Army Regulation 525–15

Military Operations

Software Reprogramming for Cyber Electromagnetic Activities

Headquarters
Department of the Army
Washington, DC
19 February 2016

UNCLASSIFIED

SUMMARY of CHANGE

AR 525-15
Software Reprogramming for Cyber Electromagnetic Activities

This major revision, dated 19 February 2016--

- Changes the title from Software Reprogramming for Electronic Warfare and Target Sensing Systems to Software Reprogramming for Cyber Electromagnetic Activities (cover).

- Introduces expanded scope for software reprogramming support to cyber electromagnetic activities (chap 1).

- Adds responsibilities for Headquarters, Department of the Army, commands, and direct reporting units to provide support for electronic warfare reprogramming mission requirements (chap 2).

- Establishes cyber electromagnetic activities software reprogramming integration and interoperability implementation strategy (chap 3).

Headquarters
Department of the Army
Washington, DC
19 February 2016

*Army Regulation 525–15

Effective 19 March 2016

Military Operations

Software Reprogramming for Cyber Electromagnetic Activities

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation sets forth Army policy for software reprogramming for electronic warfare and target sensing systems. It covers managerial requirements necessary to implement electronic warfare and target sensing systems operations and training oversight for actions in peacetime and wartime, to include U.S. wartime reserve modes in order to administer counter threat changes. It establishes responsibility for Army counter-threat-change capabilities.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to all proponent agencies involved in research and development, acquisition, life cycle support, intelligence, planning and integration, and operations activities of electronic warfare and target sensing systems requirements.

Proponent and exception authority. The proponent of this regulation is Deputy Chief of Staff, G–3/5/7. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–3/5/7 (DAMO–ODE), Washington, DC 20310–3200.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–3/5/7 (DAMO–ODE), Washington, DC 20310–3200.

Distribution. This regulation is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 525–15, dated 23 August 2010.

UNCLASSIFIED

Contents—Continued

Chapter 1
Introduction

1–1. Purpose

This regulation establishes policy, assigns responsibilities, and provides strategy for integration and interoperability of cyber electromagnetic activities (CEMA). CEMA consist of cyberspace operations, electronic warfare (EW), and spectrum management operations. This policy emphasizes CEMA EW systems conducting electronic attack (EA), electronic warfare support (ES), and electronic protection (EP) through rapid software reprogramming (RSR). It is the Army policy for CEMA EW mission software products (MSPs) and Mission Enabling Software (MES). MSP include aviation survivability equipment software, mission data sets, and ground-based counter-improvised explosive device software, known as threat load sets, and nonmission software products such as the Army Reprogramming Analysis Team (ARAT) survivability software loader development and distribution. It describes the operation of Army capability to identify and counter changes to threat system composition, capabilities and signatures within the electromagnetic spectrum (EMS) and coordinated with spectrum management operations. MES encompasses all other Army Reprogramming Analysis Team–Program Office (ARAT–PO) products, for example, computer based training, system software support and maintenance, pattern developments, and CEMA threat verification and validation. The Army creates effective countermeasures to hostile introduction of new CEMA threat systems and changes that impact the Army's ability to detect, classify, declare, and counter the threat. The development of these countermeasures enhances security and preservation of friendly forces and equipment. This policy gives the Army a process which enables soldiers a reach-back RSR capability that will assist commanders to attain tactical superiority, achieve surprise, gain and retain the initiative, maintain awareness of new and emerging threats, and obtain decisive results while maintaining vigilant data collection efforts to detect introduction of new threat signals or changes to existing threats through the RSR of CEMA systems.

1–2. References

See appendix A.

