized EW execution. During contingency operations, the JCEWS is the staff organization that coordinates joint and multinational EW at the joint force level. This organization is responsible for the coordination of EW/TSS reprogramming and recommending EW targets to support the combatant commander's campaign plan to the Joint Targeting Coordination Board (JTCCB). Joint Force (JF) C32 cell, JFACC, or other joint targeting organizations established by the combatant commander. A typical JCEWS is depicted in Figure II-2.

d. Reprogramming. Reprogramming is integrated into operational plans through EW mission planning and the weaponeering phase of the targeting process for physical destruction. Specifically, C2 Attack considerations include reprogramming of smart munitions to optimize weapons effects based upon signature parametrics of the intended targets. C2 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 C2W Appendix of the Operations Annex to the JTF operations plan/order (OPLAN/OPORD).



\* CJTF DETERMINES STAFF RELATIONSHIP.  
 \*\*MAY BE PLACED UNDER THE JOC OR BE ASSIGNED TO ONE OF THE COMPONENT COMMNDs.

Figure II-1. Typical J-3 Organization

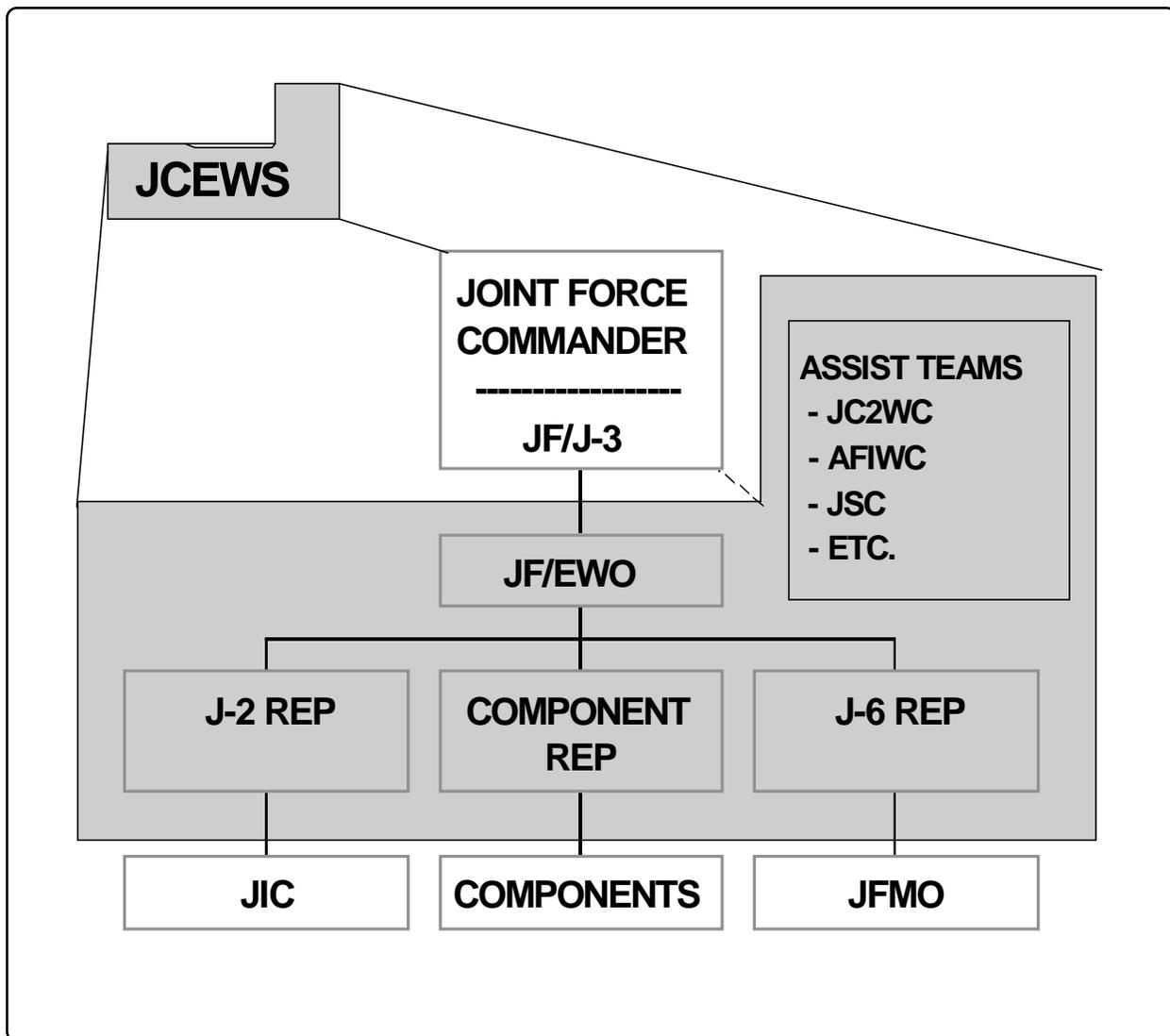


Figure II-2. Notional JTF C2W Cell

e. JCEWS 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 JCEWS 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, its implementation will require close coordination and deconfliction of efforts among the C2W 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 (J-2) representative to the JCEWS may, through the intelligence collection process, be the first to identify a possible parametric signature change. The identification of 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 Intermediate Processing Center (IPC) for further assessment and validation.

(2) Alternatively, the joint staff electronic warfare officer (EWO) may identify possible parametric signature changes through the analysis of 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 J-2 collection manager for tasking to JTF or national intelligence assets.

(3) Upon receiving validation of parametric signature changes, the operations staff will develop courses of action recommending to the commander a tactics, techniques and procedures (TTP) change, a software/firmware change, a targeting recommendation, or any combination of the above. A TTP may be developed instead of a reprogramming change or as an interim measure while waiting for development of a software/firmware change. The decision to

implement a TTP or a software/firmware change is made by each service component commander. If reprogramming is impractical due to operational concerns, modified threats should receive priority as operational targets and be recommended by the C2W/EW staff as high priority targets to the JTF targeting board. If a threat is targeted and battle damage assessment (BDA) reports destruction, the JCEWS will ensure service reprogramming centers receive this information.

### **3. Component Reprogramming**

a. US Army. Operational EW mission reports may originate at the C2W cell at division or corps level depending upon the echelon of force designated as the Army component (Army forces [ARFOR]). The division or corps EWO and G-2 representative will coordinate regarding the OCR 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 OCR will be submitted through intelligence channels, through the JTF IPC to the Joint Chief of Staff (JCS) J-2 who will task component S&TI centers (in peacetime) or the theater IPC (during crisis or hostilities) as appropriate. The S&TI centers (in peacetime) or the theater IPC (during crisis or hostilities) will validate the change and alert ARAT-TA and Communications and Electronics Command (CECOM) Software Engineering Center (SEC) 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.

b. US 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 electronic warfare coordination cell (EWCC) or C2W cell at the Marine air-ground task force (MAGTF)/

Marine forces (MARFOR) component commander level. At the MAGTF level, the commanding general, via the EWCC within the C2W 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 TCAR will be addressed for ACTION to the EWOPFAC and information (INFO) to the appropriate theater IPC during peacetime and ACTION to the IPC during crisis or war for threat validation. The appropriate S&TI center will validate suspected threat changes in peacetime while this responsibility will be transferred to the appropriate theater IPC during crisis or war. Upon receipt of a TCAR, EWOPFAC will begin assessing the impact of the reported threat change on Marine Corps tactical air (TACAIR), rotary wing, or air cargo/transport EW equipment. (The AN/ALQ-99 does not currently fall under the purview of EWOPFAC for reprogramming support.) If the threat change is validated by either the S&TI center or IPC and it is determined that reprogramming is necessary, EWOPFAC will immediately begin development of parametric data to recognize the threat and respond 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, EWOPFAC will send parametric data to the appropriate tactical system support center (TSSC)/software support activity (SSA) via the Multiservice Electronic Combat Bulletin Board System (MSECBBS) or by other means for engineering consistent with EW system requirements. The TSSC/SSA will disseminate updated EW libraries to fleet users via the most expeditious means and provide notification via the Electronic Warfare Reprogrammable Library (EWRL) Distribution Notice Message (DNM). The unit(s) receiving the

new library will provide follow-up feedback with the EWRL Receipt/Load Verification Message (RLVM) completing the reprogramming process.

c. US 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 command and control warfare commander (C2WC) at the combined task group (CTG)/combined task force (CTF) level depending upon the echelon of force designated as the Navy forces (NAVFOR) component. The NAVFOR component commander, usually via the C2WC, has internal management responsibility for the reprogramming effort of the deployed force, including necessary coordination. The TCAR will be addressed for ACTION to the EWOPFAC and for INFO to the appropriate theater IPC during peacetime and ACTION to the IPC during crisis or war for threat change validation. The appropriate S&TI center will validate suspected threat changes in peacetime while this responsibility will be transferred to the appropriate theater IPC during crisis or war. Upon receipt of a TCAR, EWOPFAC will begin assessing the impact of the reported threat change on Navy EW equipment. If the threat change is validated by either the S&TI center or IPC and it is determined that reprogramming is necessary, EWOPFAC will immediately begin development of parametric data to recognize the threat and respond with a SIM. The SIM is sent ACTION to the CTG/CTF commander and INFO to the submitting unit and other commands requiring the information. If the CTG/CTF commander decides to reprogram, EWOPFAC will send parametric data to the appropriate TSSC/SSA via the MSECBBS or by other means for engineering consistent with EW system requirements. The TSSC/SSA will disseminate updated EW libraries to fleet users via the most expeditious means and provide notification via the EWRL DNM.

The unit(s) receiving the new library will provide follow-up feedback with the EWRL RLVM completing the reprogramming process.

d. US Air Force. Operational Mission Reports (MISREPs) or OCRs may originate at any level but are collated and reviewed at the wing or numbered Air Force level depending upon the echelon of force designated as the Air Force forces (AFFOR) component. The AFFOR or major command (MAJCOM) will determine if further evaluation will be done on the MISREP or OCR. Flagging reports may provide additional information in the evaluation process. The reprogramming centers will 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 OCR. A SIM will then be sent to the appropriate operational commands and cognizant organizations. A Reprogramming Impact Message (RIM) may follow if appropriate. The implementation message will be sent by AFFOR or the appropriate MAJCOM (for example, Air Combat Command [ACC] or Air Force Special Operations Command [AFSOC]).

e. Special Operations Forces (SOF). SOF will 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 EH-53/54 helicopters are reported through Air Force channels to the Electronic Combat Support Facility (ECSF), Warner Robins Air Force Base, Georgia.

#### **4. Coordination Between Services**

a. CJCSM 227-86, *Joint EW Reprogramming*, requires the coordination of EW reprogramming among each of the services. The Joint Command and Control Warfare

Center (JC2WC) 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 JCEWS 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 C2W/EW officer. The CINC/JTF EW officer is responsible for facilitating the exchange of reprogramming data among the components. Each component C2W/EW officer is responsible for coordinating the EW reprogramming information among subordinate organizations. If a JCEWS cell is not formed, a separate EW cell can be formed to exchange reprogramming information and provide components the required information.

c. The CINC/JTF EW officer receives status information from each component C2W/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 CINC/CJTF staff can input a priority intelligence collection requirement to attempt to determine the specific signals causing the misidentification.

d. The CINC/JTF EW officer uses this information to keep the J-3 and commander informed. This information can be used 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.