1–3. Explanation of abbreviations and terms

See glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Program objectives

The principal objective of providing EW operational software programming support is to detect, classify, and declare new and changed cyber electromagnetic threats, and to support mitigation of these changes in order to allow commanders to conduct missions as required. There is special emphasis on reducing ambiguity because of the covert nature of new and changing threats. Failure to respond to these changes in threat composition or signature may disrupt operations and negatively impact mission accomplishment and force preservation. RSR for post-production software support (PPSS) includes ground and air EA, ES, and EP software and firmware including radar warning receivers, radar jammers, missile warning receivers, radar frequency interferometry systems, laser detection systems, integrated radio frequency, infrared countermeasures, electro-optical systems, countermeasure dispensing systems, counter radio-controlled improvised explosive devices, radio frequency jammers, communications jammers, the EW Planning and Management Tool, and future Army reprogrammable CEMA systems. The following activities will contribute to the Army's principal EW RSR objective above:

a. Field Army EW sensors, and smart weapon systems that are software configurable at the application level and/or hardware modular in order to adapt to hostile introduction of new and changed threats.

b. Exercise cyber security process and procedures in the development of mission software for EW systems.

c. Field Army capabilities that incorporate configurable software and firmware to counter threat changes.

d. Update threat reprogrammable EW mission software product content, (that is, threat library, operational flight program, filtering parameters, and geolocational parameters), via secure network to EW officers (EWOs) and aviation mission survivability officers (AMSOs) in Army service component commands (ASCCs).

e. Operate a sustained program that is software programmer accessible to collect and evaluate employment, deployment, and signature information for systems operating in the EMS. This program will be essential for providing friendly EA, ES, and EP and to successfully engage or defeat hostile or potentially hostile systems.

f. Maintain essential data about the U.S., allied forces, and coalition partners' RSR and their counters to enemy capabilities while ensuring effectiveness of capabilities through thorough testing and evaluation.

g. Support U.S. forces and others with RSR as required and consistent with security guidelines regarding the dissemination of threat and/or counter-threat information to non-U.S. forces.

h. Reduce or eliminate the effects of new and changed enemy-introduced threats.

i. Increase friendly RSR effectiveness during operations.

j. Reduce the susceptibility of U.S. systems to new and changed threats through increased situational awareness and improved EW capabilities to detect them. Support situational awareness capability.

k. Maintain the ARAT–PO rapid reprogramming infrastructure for Army EW software sustainment and tactical CEMA that supports the ASCC commander's ability to quickly respond to the combatant commander's missions across the full range of military operations as an Army core capability. ARAT–PO is chartered by U.S. Army Materiel Command (AMC) as the responsible official for EW Post Production Software Support under AMC-U.S. Army Communications and Electronics Command (CECOM) Software Engineering Center (SEC).

Chapter 2
Responsibilities

2–1. Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The ASA (ALT) will—

a. Ensure that sensor-based weapons and CEMA systems are developed using software reprogrammable signature detection, classification, and response capabilities that can be responsive and enabling to EW, spectrum management and cyber operations.

b. Coordinate with the Deputy Chief of Staff, G–2 (DCS, G–2) and the Deputy Chief of Staff, G–3/5/7 (DCS, G–3/5/7) to support the direction and control of requirements development for the data production and database capabilities needed to support signature software reprogramming.

c. Provide staff coordination with the DCS, G–2, the DCS, G–3/5/7 and the Deputy Chief of Staff, G–8 (DCS, G–8) (DAPR–FDI) for the development of essential EW systems and RSR capabilities identified through the Research, Development, and Acquisition Planning, Programming, Budgeting, and Execution System. Coordinate with U.S. AMC, within the scope of the National Disclosure Policy–1 (NDP–1), to encourage allied incorporation of friendly RSR capabilities into appropriate foreign military sales (FMS) systems.

d. Ensure all program managers (PMs) with software reprogrammable EW systems include integrated logistics assessments for EW systems and RSR in coordination with the CECOM SEC ARAT–PO. Ensure the requisite information technology infrastructure is established and maintained to support effective RSR functions.

e. Ensure PMs assess impact of RSR changes regarding system safety where the change to the reprogrammable software impacts the interface control document with the host platform or as appropriate.

2–2. Chief Information Officer/G–6

The CIO/G–6 will—

a. Serve as the liaison to relevant Army and Joint technical and user groups served by ARAT–PO for EW, and RSR to ensure proper bandwidth and priority.

b. Designate EW RSR as a tactical support element to combatant commanders using the EMS to identify threats, affect targets, and protect soldiers, on a non-interference basis with friendly communications and considered separate from standard information systems.

c. Ensure and support secure and classified communications, information management, and information technology capability for RSR functions.

d. Coordinate RSR information management and information technology hardware, infrastructure, and access requirements with Second Army, combatant commands (CCMDs), ASCCs, and the ARAT–PO as required preventing a mission gap.

e. Ensure that policies and doctrine do not cause an ASCC mission gap in performance of a Combatant Commander mission for the RSR infrastructure for CEMA systems (for example, spectrum management operations).

f. Ensure, through policy, EW EA systems deconfliction within the EMS. Provide spectrum management necessary to protect communications while permitting essential EA operations.

2–4. Chief, National Guard Bureau

The CNGB will—

a. Coordinate with Commander, AMC and CECOM for ARAT staff assistance visits to support unit cyber, EW, and/or RSR training and deployments as necessary.

b. Provide the necessary resources for EW and/or CEMA RSR requirements specific to U.S. Army National Guard unit EW readiness.

2–5. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Coordinate with the CIO/G–6, the DCS, G–3/5/7, DCS, G–8, and the CG, AMC to ensure that EW reprogramming requirements for collection, intelligence production, database maintenance, and related research and development are identified and integrated in accordance with Department of Defense Directive (DODD) 5250.01.

b. In coordination with the DCS, G–3/5/7, represent the Army Staff in Joint intelligence forums that discuss changes to threat system composition, capabilities, and signatures, and the means to counter those changes.

c. Ensure that scientific and technical intelligence centers, for example, National Ground Intelligence Center, are capable of vetting EW parametric data in support of RSR and maintaining vetted threat data to Army ground and airborne systems.

d. Support the integration of Title 50 (50 USC) intelligence products for use in mission software and products utilized by Army EW and CEMA systems.

e. The CG, U.S. Army Intelligence and Security Command will—

(1) In coordination with the DCS, G–2 and DCS, G–8, budget for and provide EW threat, signature, electronic intelligence, and applicable all-source data necessary to identify changes in the threat composition or operation to the ARAT–PO for rapid reprogramming of EW system capabilities based on requirements provided to the intelligence community by ARAT–PO, PEO and/or PM, and ASA (ALT).

(2) Develop and maintain threat tools and parametric databases to support current and future EW system requirements.

(3) Provide required Army contribution to EW and measurement and signal intelligence reprogramming databases, as appropriate.

(4) In coordination with CECOM, SEC, and/or ARAT–PO and the Research, Development, and Engineering Command (RDECOM), Communications-Electronics Research, Development, and Engineering Center (CERDEC), review and validate input from ASCCs. Review and approve ASCC-recommended procedures for receiving new and changed threat data from CCMD.

(5) Review ARAT–PO mission software production requirements and provide updated EW databases for air and ground EW and/or CEMA systems.

(6) Execute policy for 50 USC intelligence products utilized in developing or reprogramming EW mission software and products.

(7) In coordination with the DIA Intelligence Mission Data Center (IMDC), ensure that future Life Cycle Mission Data Plan requirements are evaluated during the early system acquisition cycle as a factor to proceed past a Milestone B decision.

2–6. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Validate the Army's EW operational support infrastructure efforts to ensure that timely and effective mission software reprogramming is available to meet mission requirements.

b. Ensure Army EW requirements, to include RSR, are represented, as required, within relevant PEG: General Purpose Forces, Information Management (Sustaining), Intelligence, Army National Guard, U.S. Army Reserve, Modernization, Supply and Maintenance, and School and Institutional Training.

c. Coordinate with the appropriate EW organization within Army Commands, ASCCs, Direct Reporting Units, and the Joint community to ensure the ARAT–PO EW and RSR operations are integrated, as applicable.

d. Develop RSR policy, programs, and force requirements for Regular Army, Army National Guard/Army National Guard of the United States, U.S. Army Reserve (USAR), and U.S. Army Special Operations Command (USASOC).

e. In coordination with AMC, ASA (ALT), and TRADOC, ensure EW and RSR are addressed in system requirements documents.