# THE REPROGRAMMING PROCESS

## 1. Joint 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. In preparation 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. Reprogramming is used by the Army, Navy, and Marine Corps to refer to all time-sensitive reprogramming actions. The Air Force uses the term PACER WARE to refer to all realworld Air Force reprogramming actions.

c. Reprogramming Changes. Several types of changes constitute reprogramming. These changes fall into three major classifications: TTP, software, and firmware/hardware. The rationale for selection of 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 are to be implemented 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 can not afford to wait for engineers to design a software or hardware change.

(2) Software. Software changes include actual changes of programmable EW and TSS equipment. This type of change requires the support of an SSA 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, newer systems may be reprogrammed rapidly at the unit level 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 EWOPFAC, in coordination with multiple TSSCs/SSAs, provides reprogramming support to naval EW 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 services' reprogramming support programs are described in the following paragraphs:

a. Army Target Sensing Systems Rapid Reprogramming (ATRR). The mission for engineering and reprogramming Army TSS is established in Army Regulation (AR) 525-15, *Software Reprogramming Policy for Target Sensing Weapon Systems*, 1 Feb 93. The Army's Threat Change Analysis Center is the ARAT-TA, Eglin Air Force Base, Florida. The primary Army reprogramming software engineering centers are CECOM Software Support Center, Fort Monmouth, New Jersey, and Missile Command (MICOM) Software Support Center, Huntsville, Alabama. The Army also has ARAT-support cells (SC) located at TRADOC centers and schools for aviation, air defense artillery, intelligence, fire support, and armor. The ATRR process supports the tactical commander by—

(1) Providing a timely warning of a reprogramming requirement created by a change in the threat environment.

(2) Providing hardware and reprogramming software for reprogrammable Army TSS using the electronic warfare integrated reprogramming (EWIR) database (DB) and/or MASINT data as the baseline to discriminate between fielded systems' mission data and recently collected threat signatures from the battlefield.

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

b. Navy-Marine Corps EWRL Support Program. 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 effectively counter hostile WARM and to maintain a vigilant intelligence review effort in order to minimize the impact of threat WARM or threat parameter changes on Navy/Marine Corps reprogrammable systems (that is, RWRs, electronic warfare support (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 will continue to function effectively during crisis and war. EWOPFAC, located in Chesapeake Virginia, is a detachment of the FIWC and has been designated to provide this support. The EWOPFAC coordinates with any of nine engineering centers (EW system dependent) for routine cyclic updates or reprogramming support. The EWOPFAC DET, Honolulu, Hawaii, is responsible for the Pacific area of operations. The Radar Parametrics Data Set (RAPADS) portion of the Navy Emitter Reference File (NERF) is used to the maximum extent possible in the library building process. 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, etc.).

c. EWIR. The Air Force EW reprogramming process is called 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 between 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 AFIWC/OSR at Kelly Air Force Base, Texas. Flagging includes intelligence analysis and initial software system impact analysis. Hardware and additional software analyses are performed by the operational EW RCs at the 68th Electronic Combat Group, Eglin Air Force Base, Florida, and ECSF (AFSOC), Robins Air Force Base, Georgia. 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. Test validation of data is performed at the logistics and operational RCs.

d. MSECBBBS. Implementing reprogramming changes has become more timely and simple by using the MSECBBBS. 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 MSECBBBS 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 set (MDS) programs based on the EW/TSS organic to their unit but have no privileges to load an MDS on the MSECBBBS. In contrast, software support centers (SSCs) and TSSCs/SSAs can load and update MDS information but have restricted access to intelligence summaries (to protect operational security requirements). Service threat change analysis centers and EWOPFAC are responsible for maintaining access and privilege lists for their service. Principal products posted and maintained on the MSECBBBS are—

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

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

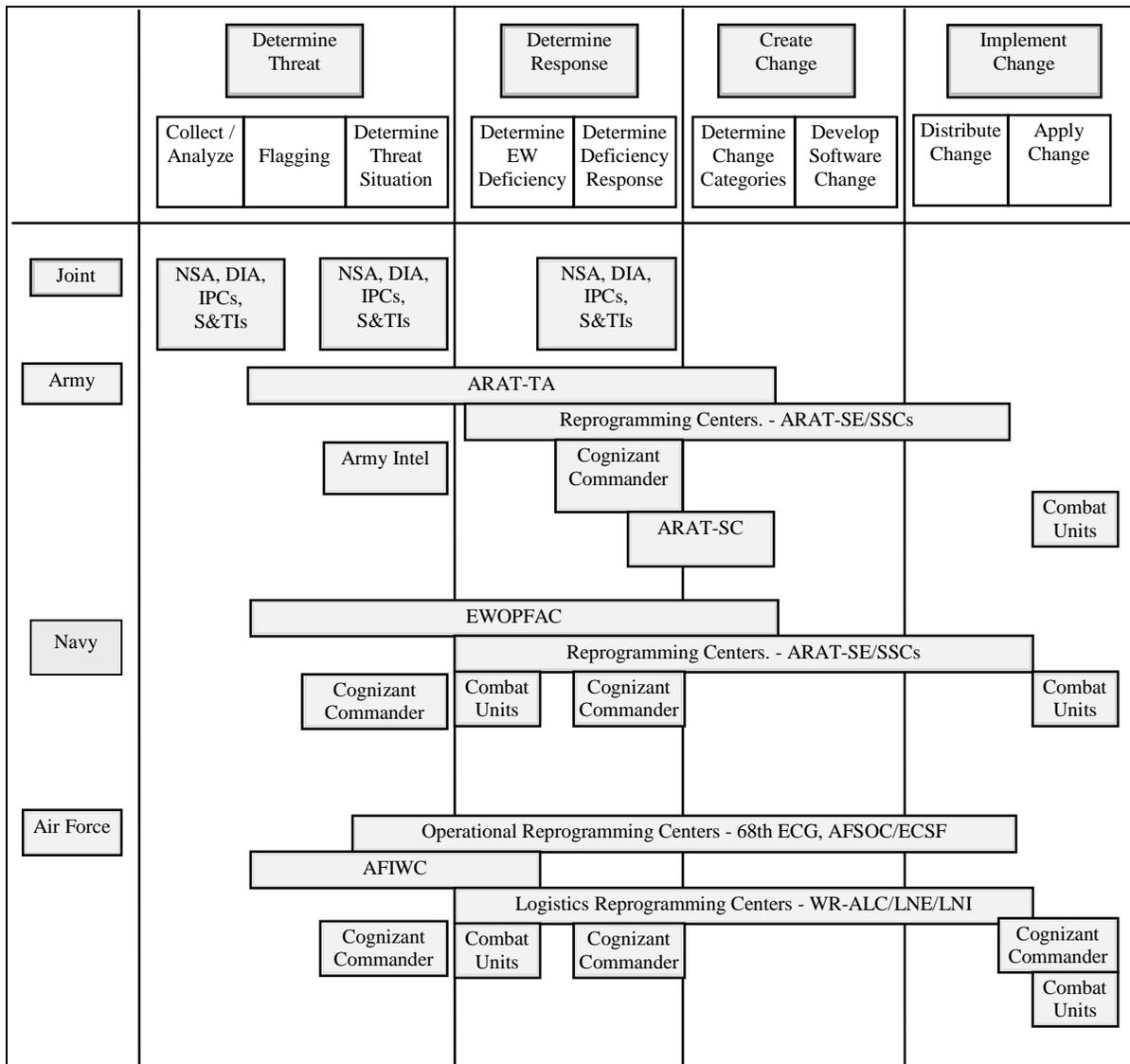


Figure III-1. Reprogramming Process Current Roles

### 3. The Reprogramming Process

**Process Phases.** The reprogramming process can be 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. A more detailed top-level view of this process is presented in Joint Publication 3-51, *Electronic Warfare in Joint Military Operations*,

### Appendix F, EW Reprogramming—Joint Coordination and Service Procedures.

a. Determine the Threat. Determining the threat is subdivided into three categories: collection and analysis, flagging, and determine the threat situation.

(1) Collection and Analysis. The first step in determining the threat involves the collection of all-source threat system parametric information and the reporting of that data to intelligence processing centers and service EW flagging activities.

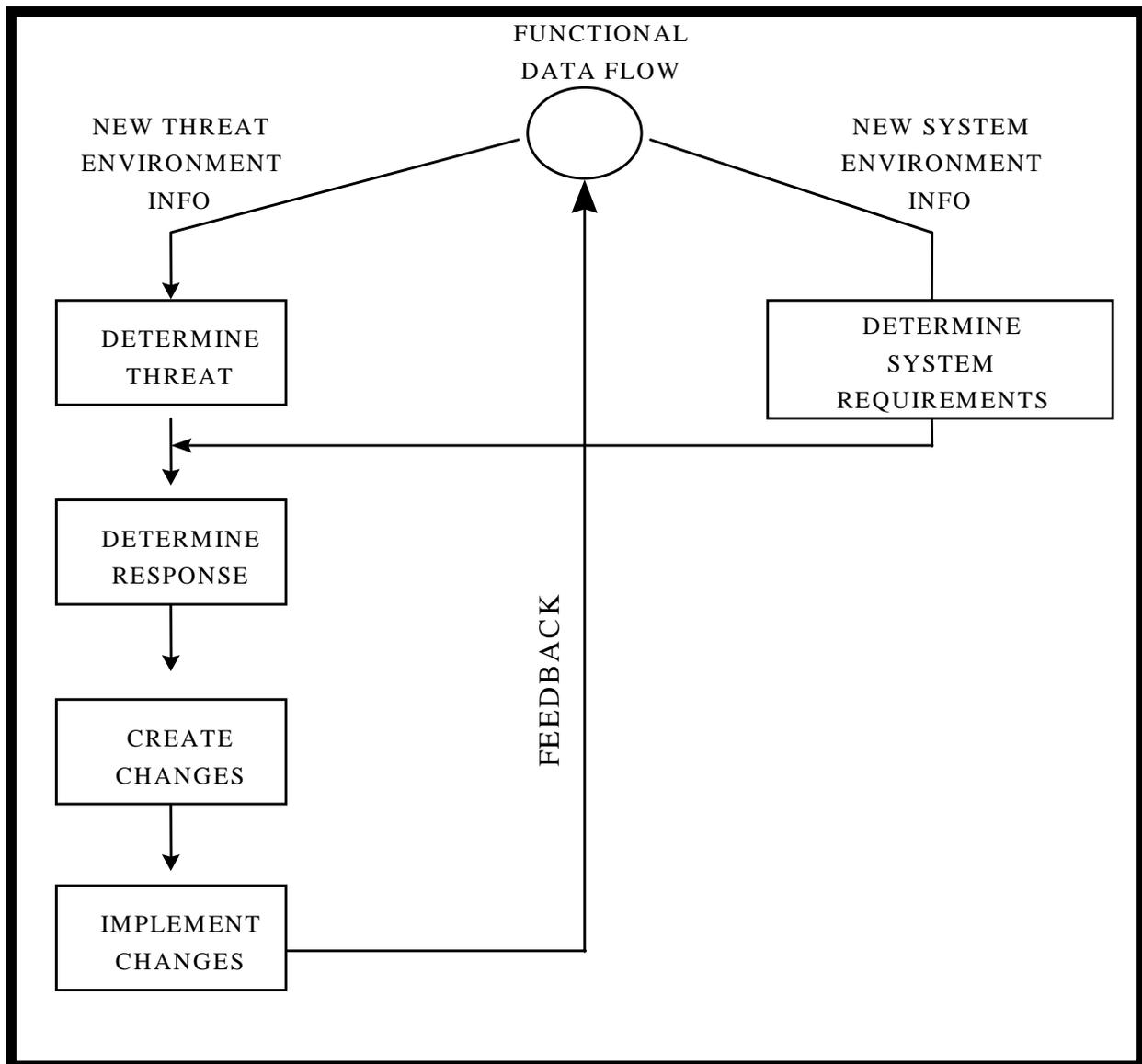


Figure III-2. Reprogramming Process

(a) S&TI centers develop detailed parametric analyses of threat radars. The resultant assessed technical intelligence is consolidated into a combined EWIRDB product with detailed parametrics for over 2000 radars. Besides these assessed parametric values, the EWIRDB includes the observed values provided by NSA and the reported values for American radars provided by the AFIWC.