f. Coordinate RSR matters with the other military Services and allies as permitted by disclosure and security classification directives.

g. Oversee the Army's contribution to North Atlantic Treaty Organization Emitter Database and U.S. Electromagnetic System (USELMS) Database.

h. In coordination with the DCS, G–2, represent the Army Staff in Joint intelligence forums that consider counter-threat-change matters and advise other counterparts.

i. Headquarters, Department of the Army staff proponent and ARAT–PO contact for EW RSR policy actions within the Army, and ARAT support to other Services, Department of Defense, and other government agencies. This includes support to homeland defense requirements per Army policy and direction.

j. Develop and integrate EW training policy that includes RSR as a standing objective in major Army training exercises.

k. Establish the Implementation Authority for mission software implementation consistent with Army and Joint policies.

2–7. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Ensure that logistical policies support the capability to perform software installation and RSR at the platform or weapon level.

b. Support the AMC, CECOM, ARAT–PO with the necessary logistical sustaining resources to ensure a robust, efficient, and rapid software reprogramming infrastructure and PPSS across the CEMA portfolio of systems.

c. Represent ARAT–PO sustainment requirements in the Army Planning, Programming, Budgeting, and Evaluation System.

d. In conjunction with the DCS, G–2, ensure the ARAT–PO is involved in the development, delivery, and maintenance of any EW RSR capability provided under FMS.

2–8. Deputy Chief of Staff, G–8

The DCS, G–8 will—

a. Coordinate with AMC (ARAT–PO) for review and validation of requirements for EW RSR developmental efforts to compete for resources during the program objective memorandum and program budget review process.

b. Plan and program resources for ARAT–PO research, development, test, and evaluation activities.

c. Ensure that CEMA systems transitioning to sustainment from ASA (ALT) PEOs and/or PMs ensure efficient use of existing Government organic core sustainment infrastructure (that is, PPSS) in support of new system acquisition.

2–9. Chief, Army Reserve

The CAR will—

a. Coordinate with Commander, AMC and CECOM for ARAT staff assistance visits to support unit cyber, EW, and/or RSR training and deployments, as necessary.

b. Ensure Army Reserve training requirements for EW and RSR are included in the USAR training PEG.

c. Ensure the requisite operational and logistical resources are available at the unit level to support ARAT–PO staff assistance visits.

2–10. Commanding General, U.S. Army Materiel Command

The CG, AMC will—

a. Designate the ARAT–PO via charter as the Army responsible official for—

(1) EW PPSS mission software reprogramming infrastructure and EW support to CEMA, as required.

(2) RSR capability assessment office for operational CEMA (EW and cyber) equipment.

b. Provide the ARAT–PO with the resources and facilities necessary to provide timely EW software reprogramming compliant with 10 USC 2460 definition of depot-level maintenance and repair which includes RSR support to meet current operational mission requirements and ensure adequate infrastructure to meet anticipated and/or future requirements no later than 4 years after initial operational capability.

c. Coordinate with and provide DCS, G–2 and the ARAT–PO with threat system intelligence support necessary to continuously conduct system engineering evaluations. Ensure the ARAT–PO coordinates with acquisition PEOs and/or PMs developing and fielding systems operating in the EMS so the effects of CEMA PPSS are adequately represented in order to support leader decisions centered on organizing, equipping, and employing ground forces.

d. In coordination with TRADOC organizations (TRADOC capability managers (TCMs), Centers of Excellence, and Schools) provide continuous review from a software engineering and system capability perspective and evaluation of methods, models, and tools, doctrinal publications, EW software engineering reprogramming training, and other training as directed.

e. Ensure and incorporate reprogrammable memory for all EW and applicable cyber systems operating in the EMS while observing operations security guidance.

f. Direct and provide resources to ARAT–PO to support the software requirement for all EW systems to be reprogrammable at the organizational maintenance or operator level.

g. Coordinate with the DCS, G–4 and DCS, G–8, to ensure Army EW PPSS requirements are incorporated in appropriate budgetary requirements.

h. Ensure EMS deconfliction strategies and capabilities necessary to protect communications while still permitting essential EA operations to be incorporated into all EA, ES, and EP systems associated with RSR.