(b) Threat changes are validated by the S&TI centers in peacetime and the theater IPCs during hostilities. These validated changes are forwarded to

the threat change analysis centers, EWOPFAC, and EW RCs/TSSCs/SSAs for application.

(2) Flagging. 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. Signal-related (parametric) variances are identified by intelligence analysts at the theater IPCs and service EW

flagging activities. 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 MDS. 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, AFIWC/OSR 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 collected ELINT signals of interest to manually flag other than expected results. ARAT-TA maintains full-time positions at AFIWC to build and maintain flagging models for supported EW/TSS. Flagging models are the key to providing worldwide awareness of EW/TSS capabilities in near-real-time (NRT). These models are automated to sort through hundreds to thousands of messages generated by collection systems each day; a task that would otherwise require dozens of highly trained analysts. Signals that are not correctly identified by AFIWC models are "flagged." This data is sent to ARAT-TA for analysis and system impact determination. Each MDS requires a unique model since the MDS contains a different mix of threats and system response/display options.

(c) The Navy's EWOPFAC 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 and 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) Determine the Threat Situation. 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) S&TI centers have resident foreign threat system experts and are designated as validation authorities in peacetime.

(b) During hostilities, the combatant command's IPC assumes the threat validation authority for threat

changes with the S&TI producers acting as technical advisors. Additional IPC responsibilities include the tracking and maintenance of tactical orders of battle (OBs) and locations for current threats.

(c) All the services acknowledge that some reprogramming changes are driven by considerations outside of the intelligence arena. 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 the OCR Message. The Navy and Marine Corps use the TCAR Message to insert their service concerns into the reprogramming cycle (see Appendix B for message formats).

•Parametric Threat Change Validation (Crisis and/or Wartime). Validation of threat system parametrics is a sophisticated engineering-level challenge that involves the examination of technical electronics intelligence (TECHELINT) and MASINT reporting considering all-source threat system capability assessments. National S&TI producers validate parametric entries in the national EWIR and MASINT DBs during peacetime. These producers also serve as technical advisors to the IPCs in peace and war. During a crisis and/or wartime situation, threat change validation authority is transferred from the S&TI centers to the IPC.

•Components of a Functional Parametric Threat Change Validation (Crisis/Wartime). Components of a functional parametric threat change validation model are defined in Figure III-3.

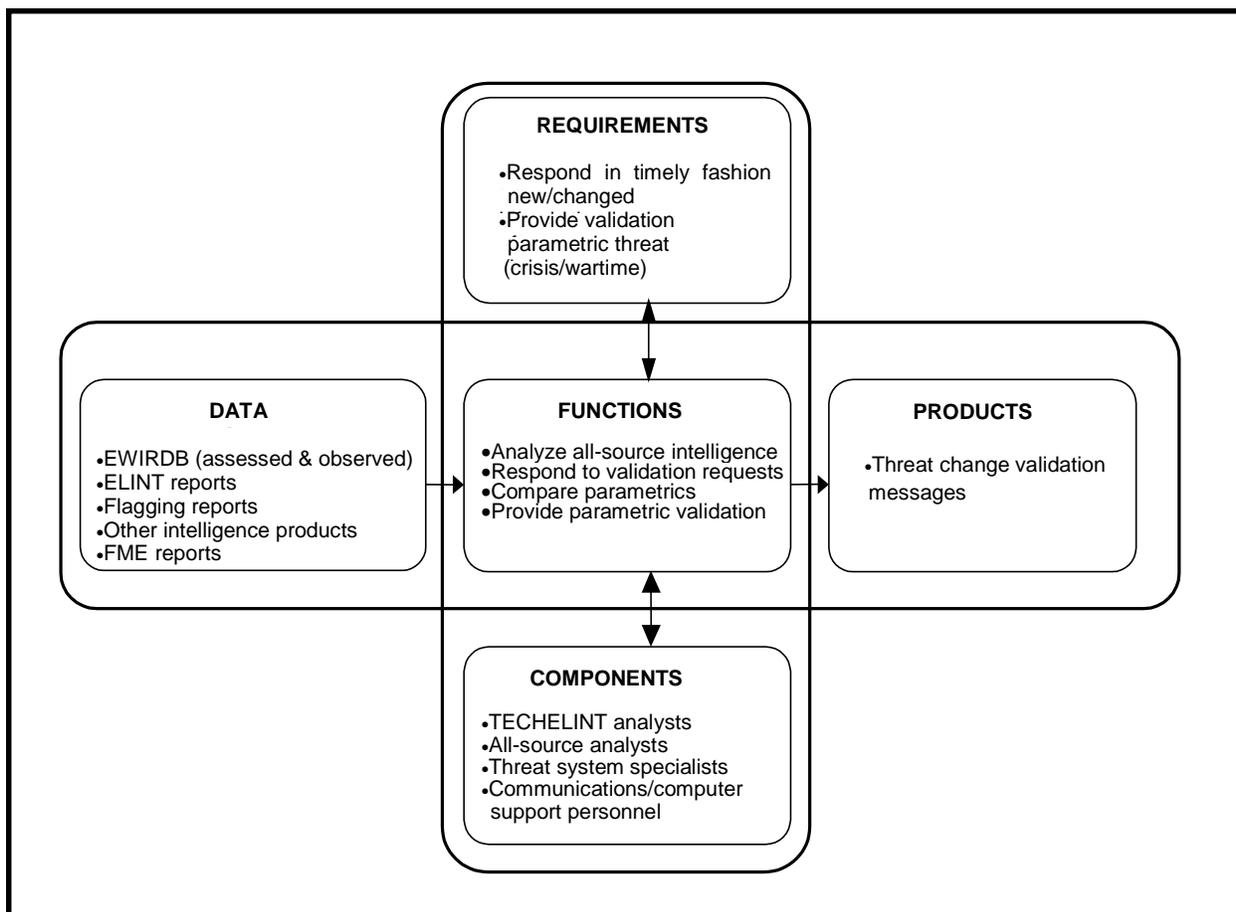


Figure III-3. Parametric Threat Change Validation (Crisis/Wartime)

(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 EWIR DB remains the comprehensive baseline of current validated data during crisis/wartime. However, since the EWIR DB has a lengthy update cycle (1-3 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 the careful consideration of the feasibility of an apparent threat change. Collector bias must be accounted for in these deliberations. Also, the possibility of system malfunctions must be considered.

(g) Components. Validation is a judgment requiring 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. In crisis/wartime, the Threat Change Validation Message (TCVM) is the primary method used by the theater IPCs 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.

b. Determine the Response.

(1) Validated threat change information is used to assess its impact upon friendly EW and TSS equipment before a decision is made whether to initiate reprogramming. Joint Publication 3-51 specifies two parts to determine the response determine deficiencies and determine 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 the application of 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. To evaluate the proposed concepts, the basic requirements, data, functions, components, and products of a functional threat change analysis model are defined in Figure III-4.

(a) Requirements. The threat change analysis function provides an initial assessment of the impact of new/changed

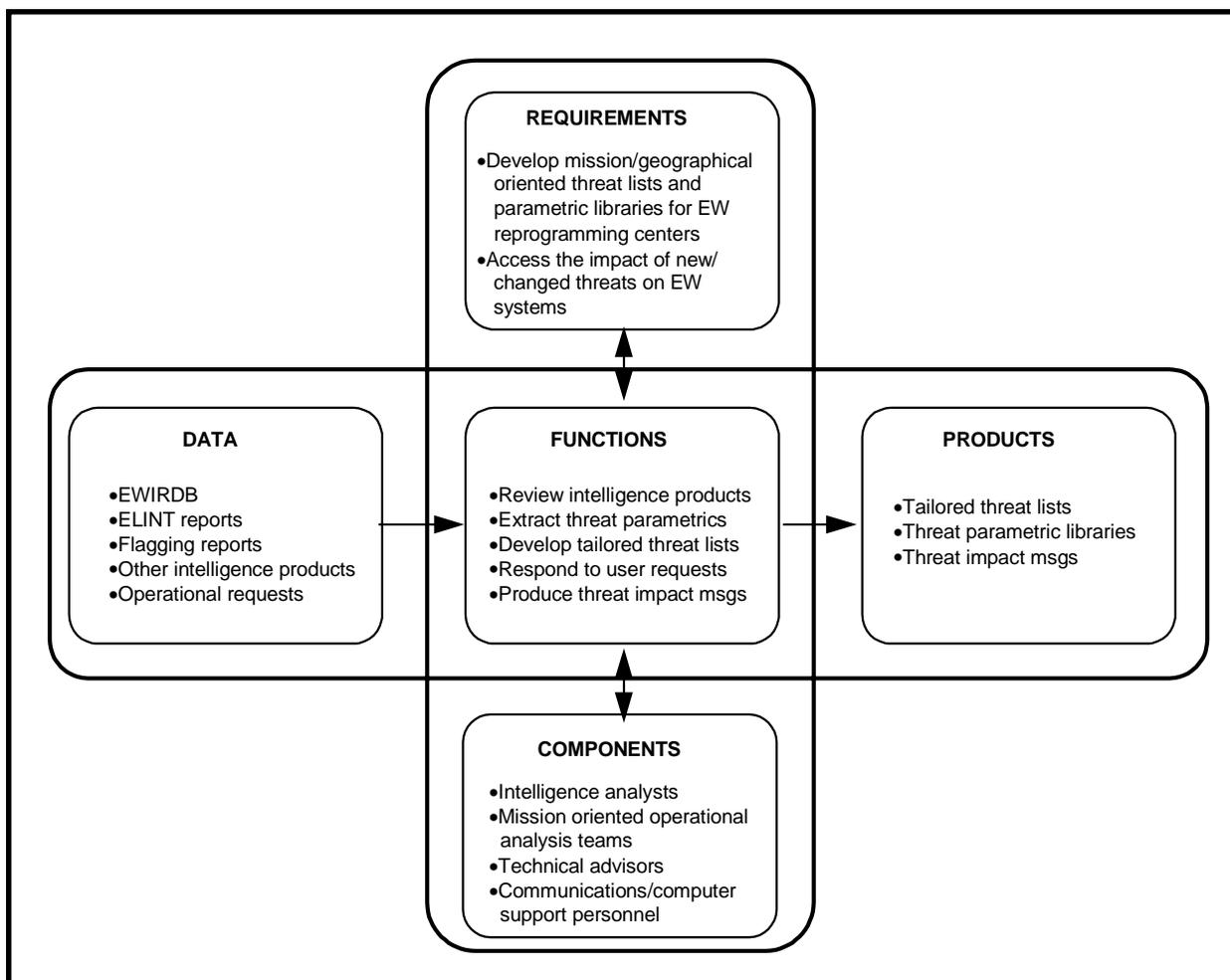


Figure III-4. Threat Change Analysis

threats on the individual EW systems (this includes EW flagging, determine EW deficiencies, determine response to deficiencies, and determine change categories actions). In addition, development of mission/geographically oriented threat lists and parametric libraries for individual EW systems also are included into 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 DBs that provide additional and/or tailored information for reprogramming. ELINT reports are viewed

directly 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 automated flagging of ELINT reports based on EW system models to filter the signals of interest. The new/changed data is used 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 and identifies 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 development of EW system MD/UDF. The SIM is sent to operational users to identify EW system deficiencies related to new/changed threat environments.