i. Coordinate with the CIO/G–6 to ensure a classified communications capability to provide EW mission data sets directly to the field commanders.

j. Require ARAT–PO support to Joint and Army exercises as required, life cycle sustainment of EW and/or cyber systems, crisis response teams including Army explosive ordnance disposal and other government agencies in support of Homeland Defense.

k. Provide direct support to FMS case management requiring PPSS services such as software development, threat

analysis, equipment, and training support to meet U.S. Army Security Assistance Command requirements that include installation and test as well as RSR designs that provide for Joint and allied interoperability.

l. Ensure development of MES products for example, computer-based training, system software support and maintenance, pattern developments, threat verification and validation, and future cyber products, as needed.

2–11. Commanding General, U.S. Forces Command

The CG, FORSCOM will—

a. Prepare, inspect, and ensure assigned forces are maintained at the highest possible readiness level to conduct EW operations, receive, and process EW mission software products for all reprogrammable equipment.

b. Establish and execute a CEMA readiness evaluation strategy similar to current aviation resource management survey for both air and ground Army organizations.

c. Establish and maintain in coordination with ARAT–PO a RSR support and assistance program to familiarize and assist unit missions and deployments.

d. Coordinate with U.S. Army Test and Evaluation Command (ATEC) to provide for required conduct and programming of operational (troop) tests of EW systems and software.

e. Ensure those forces postured in Tier 1 readiness have current EW mission software products to support required deployments and are exercised in their use.

2–12. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

a. Develop tactics, techniques, and procedures (TTP) in support of Army EW software reprogramming by theater, operational area, or mission and provide guidance for the planning, execution, and evaluation of RSR activities in operations and training.

b. Identify gaps affecting EW PPSS across the doctrine, organization, training, materiel, leadership, and education, personnel, and facilities and provide potential solutions to the deficiencies determined during capabilities based analysis process.

c. Ensure that the principles of the RSR process and ARAT–PO processes for download and/or upload of EW systems mission software are included in the instructional POI at Army institutions as appropriate.

d. Ensure TRADOC representation and support of the EW configuration control board for EW RSR.

e. Submit priority intelligence requirements to CG, U.S. Army Intelligence and Security Command using prescribed procedures and methods. Submit requests for materiel support for counter-threat capability development in accordance with AR 381–11.

f. Ensure EMS requirements and impacts for CEMA are considered in capabilities-based assessments.

g. Ensure the representation of EW RSR during the Capabilities Based Analysis Process including the priority requirement for EM threat information.

h. Integrate RSR capabilities into doctrinal and training publications.

i. Coordinate with AMC to provide qualified ARAT–PO instructors on EW RSR procedures and equipment to EWOs and AMSOs at appropriate TRADOC centers of excellence and as required.

j. Coordinate with ARAT–PO for experiments with EW systems and EW RSR at appropriate network integration evaluations.

2–13. Commanders, Army service component commands

The Commanders, ASCCs will—

a. Ensure Army CEMA representatives to the CCMD staff are trained on counter-threat-change capabilities and ARAT–PO infrastructure and activities.

b. Ensure deploying units and crews receive training on the current software and TTP for all EW systems required for military operations.

c. Develop procedures for implementing TRADOC's stated TTP, training, doctrine, and other responses to enemy introduction of new or modified existing threats.

d. Exercise established procedures to exchange data electronically with Joint Services for EW reprogramming, operations, and tactics.

e. Exercise RSR procedures in accordance with respective command authorities.

f. Include RSR objectives in exercises and training events.

g. Ensure that counter-threat-change objectives are planned and coordinated with appropriate Service operations and intelligence organizations.

h. Support Army and Joint Services reprogramming exercises and requirements as directed by DCS, G–3/5/7 or geographical CCMD.

i. The Commander, U.S. Army Special Operations Command will coordinate with ARAT–PO for required RSR support and provide necessary funding for that support.