(3) Joint/C2W Decision Process. The C2W cell reviews the number of threat systems changing and their impacts to friendly systems, current targeting list, ATO, operations tempo, etc., 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 C2W cell should communicate this to the reprogramming centers to allow prioritization of more critical reprogramming actions. The C2W cell needs to be actively involved in the theater issues driving reprogramming and communicate decisions to the services and reprogramming centers.

c. Create the Change. During this phase several actions happen including developing and generating the change, testing/validation of the change, and documenting the change. This document focuses on the three most common types of reprogramming to discuss in more detail—

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. The reprogramming of jamming techniques will be addressed below in paragraph (2)(d). The basic requirements, data, functions, components, and products of a functional MD Development and coding model are depicted in Figure III-5.

(a) Requirements. The MD Development function provides mission and geographically tailored MD for EW systems and includes—determine the response to deficiencies, determine the change category, and develop the software change actions defined in Joint Publication 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. MDS 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. NGIC is the DOD technical leader to establish a comprehensive MASINT DB for DOD use. The ARAT program is working with NGIC, INSCOM, TRADOC, and TSS program managers to ensure that MDS development tools and process are developed with fielded systems.

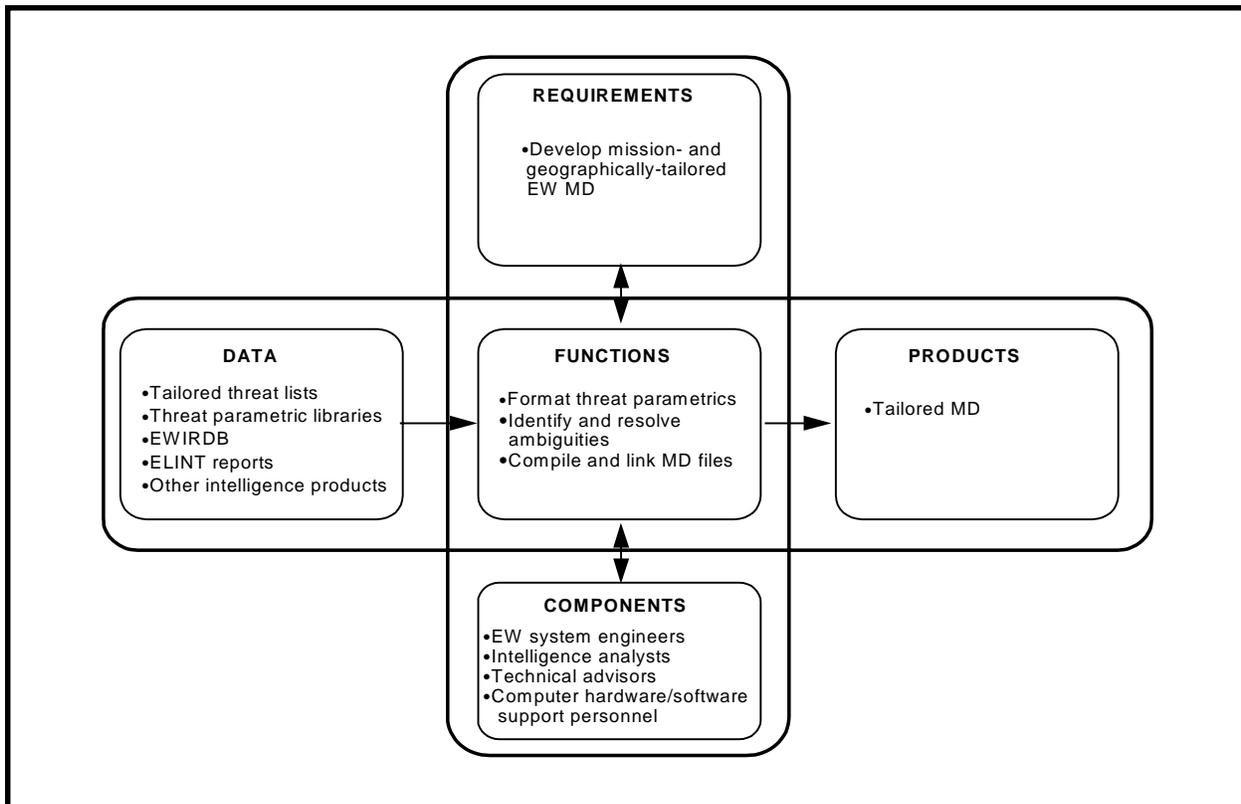


Figure III-5. Mission Data Development and Coding

(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 upon the expertise of the reprogrammer. At this time, ambiguity resolution is more of an art than it is 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 wide variety of computer hardware and MD development and analysis tools. They are supported in these tasks by intelligence analysts, technical advisors, and support personnel.

(e) **Products.** Mission and geographically-tailored MDs are developed and distributed to combat units.

(2) EA Jamming Technique Reprogramming. A functional model depicting the EA technique reprogramming processes is shown in Figure III-6.

(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 towards the latter.

(b) Data. The EA jamming technique reprogramming function requires data from many sources. Threat lists identify the specific threats to be included in the MD and 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 new techniques must be developed and optimized, 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/revise 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

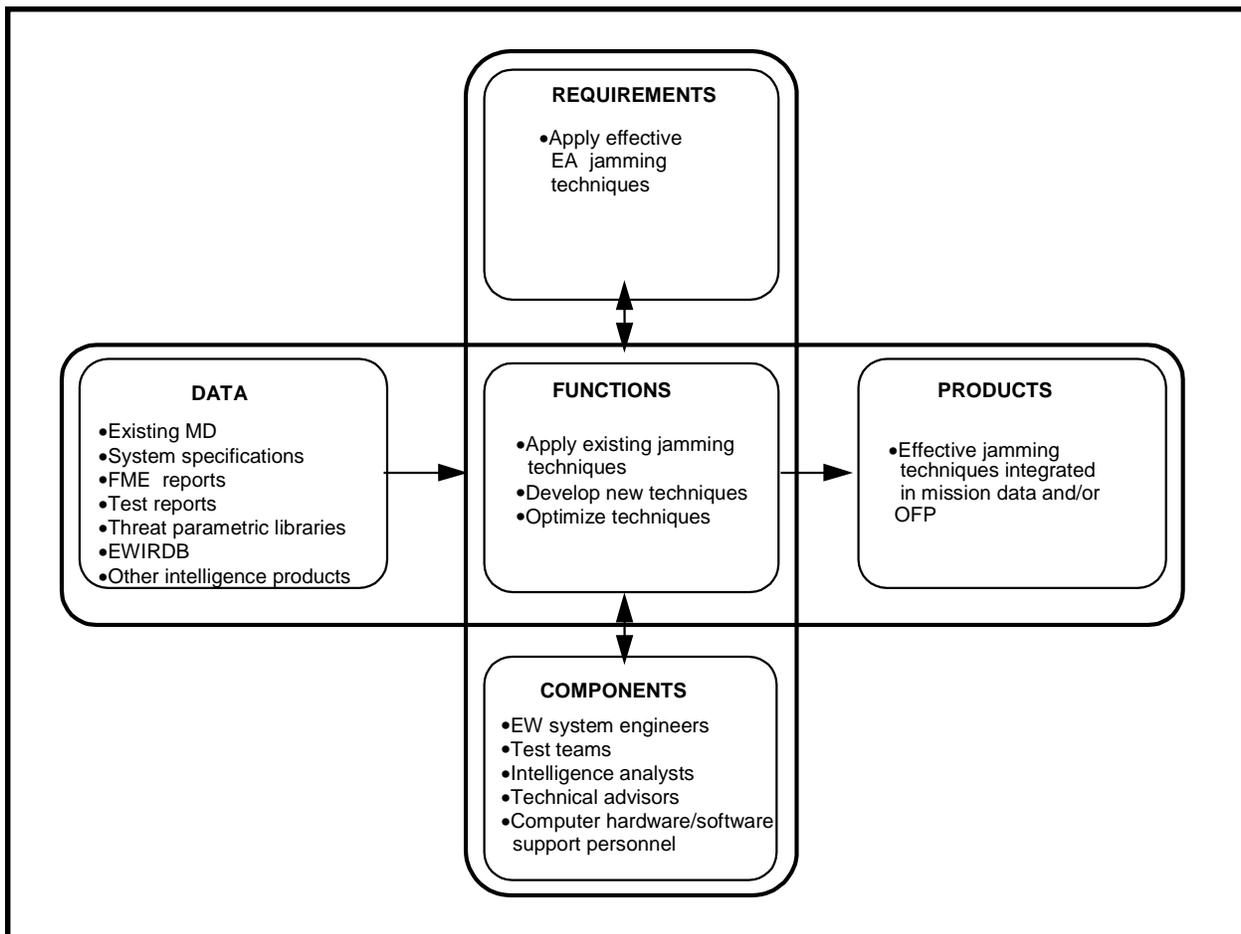


Figure III-6. EA Technique Reprogramming Process

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. Test teams and engineers are supported in these tasks by intelligence analysts, technical advisors, and support personnel.

(e) Products. The Reprogramming process produces new and optimized jamming techniques for use in 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. The OFP development and coding functional model is depicted in Figure III-7.

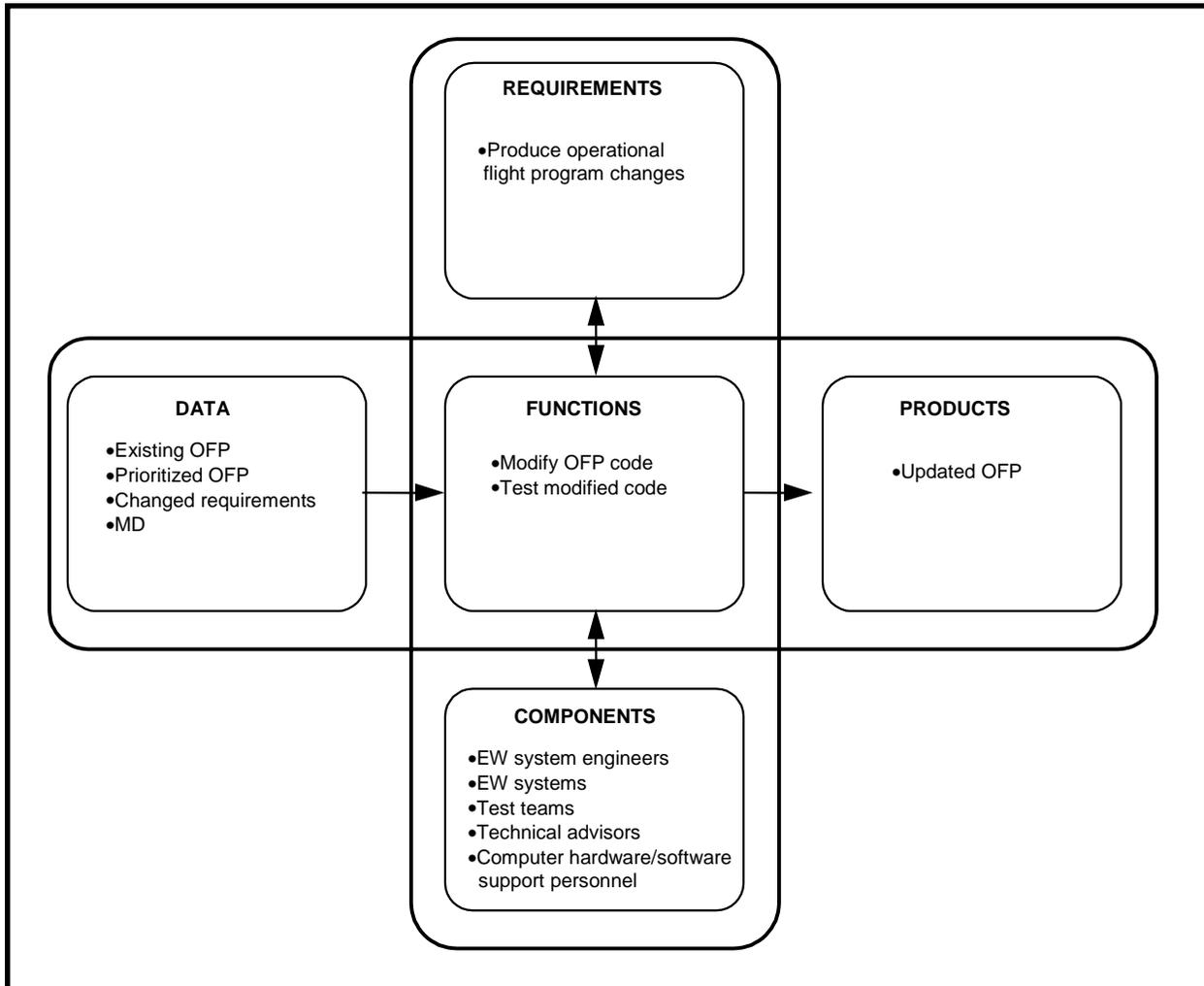


Figure III-7. OFP Development and Coding Functional Model

(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 Joint Publication 3-51.

(b) Data. The OFP development and coding functions use the existing OFP as a baseline. Prioritized OFP change requirements are used to 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 wide variety of computer

hardware, MD development, and analysis tools. They are supported in these tasks by technical advisors, support personnel, and test teams.

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

f. Implement the Change.

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

(2) Distribution of the change is accomplished through logistics channels, GENSER/DSCS 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 MSECBBBS accessed through the Secret Internet Protocol Network (SIPRNET) or secure telephone unit-III (STU-III).

## Appendix A

### POINTS OF CONTACT (POCs)

#### 1. Joint Command and Control Warfare Center EW Reprogramming Branch

JC2WC/PDR  
2 Hall Blvd, Ste 217  
San Antonio, TX 78243-7008  
DSN: 969-4617/4714

#### 2. US Army

##### a. US Army Land Information Warfare Activity (LIWA)

ATTN: IAIW-DD  
8825 Beulah Street  
Fort Belvoir, VA 22060-5246  
Voice: DSN 235-2266                      Comm: (703) 706-2266  
FAX: DSN 656-1003                      Comm: (703) 806-1003

b. Army Reprogramming Analysis Team - Threat Analysis (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 882-8899                      Comm: (904) 872-8899  
FAX: DSN 882-4268                      Comm: (904) 872-4268

##### 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 US Army Intelligence and Security Command (INSCOM) MASINT Division

ATTN: IAOP-OR-ITM

8825 Beulah Street

Ft Belvoir, VA 22060-5246

Voice: DSN 235-2464

Comm: (703) 706-2464

FAX: DSN 235-1149

Comm: (703) 806-1149

### 3. US Navy/Marine Corps

Fleet Information Warfare Center (FIWC)/Electronic Warfare Operational Programming Facility (EWOPFAC)

5100 Relay Road

Chesapeake, VA 23322

DSN 564-1336 Ext: 8634

Comm: (757) 421-8634

FAX 564-1336 Ext: 8623

Comm: (757) 421-8623

### 4. US Air Force

MAJCOM POCs:

ACC/DOIE Langley AFB, VA

DSN 574-5905

PACAF/DOTW Hickam, HI

DSN 315-449-5182

USAFE/DOTW Ramstein AB, GE

DSN 314-480-6582

CENTAF MacDill AFB, FL

DSN 965-4360

USAF Reprogramming Centers POCs:

53 Wing EWIR POCs

68 ECG/ERC

203 West D Ave

Suite 103

Eglin AFB, FL 32542

DSN 872-2166

Comm: (904) 882-2166

General Reprogramming and MSECBBBS Info—

68TSS/ETS  
DSN 872-2166

Specific Systems POCs:

36 ETS/EEC  
DSN 872-2052  
Systems: ALQ-131/188/184/184, U-2, SR-71, Mission Data, JAWS/ETSS,  
ALR-62/69/56

36 ETS/EED  
DSN 872-2827/2325/9713  
Systems: ALIC, HTS N/ASQ-213, HARM EC-130E COMPASS CALL, EF-11/EA-6B

36 EST/EEE  
DSN 872-3319  
Systems: ALE-40/45/47, ASTE, CMWS

36 ETS/EEF  
DSN 872-9342  
Systems: B-52, F-15 TEWS

36 ETS/EEI  
DSN 872-4642/4643  
Systems: B-1, B-2, F-22

Other Reprogramming Centers POCs:

AFSOC/ECSF Robins AFB, GA	DSN 468-2010	AFSOC Systems
---------------------------	--------------	---------------

WR-ALC/LNE Robins AFB, GA	DSN 468-2261	OFP
---------------------------	--------------	-----

Air Force Information Warfare Center POCs:

AFIWC/OSR 102 Hall Blvd, Suite 302 San Antonio, TX 78243	DSN 969-2021	Flagging
--	--------------	----------

## Appendix B

### 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.

#### I. FLAGGING MESSAGE (FLG) (ALL SERVICES)

DTG: DDTTTTZ MMM YY

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

From: AFIWC

To: Analysis Centers (ARAT-TA), others

Info: appropriate agencies, as required

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

Subject: [CODEWORD] - FLAGGING MESSAGE FLGYMMDD### FOR [System](U)

Ref: [MSGID, DTG, From, Subject] {as appropriate; TACELINT messages one per line}

1. (U) This is a [CODEWORD] message WHICH MAY POTENTIALLY IMPACT BATTLEFIELD SURVIVABILITY. PLEASE PASS TO ELECTRONIC WARFARE OFFICER/STAFF IMMEDIATELY.
2. (Classification) This flagging message contains information that potentially may affect [System] with operational flight program (OFP) [###] and mission data set (MDS) [###] in [Theater].
3. (Classification) Flagging Model Data: [YMMDDHHNNS] [ELNOT] [Flag Type] [Display] [Line#] {at a minimum}
4. (Classification) SIGNAL PARAMETRICS: [RF] [PD] [ST] [SP/IR] [MT] [PRI(s)] {at a minimum}
5. (U) POC IS [Name], [Unit/Organization], [Phone#(s) (DSN/CML)], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

#### Legend:

YMMDDHHNNS: Date-Time of signal emission; MM: Month (number, e.g. 08; SS: Seconds

Flag Type: what problem type flag is generated by the flagging model software

Display: the signal anomaly will cause this display to appear (if applicable) on the SYSTEM as it is currently programmed

Line#: corresponds to a line number in the appropriate MDS analytical Flagging table database

RF: Radio Frequency; PD: Pulse Duration; ST: Scan Type; SP/IR: Scan Period/Illumination Type; MT: Modulation Type; PRI: Pulse Repetition Interval

## II. SYSTEM IMPACT MESSAGE (SIM) (ALL SERVICES)

DTG: DDTTTTZ MMM YY

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

From: Analysis Center (ARAT-TA)

To: Affected Theater Command, Units/Commands, others

Info: Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), Materiel Manager, appropriate agencies, as required

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

Subject: [CODEWORD] - SYSTEM IMPACT MESSAGE SIMYY### FOR [System] (U)

Ref: [MSGID, DTG, From, Subject] {as appropriate}

1. (U) This is a [CODEWORD] message WHICH IMPACTS BATTLEFIELD SURVIVABILITY. PLEASE PASS TO UNIT ELECTRONIC WARFARE OFFICER/STAFF IMMEDIATELY.
2. (Classification) ATTENTION: THIS MESSAGE HAS THE POTENTIAL TO IMPACT ALL UNITS IN [Theater] EQUIPPED WITH [System] USING OPERATIONAL FLIGHT PROGRAM (OFP) ### AND MISSION DATA SET (MDS) ###.
3. (Classification) DESCRIPTION OF THREAT CHANGE: {be as specific as possible}
4. (Classification) AFFECT TO SYSTEM INDICATED ABOVE: {be as specific as possible}

Then select one of the following four choices based upon the situation:

5. (Classification) THIS THREAT CHANGE IS BEING EVALUATED TO DETERMINE IF MDS REPROGRAMMING IS WARRANTED. UNTIL NOTIFIED OF THE DECISION, THE FOLLOWING TACTICS, TECHNIQUES, AND PROCEDURES (TTP) ACTIONS SHOULD BE ADOPTED TO OVERCOME SYSTEM ANOMALIES/DEFICIENCIES: [TTP information] {be as specific as possible}
5. (Classification) MISSION DATA SET (MDS) REPROGRAMMING IS CURRENTLY UNDERWAY. UNTIL COMPLETED, THE FOLLOWING TACTICS, TECHNIQUES, AND PROCEDURES (TTP) ACTIONS SHOULD BE ADOPTED TO OVERCOME SYSTEM ANOMALIES/DEFICIENCIES: [TTP information] {be as specific as possible}
5. (Classification) THIS THREAT CHANGE HAS BEEN EVALUATED AND THERE WILL BE NO MDS REPROGRAMMING CHANGE. THE FOLLOWING TACTICS, TECHNIQUES, AND PROCEDURES (TTP) ACTIONS WILL REDUCE THE THREAT: [TTP information] {be as specific as possible}
5. (Classification) [TTP information] {be as specific as possible}

In any case, end paragraph with:

TTP INFORMATION HAS BEEN COORDINATED AND APPROVED BY THE [TRADOC Center].

6. (U) POC IS [Name], [Unit/Organization], [Phone#(s) (DSN/CML)], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**III. REPROGRAMMING IMPACT MESSAGE (RIM)  
(ARMY AND AIR FORCE ONLY)**

DTG: DDTTTTZ MMM YY

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

From: Analysis Center (ARAT-TA)

To: Affected Theater Command, Units/Commands, others

Info: Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), Materiel  
Manager, appropriate agencies, as required

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

Subject: [CODEWORD] - REPROGRAMMING IMPACT MESSAGE RIMYY### FOR  
[System] (U)

Ref: [MSGID, DTG, From, Subject] {as appropriate; SIM as a minimum}

1. (U) This is a [CODEWORD] message WHICH IMPACTS BATTLEFIELD SURVIVABILITY. PLEASE PASS TO UNIT ELECTRONIC WARFARE OFFICER/STAFF IMMEDIATELY.
2. (Classification) ATTENTION: THIS MESSAGE IMPACTS ALL UNITS IN [Theater] EQUIPPED WITH [System] USING OPERATIONAL FLIGHT PROGRAM (OFP) ### AND MISSION DATA SET (MDS) ##.
3. (Classification) THIS MESSAGE ANNOUNCES THE RELEASE AND AVAILABILITY OF MDS ### [Theater] TO REPLACE MDS ### [Theater] FOR THE ABOVE INDICATED SYSTEM. THE MAIN DIFFERENCE BETWEEN THESE TWO MDS'S IS THE FOLLOWING: {be as specific as possible}
4. (U) THE NEW MDS ### IS AVAILABLE FOR DOWNLOAD FROM THE MULTI-SERVICE ELECTRONIC COMBAT DATA DISTRIBUTION SYSTEM (MSECDDS). THE NEW FILE FOR MDS ### IS NAMED: MDS###.EXE. IT IS LOCATED IN THE [System] LIBRARY. MDS###.EXE IS A GROUP OF FIVE INDIVIDUAL FILES WHICH CAN BE SELF-EXTRACTED AFTER DOWNLOADING FROM THE MSECDDS. THE FILES CONTAINED IN MDS###.EXE ARE: ###LIST.TXT (KNEEBOARD SHEET), ###NOTES.TXT (PERTINENT NOTES), ###HEX.HEX (HEXADECIMAL FILE) FOR LAPTOP UPLOAD TO [System], ###HEX.UDM (HEXADECIMAL FILE) FOR MEMORY-LOADER/VERIFIER (MLV) UPLOAD TO [SYSTEM], AND ###FLAG.TXT (FLAGGING INFORMATION FILE). 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 TO YOU, PLEASE CONTACT THE POC.
5. (U) POC IS [Name], [Unit/Organization], [Phone#(s) (DSN/CML)], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**IV. IMPLEMENTATION MESSAGE (IMP)  
(ARMY AND AIR FORCE ONLY)**

DTG: DDTTTTZ MMM YY

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

From: Theater Command, MAJCOM

To: Units/Commands, others

Info: Analysis Centers (ARAT-TA), Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), Materiel Manager, others

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

Subject: [CODEWORD] - IMPLEMENTATION MESSAGE IMP[DTG] OF RIMYY###  
FOR [System] (U)

Ref: [MSGID, DTG, From, Subject] {as appropriate, SIM and RIM at a minimum}

1. (U) This is a [CODEWORD] message WHICH IMPACTS BATTLEFIELD SURVIVABILITY. PLEASE PASS TO UNIT ELECTRONIC WARFARE OFFICER/ STAFF IMMEDIATELY.
2. (Classification) [From] AUTHORIZES INSTALLATION OF MDS ### TO REPLACE MDS ### IN ALL AFFECTED [System] USING OPERATIONAL FLIGHT PROGRAM (OFP) ### IN [Theater].
3. (U) UNITS WILL REPLY TO THIS HEADQUARTERS VIA UNIT LOAD MESSAGE (ULM) WHEN INSTALLATION ACTION IS COMPLETED.
4. (U) POC IS [Name], [Unit/Organization], [Phone#(s) {DSN/CML}], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**V. UNIT LOAD MESSAGE (ULM)  
(ARMY AND AIR FORCE ONLY)**

DTG: DDTTTTZ MMM YY

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

From: Units/Commands

To: Chain of Command, Theater Command, MAJCOM, others

Info: Analysis Centers (ARAT-TA), Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), Materiel Manager, others

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

Subject: [CODEWORD] - UNIT LOAD MESSAGE ULM[DTG] OF MDS ### FOR [System] (U)

Ref: [MSGID, DTG, From, Subject] {as appropriate, SIM and RIM at a minimum}

1. (U) This is a [CODEWORD] message WHICH IMPACTS BATTLEFIELD SURVIVABILITY. PLEASE PASS TO ELECTRONIC WARFARE OFFICER/STAFF IMMEDIATELY.
2. (Classification) AT [DTG], THE BELOW LISTED UNIT(S) HAS(HAVE) COMPLETED INSTALLING MDS ### INTO ITS(THEIR) OPERATIONAL FLIGHT PROGRAM (OFP) ### EQUIPPED [System] IN [Theater]: {list specific unit(s)}
3. (Classification) PROBLEMS ENCOUNTERED: {if any, be as specific as possible}
4. (U) POC IS [Name], [Unit/Organization], [Phone#(s) {DSN/CML}], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**VI. OPERATIONAL CHANGE REQUEST (OCR)  
(ARMY AND AIR FORCE ONLY)**

DTG: DDTTTTZ MMM YY

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

From: Unit/Command, Theater Command

To: Chain of Command, Theater Command, MACOM, Materiel Manager, others

Info: Analysis Centers (ARAT-TA), Reprogramming Centers (ARAT-SE), TRADOC Centers (ARAT-SC), others

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

Subject: [CODEWORD] - OPERATIONAL CHANGE REQUEST OCR[DTG] FOR [System] (U)

Ref: [MSGID, DTG, From, Subject] {as appropriate}

1. (U) This is a [CODEWORD] message WHICH IMPACTS BATTLEFIELD SURVIVABILITY. PLEASE PASS TO ELECTRONIC WARFARE OFFICER/STAFF IMMEDIATELY.
2. (Classification) [Describe specific problem/background situation. Include System, Operational Flight Program (OFP), Mission Data Set (MDS), Theater information as appropriate]
3. (Classification) [Describe requested corrective action to be taken, to include Theater Command/MACOM validation]
4. (U) POC IS [Name], [Unit/Organization], [Phone#(s) {DSN/CML}], [e-mail(s)] {as appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**VII. ELECTRONIC WARFARE ANALYSIS REQUEST (EWAR)  
(ARMY AND AIR FORCE ONLY)**

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

INFO: appropriate agencies, as required

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

SUBJECT: [CODEWORD] - ELECTRONIC WARFARE ANALYSIS REQUEST  
EWARYY### (U)

REF: [MSGID, DTG, From, Subject] {as appropriate}

1. (U) This is a [CODEWORD] message.
2. (Classification) REQUEST ANALYTICAL SUPPORT IN ANSWERING THE  
FOLLOWING QUESTION(S): {be as specific as possible}
3. (U) POC IS [Name], [Unit/Organization], [Phone#(s) {DSN/CML}], [e-mail(s)] {as  
appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

**VIII. THREAT CHANGE VALIDATION REQUEST (TCVR)  
(ARMY AND AIR FORCE ONLY)**

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

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

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

SUBJECT: [CODEWORD] - THREAT CHANGE VALIDATION REQUEST

TCVRYYY### (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 [XXXXXX]) 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) {DSN/CML}], [e-mail(s)] {as  
appropriate}

DERIVED FROM:

DECLAS ON:

DATE OF SOURCE: DD MMM YYYY

## IX. SAMPLE MAINTENANCE INSTRUCTION MESSAGE (MIM) FORMAT (AIR FORCE ONLY)

FROM/(Reprogramming center releasing the message)//  
TO/(Units who use the affected system.)//  
INFO/(Their MAJCOMS and/or JFACCs/CFACCs/AOCs, and other agencies as required)//  
MSGID/GENADMIN/(Unit releasing the message)//  
SUBJ/PACER WARE MIM ALR-69 SWV 0806 PW 95 AWF001{U}// (See attachment 13 for message designation standards.)  
REF/A/MSG/68 ECG ERC/123456ZJAN95// (Reference all previous, pertinent messages.)  
AMPN/REF A IS SIM // (Describe the referenced message.)  
POC/(last name of author)/(rank)/(office symbol)/LOC:(base)/TEL:(DSN or commercial number)//  
RMKS/1. {U} THIS IS AN AIR FORCE PACER WARE MESSAGE.  
2. {?} (Specific maintenance instructions for loading the software change.)  
3. {?} (All maintenance impacts which are caused by the software change, to include additional tests that might be required.)  
4. {U} IMPLEMENTATION INSTRUCTIONS: INSTALLATION OF THIS CHANGE MUST BE APPROVED BY MAJCOM OR AIR COMPONENT COMMANDER. DO NOT INSTALL UNTIL PROPER IMPLEMENTATION INSTRUCTIONS ARE RECEIVED.  
5. {U} (Contact instructions if other than POC of message, otherwise not required.)  
6. {U} THIS IS AN AIR FORCE PACER WARE MESSAGE.//  
DECL/(date to declassify or OADR)//

### INSTRUCTIONS:

- A3.1. This message attempts to follow the US Message Text Format (USMTF) General Administrative (GENADMIN) message format. Originators will ensure the complete message complies with USMTF.
- A3.2. Each message identification number (e.g., PACER WARE OCR ALR-69 SWV 0805 PW 95 AWF001) **MUST** be complete on a single line. Do not break the string (PACER WARE... AWF001) to continue it on another line.
- A3.3. Multiple message identification numbers must be separated by a comma (,).
- A3.4. For current address listings, refer to the Air Force Plain Language Address Directory.
- A3.5. For exercise messages use SERENE BYTE in place of PACER WARE. **Do not use both.**
- A3.6. If message is classified, ensure paragraphs are correctly classified and marked, to include subject line. For ease of communication and distribution, keep the subject line  
UNCLASSIFIED.

**X. TIME COMPLIANCE TECHNICAL ORDER MESSAGE (TCTO) FORMAT  
(AIR FORCE ONLY)**

FROM/EW MGT DIR ROBINS AFB GA//LNERC//

TO/(Units who use the affected system.)//

INFO/(Their MAJCOMS and/or JFACCs/CFACCs/AOCs, and other agencies as required)//

MSGID/GENADMIN/(Unit releasing the message)//

SUBJ/PACER WARE TCT ALR-69 SWV 0806 PW 95 AWF001{U}// (See attachment 13 for message designation standards.)

REF/A/MSG/68 ECG ERC/123456ZJAN95// (Reference all previous, pertinent messages.)

AMPN/ REF A IS SCM ALR-69 SWV 0806 PW 95 AWF001// (Describe the referenced message.)

POC/(last name of author)/(rank)/(office symbol)/LOC:(base)/TEL:(DSN or commercial number)//

RMKS/1. {U} THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. {U} FOR COMM CENTERS: THE ELECTRONIC WARFARE MANAGEMENT DIRECTORATE (WR-ALC/LNERC) WILL BE TRANSMITTING (Number of data files) EWIR DATA FILES TO YOUR STATION WITHIN THE NEXT HOUR. THE LMF WILL BE CC AND THE CIC WILL BE FGBR. PLEASE DISTRIBUTE UPON RECEIPT.

3. {?} (This paragraph is divided into the following sections: Application; Purpose; When to be accomplished; By whom to be accomplished; What is required; How work is accomplished; Supplemental information; and Records.)

4. {U} (Contact instructions if other than POC of message, otherwise not required.)

5. {U} THIS IS AN AIR FORCE PACER WARE MESSAGE.//

DECL/(date to declassify or OADR)//

**INSTRUCTIONS:**

A3.1. This message attempts to follow the US Message Text Format (USMTF) General Administrative (GENADMIN) message format. Originators will ensure the complete message complies with USMTF.

A3.2. Each message identification number (e.g., PACER WARE OCR ALR-69 SWV 0805 PW 95 AWF001) **MUST** be complete on a single line. Do not break the string (PACER WARE... AWF001) to continue it on another line.

A3.3. Multiple message identification numbers must be separated by a comma (,).

A3.4. For current address listings, refer to the Air Force Plain Language Address Directory.

A3.5. For exercise messages use SERENE BYTE in place of PACER WARE. **Do not use both.**

A3.6. If message is classified, ensure paragraphs are correctly classified and marked, to include subject line. For ease of communication and distribution, keep the subject line UNCLASSIFIED.

**XI. THREAT CHANGE ANALYSIS REQUEST (TCAR) MESSAGE  
(NAVY AND MARINE CORPS ONLY)**

1. The unit/activity which 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.

**NOTE:** Classification of all message examples is for illustration purposes only.

FM: ORIGINATOR

TO: EWOPFAC CHESAPEAKE VA//30//

Applicable Unified Command Intelligence Center (IC)

INFO: Chain of Command

S E C R E T//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/01234E0

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//

**XII. EWRL RAPID REPROGRAMMING DISTRIBUTION NOTICE MESSAGE (DNM)  
(NAVY AND MARINE CORPS ONLY)**

1. Upon CTG/CTF direction to reprogram, EWOPFAC will deliver parametric data to the appropriate TSSC/SSA via the most expeditious, secure means possible.
2. The TSSC/SSA will engineer EWOPFAC data consistent with system requirements. The TSSC/SSA will provide notification of library update via the EWRL Rapid Reprogramming DNM to the following addressees:

ACTION: Cognizant Commander  
INFORMATION: All Concerned

3. Use the DNM example provided here. It contains the correct format and a sample report.

FM: TSSC/SSA  
TO: Cognizant Commander  
INFO: ALCON  
C O N F I D E N T I A L//N03430//  
EXER/NORTHERN FLEX//  
MSGID/GENOPS/(Originator)//  
SUBJ/DISTRIBUTION NOTICE MESSAGE 001-97 (U)//  
REF/A/RMG/(Cognizant Commander)/DTG//  
REF/B/RMG/EWOPFAC/DTG//  
NARR/REF A DIRECTS REPROGRAMMING. REF B IS SIM.  
POC///  
RMKS/1. (C) IAW REFS (A) AND (B), ORIG WILL POST UPDATED THREAT LIBRARY TO SECURE BULLETIN BOARD SYSTEM BTWN 17-18 JUL 96. TO DOWNLOAD, CALL (247) 787-2837 (DSN)432-8437.  
2. (U) RQST CONFIRM DATE/TIME AND AVAILABILITY OF TRANSMISSION LINK AND DESIGNATED PERSONNEL.  
3. (U) RQST RLVM UPON RECEIPT/LOAD.//  
DECL/XX//

**XIII. EWRL RAPID REPROGRAMMING RECEIPT/LOAD VERIFICATION  
MESSAGE (RLVM)  
(NAVY AND MARINE CORPS ONLY)**

The RLVM provides follow-up to the DNM and completes the rapid reprogramming process. The CTG/CTF or the specific unit receiving the new library originates the RLVM providing library and equipment status. Refer to the RLVM provided below for correct format and a sample report.

FM: Cognizant Commander/Unit(s) receiving new library  
TO: EWOPFAC  
TSSC/SSA  
INFO: Chain of Command  
UNCLAS//N03430//  
OPER/NORTHERN FLEX//  
MSGID/GENOPS/(Originator)//  
SUBJ/RECEIPT LOAD VERIFICATION MESSAGE 001-97 (U)//  
REF/A/RMG/(Appropriate TSSC/SSA)/DTG//  
AMPN/DISTRIBUTION NOTICE MESSAGE//  
POC///  
RMKS/1. CTF955 UNITS RCVD UPDATED THREAT LIBRARY 31JUL96. LOADS  
COMPLETE, SYSTEMS OPERATIONAL.//  
BT

## Appendix C

# 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, USACOM UNIFIED ENDEAVOR, etc.) to exercise the CINC/JTF C2W staff and the IPC. On a rotating basis, each CINC/JTF staff is exercised 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 IPC is also exercised. Additionally, support of the IPCs 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. ATRR Involvement in Army and Joint Service MDS Programming Exercises

a. The ATRR program is the Army point of contact for participation in MDS software programming exercises. The program has been involved in the demonstration of programming capability since 1988. In the future, the ATRR program objective is to expand Army participation in these exercises as units receive the capability to perform MDS programming at the unit level. MDS software programming will become more visible with the following initiatives:

(1) Army BRAVE BYTE. The Army component of the JC2WC PROUD BYTE exercise. BRAVE BYTE is an annual exercise that is conducted as part of a major theater level exercise such as Team SPIRIT or ULCHI FOCUS LENS in Korea or REFORGER in Europe. Units participating in these exercises are contacted to download and install exercise MDS.

(2) National Training Center. MDS software programming is being incorporated into NTC cycle training to exercise programming capabilities and tailor MDS operation for the NTC.

(3) External Evaluation (Ex Eval). MDS software programming tasks are being incorporated as Ex Eval for Aviation units.

b. Typical List of Army Reprogramming Training Objectives:

(1) Assess the ability of the ARAT-TA and ATRR-PO/SE/SC to adequately staff and equip software support and reprogramming facilities relative to number of participating units and systems to determine our collective capability to sustain a 24-hour operational tempo.

(2) Assess the timely and accurate flow of information between members of the software reprogramming community (ARAT-SC, CECOMs SED, PM-AEC, ARAT-TA).

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

(4) Evaluate the capability of the existing Multiservice Electronic Combat Bulletin Board System and communications architecture to exchange information and software reprogramming 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 FLAG models to detect parametric changes and anomalies.

(6) Evaluate the decision process that will create and implement a TTP change.

(7) Evaluate the reprogramming community's actions and training as it pertains to software rapid reprogramming.

(8) Determine if the scripted TACELINT simulators, signal generators, and exercise intelligence collection is adequate to replicate new or changed emitters for the purpose of rapid reprogramming.

### 3. Naval Exercises

a. The Navy has supported the joint EW communities PROUD BYTE exercises since 1992 through the NEPTUNE BYTE exercise program. NEPTUNE BYTE exercises come under the purview of the Joint Coordination of Electronic Warfare (JCEWR) process that examines the ability of the EWRL community to quickly provide TG/TF commanders with updated EW libraries by evaluating administration, equipment, communications, and personnel used in Navy, Marine Corps, and joint EWRL efforts. Managed by the Electronic Warfare Operational Programming Facility (EWOPFAC), NEPTUNE BYTE is designed to meet 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 for all deploying Atlantic Fleet Battle Group staff by Commander Second

Fleet. Since 1992, EWOPFAC has conducted training for JTF exercises three times per fiscal year. Training scenarios follow identical objectives as outlined for the NEPTUNE BYTE exercise program.

#### **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 for the exercise of 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 1 month of the annual exercise nor within the same quarter. (The annual exercise serves as a quarterly exercise.) The decision on which units and systems participate in the quarterly exercises are normally made by the unit commanders and appropriate MAJCOM.

## References

### Joint

Joint Pub 1-01, *Joint Publications System, Joint Doctrine and Joint Tactics, Techniques and Procedures Development Program*

Joint Pub 1-02, *DOD Dictionary of Military and Associated Terms*

Joint Pub 3-0, *Doctrine for Joint Operations*

Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*

Joint Pub 3-51, *Electronic Warfare in Joint Military Operations*

Joint Pub 5-00.2, *Procedures for Forming and Operating a Joint Task Force (Preliminary Coordination Draft)*

MCJS 227-86, *Plan for Joint Coordination of EW Reprogramming*

*Universal Joint Task List*, Office of the Chairman, The Joint Chiefs of Staff

### DIA

DDB-1730-72-91, *Joint Procedures for Intelligence Support to Electronic Warfare Reprogramming*

### Army

FM 71-100, *Division Operations*

FM 100-5, *Operations*

FM 100-6, *Information Operations*

FM 100-7, *Army in Theater Operations*

FM 100-15, *Corps Operations*

AR 381-SIGNATURES, *Army Target Signature Management*

AR 525-15, *Software Reprogramming Policy for Target Sensing Systems*

AR 525-22, *Electronic Warfare Policy*

TRADOC Pam 525-5, *Force XXI Operations*, Headquarters US Army Training and Doctrine Command, Fort Monroe, VA 23651-5000

*Army Target Sensing Systems Handbook*, Headquarters US Army Training and Doctrine Command, Fort Monroe, VA 23651-5000

Army Target Sensing Systems Rapid Reprogramming Project Plan, Army (TSS) Rapid Reprogramming Project Office, Communications and Electronics Command (CECOM) SED, IEW Division, Fort Monmouth, NJ 07703-5207

## **Marine Corps**

MCO 3430.2B, *Electronic Warfare*

FMFM 3, *Command and Control*

FMFM 3-1, *Command and Staff Action*

FMFM 6-1, *Marine Division*

FMFM 7-12, *Electronic Warfare*

FMFRP 0-14, *Marine Corps Support for the DOD Directory of Military and Associated Terms*

## **Navy**

OPNAV Instruction 3430.23B, *Tactical Electronic Warfare Reprogrammable Library*

OPNAV Instruction 5450.231, *Mission, Functions, and Tasks of the Fleet Information Warfare Center*

*Electronic Warfare Reprogramming Systems Handbook*, Electronic Warfare Operational Programming Facility (EWOPFAC), 5100 Relay Road, Chesapeake, VA 23322-4499

Neptune Byte Exercise Plan, Electronic Warfare Operational Programming Facility (EWOPFAC), 5100 Relay Road, Chesapeake, VA 23322-4499

Electronic Warfare Operational Programming Facility Reprogramming at Sea Training Plan

## **Air Force**

AFI 10-703, *Electronic Warfare Integrated Reprogramming*

# Glossary

## PART I-ABBREVIATIONS AND ACRONYMS

### A

AAA	antiaircraft artillery
ACC	Air Combat Command
AFDC	Air Force Doctrine Center
AFFOR	Air Force forces
AFI	Air Force instruction
AFSOC	Air Force Special Operations Command
AFIWC	Air Force Information Warfare Center
AIC	Atlantic Intelligence Command
ALCM	Air Launched Cruise Missile
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
ATF	Amphibious Task Force
ATO	air tasking order
ATRR	Army target sensing systems rapid reprogramming

### B

BAT	brilliant anti-tank
BDA	battle damage assessment
BG	battle group
blvd	boulevard

### C

C2	command and control
C2W	command and control warfare
C2WC	command and control warfare commander
CECOM	US Army Communications - Electronics Command
CECOM SEC	US Army Communications - Electronics Software Engineering Center
CENTAF	USAF Central Command
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
CTF	combined task force
CTG	combined task group

## **D**

DB	database
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 facility
ELINT	electronics intelligence
ELNOT	electronics intelligence notation
EP	electronic protection
ES	electronic warfare support
ev	evaluation
EW	electronic warfare
EWCC	electronic warfare coordination cell (USMC)
EWIR	electronic warfare integrated reprogramming
EWO	electronic warfare officer
EWIRDB	electronic warfare integrated reprogramming database
EWOPFAC	Electronic Warfare Operational Programming Facility
EWRL	Electronic Warfare Reprogrammable Library (USN)
EW/TSS	Electronic Warfare and Target Sensing Systems extreme

## **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
GENSER	General Service (message)

## **I**

info	information
INSCOM	Intelligence and Security Command
intel	intelligence
IPC	intermediate processing center
IW	information warfare

## **J**

J-2	Intelligence Directorate
J-3	Operations Directorate
J-5	Operational Plans and Interoperability Directorate
J-6	Command, Control, Communications, and Computer Systems Directorate
JAC (EUCOM)	Joint Analysis Center, European Command
JCEWR	joint combine of electronic warfare
JCEWS	joint force commander's electronic warfare staff
JCS	Joint Chiefs of Staff
JC2WC	joint command and control warfare center
JF	joint force
JFC	joint force commander
JIC	Joint Intelligence Center
JICPAC	Joint Intelligence Center, Pacific
JOA	joint operations area
JOC	joint operations center
JPOTF	joint psychological operations task force
JTF	joint task force

## **L**

LIWA	land information warfare activity
------	-----------------------------------

## **M**

MAGTF	Marine air-ground task force
MAJCOM	major command (USAF)
MARFOR	Marine forces
MASINT	measurement and signature intelligence
MCCDC	Marine Corps Combat Development Command
MD	mission data
MDS	mission data set
MEF	Marine expeditionary force
MISREP	mission reports
MSECBBS	Multiservice Electronic Combat Bulletin Board System
msg	message
MSIC	Missile and Space Intelligence Center

## **N**

NAIC	National Air Intelligence Center
NAVFOR	Navy forces
NDC	Naval Doctrine Center
NERF	Navy Emitter Reference File
NGIC	National Ground Intelligence Center
NRT	near-real-time
NSA	National Security Agency

## **O**

OB	order of battle
OCR	Operational Change Request
OFF	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 officer
POC	point of contact
PSYOP	psychological operations

## **R**

RAPADS	Radar Parametrics Data Set
RC	reprogramming centers
rep	representative
RIM	Reprogramming Impact Message
RLVM	Receipt/Load Verification Message (USN)
RWR	radar warning receiver

## **S**

S&TI	scientific and technical intelligence
SC	support cells
SE	shielding effectiveness
SEAD	suppression of enemy air defenses
SIFT	selectively improved flagging technique
SIGINT	signal intelligence
SIM	System Impact Message
SIPRNET	Secret Internet Protocol Network
SOF	special operations forces
SPC	Shared Production Center
SPINS	special instruction
SSA	Software Support Activity
SSC	software support center
Ste	suite
STU-III	secure telephone unit-III

## **T**

TACAIR	tactical air
TCAR	Threat Change Analysis Report
TCVM	Threat Change Validation Message

TCVR	threat change verifications request
TECHELINT	technical electronics intelligence
TF	task force
TG	task group
TIM	Threat Impact Message
TLAM	Tomahawk Land Attack Missile
TRADOC	Training and Doctrine Command
TSS	Target Sensing System
TSSC	Tactical System Support Center
TTP	tactics, techniques, and procedures

## U

US	United States
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy
USNCSD	United States Noncommunications System Database

## W

WARM	wartime reserve modes
WR-ALC	Warner Robins-Air Logistic Center

## PART II-TERMS AND DEFINITIONS

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

**Measurement and Signature Intelligence (MASINT).** 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. (Joint Pub 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 EW/TSS to maintain a greater level of effectiveness.

**Wartime Reserve Modes (WARM).** WARM are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition weapons, and countermeasure systems that (a) will contribute to military effectiveness if unknown to or understood by opposing commanders before they are used, but (b) could be exploited or neutralized if known in advance. WARM are deliberately held in reserve for wartime or emergency use and seldom, if ever, applied or intercepted prior to such use. (Joint Pub 1-02).

# Index

## A

AFIWC vii, I-2, I-3, I-4, III-3, III-5, III-6, A-3  
AFSOC I-3, II-6, III-3, A-3  
air force information warfare center (*see* AFIWC)  
Air force special operations command (*see* AFSOC)  
Ambiguity resolution III-11  
Antiradiation missiles (*see* ARM)  
ARAT-TA I-2, II-4, III-2, III-6, B-2, B-3, B-4, B-5, B-6, B-7, B-8  
ARM I-1, I-4  
Army reprogramming analysis team - threat analysis (*see* ARAT-TA)  
Army target sensing systems rapid reprogramming (*see* ATRR)  
ATRR III-2

## B

Battle damage assessment (*see* BDA)  
BDA II-4  
Block updates I-3

## C

C2 attack I-2, II-1  
C2 protect I-2, II-1  
C2W i, iv, v, vi, vii, I-1, I-2, II-1, II-3, II-4, II-5, II-6, III-10, Glossary-3  
CJCSM 227-86, joint EW reprogramming II-6  
Collection and analysis I-4, III-4  
Collector bias III-6, III-8  
Combat identification I-4  
COMINT I-5  
Command and control warfare (*see* C2W)  
Communications intelligence (*see* COMINT)  
Cyclical updates I-3

## D

Defense intelligence agency (*see* DIA)  
DIA I-4, Glossary-2

## E

EA iv, I-1, III-2, III-10, III-12, Glossary-2  
ECSF I-3, II-6, III-3, A-3, Glossary-2  
Electronic attack (*see* EA)  
Electronic combat support facility (*see* ECSF)  
electronic intelligence (*see* ELINT)  
Electronic protection (*see* EP)  
Electronic support (*see* ES)  
Electronic warfare (*see* EW)  
Electronic warfare integrated reprogramming database (*see* EWIRDB)  
Electronic warfare reprogrammable library (*see* EWRL)  
Electronic warfare reprogramming (*see* EW reprogramming)  
ELINT v, I-1, I-3, I-4, I-5, III-6, III-8, III-9, III-10, Glossary-2, Glossary-6  
EP I-1, III-2, Glossary-2  
ES I-1, III-2, III-6, Glossary-2  
EW i, iii, iv, v, vi, vii, I-1, I-2, I-3, I-4, I-5, II-1, II-3, II-4, II-5, II-6, II-7, III-1, III-2, III-3, III-4, III-5, III-6, III-8, III-9, III-10, III-11, III-12, III-13, III-14, A-2, B-2, B-3, B-4, B-5, B-6, B-7, B-10, B-11, C-2, References-2, Glossary-2, Glossary-3, Glossary-6  
EW reprogramming vi, I-2, II-6, III-1, III-2, III-3, III-4, III-8, C-2, References-2  
EWIRDB I-4, I-5, III-5, III-8, III-9, III-10, III-12, Glossary-2  
EWRL II-5, II-6, III-2, B-11, B-12, B-13, C-2, Glossary-2

## F

Firmware/hardware v, III-1  
FIWC vii, I-3, III-2, A-2, References-2 Glossary-2  
Flagging I-2, I-3, I-4, II-4, II-6, III-3, III-4, III-5, III-6, III-8, III-9, A-3, B-3, Glossary-4  
Flagging reports I-2, II-4, II-6, III-8  
Fleet information warfare center (*see* FIWC)  
FMS I-3, A-3, C-3, Glossary-2

Foreign emitters I-4  
Foreign military sales (*see* FMS)

## I

Intelligence data v, I-2, I-3, III-9, III-10  
Intermediate processing center (*see* IPC)  
IPC II-4, II-5, III-6, III-7, B-7, B-8,  
Glossary-2

## J

jamming I-1, II-6, III-8, III-10, III-12,  
III-13  
Jamming techniques II-6, III-10, III-12,  
III-13  
JC2WC vi, vii, II-6, Glossary-3  
JCEWS vi, II-1, II-3, II-4, II-6, Glossary-3  
JFC Glossary-3  
JOA I-2, Glossary-3  
joint command and control warfare center  
(*see* JC2WC)  
joint commander's electronic warfare  
staff (*see* JCEWS)  
joint force commander (*see* JFC)  
Joint operations area (*see* JOA)  
joint task force (*see* JTF)  
JP 3-51, electronic warfare in joint  
military operations, appendix F III-4  
JTF i, iii, iv, v, vi, I-1, I-2, II-1, II-3, II-4,  
II-6, II-7, C-3, Glossary-3

## K

Kilting database I-4

## M

MASINT v, vii, I-1, I-5, III-2, III-7, III-10,  
A-2, Glossary-3, Glossary-6  
MDS III-3, III-6, III-10, III-11, B-2, B-3,  
B-4, B-5, B-6, Glossary-3  
measurement and signature intelligence  
(*see* MASINT)  
Message formats i, iv, v, III-7  
Military deception I-1  
MISREPS II-6  
Missile and Space Intelligence Center  
(*see* MSIC)

Mission data set (*see* MDS)  
Mission planning i, v, II-1  
MSECBBS II-5, III-3, III-14, A-3, C-2,  
Glossary-3  
MSIC I-4, Glossary-3  
Multiservice electronic combat bulletin  
board system (*see* MSECBBS)

## N

NAIC I-4, Glossary-3  
National air intelligence center (*see*  
NAIC)  
National ground intelligence center (*see*  
NGIC)  
National security agency (*see* NSA)  
Navy electronic operational  
reprogramming facility I-2  
Navy emitter reference file (*see* NERF)  
Navy EWOPFAC vii, I-2, I-3, II-5, III-2,  
III-3, III-5, III-6, A-2, B-11, B-12, B-13,  
C-2, C-3, References-2  
NERF III-2, Glossary-3  
NGIC I-4, III-10, Glossary-3  
Nonlethal fires I-1  
NSA I-4, III-5, Glossary-3

## O

OCR II-4, II-6, III-7, B-6, B-9, B-10,  
Glossary-4  
Office of naval intelligence (*see* ONI)  
OFP III-8, III-10, III-13, III-14, A-3, B-2,  
B-3, B-4, B-5, B-6, Glossary-4  
ONI I-4, Glossary-4  
Operational change report (*see* OCR)  
Operational flight program (*see* OFP)  
Operational mission reports vi, II-3, II-6  
operations security (*see* OPSEC)  
OPSEC I-1, Glossary-4

## P

Parametric variations III-8  
Physical destruction v, I-1, II-1, II-3, II-7  
Psychological operations (*see* PSYOP)  
PSYOP I-1, Glossary-3, Glossary-4

## R

Radar I-4, III-2, B-11, Glossary-4,  
Glossary-6  
Radar parametrics data set (*see* RAPADS)  
Radar warnings receivers (*see* RWR)  
RAPADS III-2, Glossary-4  
Reprogrammable impact message (*see*  
RIM)  
RIM II-6, B-3, B-4, B-5, Glossary-4  
RWR I-4, II-3, Glossary-4

## S

S&TI Centers I-4, II-4, III-5, III-6, III-7,  
B-7, B-8  
Scientific and Technical Intelligence  
Centers (*see* S&TI Centers)  
SEAD I-2, Glossary-4  
Secret internet protocol network (*see*  
SIPNET)  
Selectively improved flagging technique  
(*see* SIFT)  
SIFT III-6, Glossary-4  
Signature v, vi, I-1, I-2, I-3, II-1, II-3, II-4,  
III-5, III-6, C-2, Glossary-3, Glossary-6  
SIM II-5, II-6, III-10, B-2, B-3, B-4, B-5,  
B-9, Glossary-4  
SIPNET III-14, Glossary-4  
SOF II-6, Glossary-4  
Software v, I-2, I-3, II-4, II-5, III-1, III-2,  
III-3, III-6, III-10, III-13, III-14, B-9, C-2,  
Glossary-4, Glossary-6  
Special operations forces (*see* SOF)  
suppression of enemy air defense (*see*  
SEAD)  
System impact message (*see* SIM)

## T

Target sensing systems (*see* TSS)  
TCAR II-4, II-5, III-7, B-11, Glossary-4  
Threat change analysis iv, I-2, I-3, II-4,  
III-1, III-2, III-3, III-5, III-8, III-9, III-10,  
B-11, Glossary-4  
Threat change analysis request (*see*  
TCAR)  
Threat parametric signature v, I-1, I-3  
TSS i, iii, iv, v, I-1, I-2, I-3, I-5, II-1, III-1,  
III-2, III-3, III-5, III-6, III-8, III-10,  
Glossary-2, Glossary-5, Glossary-6  
TTP II-4, III-1, III-2, B-2, C-2, Glossary-5

## U

US non-communications systems  
database (*see* USNCSDB)  
USNCSDB I-4

## V

Validation iv, I-2, I-3, II-4, II-5, III-3, III-6,  
III-7, III-8, III-10, B-6, B-8, Glossary-4

## W

WARM I-2, I-3, III-2, B-11, Glossary-5,  
Glossary-6  
Warner Robbins-Air Logistics Center (*see*  
WR-ALC)  
Wartime reserve modes (*see* WARM)  
WR-ALC I-3, III-3, A-3, B-10, Glossary-5  
53rd Wing I-3

**FM 34-72  
MCRP 3-36.1B  
NWP 3-13.1.15  
AFTTP(I) 3-2.7  
13 APRIL 1998**

**BY ORDER OF THE SECRETARY OF THE AIR FORCE**

**RONALD E. KEYS  
Major General, USAF  
Commander  
Headquarters Air Force Doctrine Center**

**FM 34-72  
MCRP 3-36.1B  
NWP 3-13.1.15  
AFTTP(I) 3-27  
13 APRIL 1998**

**DISTRIBUTION:**

**Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 115744, requirements for FM 34-72.**