2–14. Commanding General, U.S. Army Test and Evaluation Command

The CG, ATEC will—

a. Ensure that system evaluation plans incorporate direct and indirect EW roles in the evaluation process.

b. Ensure that event design plans include testing of systems in an environment that represents the hostile EW threat to the extent possible.

c. In conjunction with ARAT-PO, ensure comprehensive threat load testing of EW systems during appropriate system tests and for related EW tests at the network integration evaluations.

2–15. Commanding General, Second Army

The CG, 2nd Army will—

a. In coordination with ARCYBER, develop and test information assurance or as applicable the cybersecurity on Army systems, and recommend to CG, TRADOC, organizational and operational concepts, and doctrine pertaining to the employment of EW to support Army operations in the Army's portion of the DOD information networks. In coordination with ARCYBER, integrate requirements and procedures for countering hostile EW threats in combat developments and training activities. Use AMC-developed system threat assessment report for related EW threats.

b. Coordinate with AMC, CECOM, SEC, and ARAT–PO on the needs for secure distribution of EW and CEMA mission data sets as networks evolve.

c. In coordination with CG, AMC and ARAT–PO, ensure EW RSR messaging is continuously available and with sufficient priority to accomplish directly to forces in the CCMD areas of operation via secret internet protocol router network, and coordinate planned adjustments or revisions to network policy with ARAT–PO to assure continuous support.

d. Assist ARAT–PO in the development of over-the-air delivery of mission software directly to EW systems and hosting auxiliary mission software on the networks for combat requirements, as needed and as networks mature.

2–16. Commanding General, U.S. Army Cyber Command

The CG, ARCYBER will—

a. Coordinate with AMC, CECOM, SEC, and ARAT–PO in all matters of CEMA operations.

b. Provide a representative to the CEMA configuration control board in support of CEMA RSR.

c. Ensure that ARAT–PO has operational priority in the task order waiver approval process.

d. Ensure ARAT–PO infrastructure connectivity in support of Army EW operations.

e. Integrate EW RSR into CEMA at appropriate tactical echelons in coordination with ARAT–PO, the EW TCM, and appropriate commands and staffs.

f. Authorize direct liaison with the cyber Center of Excellence for EW RSR integration and coordination with the EMS and cyber activities and operations, where appropriate.

g. In accordance with the Second Army, assist in the development and implementation of automated dissemination of EW mission software products and the hosting of alternative EW mission software products as the network system evolves with AMC, CECOM, SEC, and ARAT–PO.

2–17. Commanders of Army service component commands serving geographic combatant commands and Joint task forces

The Commanders, ASCCs serving geographic combatant commands and Joint task forces will—

a. Direct the use of friendly wartime reserve mode (WARM) as dictated by the threat environment or as directed by the geographic combatant commander. This authority may not be delegated.

b. Notify EW coordination centers and ARAT–PO when U.S. WARM capabilities must be executed.

c. Consult and exercise established procedures identified in ATP 3–13.10 to exchange data electronically with other Services for EW reprogramming, operations, and tactics.

d. Ensure standing operating procedures for reporting requirements include notification of ARAT–PO when EW mission software products have been uploaded to operational EW systems.

Chapter 3
Counter-Threat-Change Strategic Overview

3–1. New and changed threats

a. Adversaries are expected to employ both high and low technology systems with constantly changing TTPs. EW requires RSR capability to adapt to or forestall these changes.

b. The largest volume of new and changed threats will most likely be employed at the beginning of hostilities. This creates the following problems for Army forces:

(1) Detecting new and existing threats.

(2) Identifying the type of threat.

(3) Validating and verifying the threat change to be creditable.

(4) Determining how to counter the threat changes.

(5) Implementing appropriate friendly force changes to counter the new or changed threat.

3–2. Rapid software reprogramming strategy

The ARAT–PO RSR strategy focuses on the following four functional components to achieve success:

a. Detect the change. Perform continuous analysis of collected intelligence to identify when new threats, or modifications to existing threats, are introduced that may affect EW system performance or TTP.

b. Assess the change. Make use of automated tools and software models to identify or flag when changes may adversely impact EW system performance, either globally or regionally.

c. Develop the response. Use threat parametric, signature, and employment information to rapidly develop, test, and accept a response to the change. Responses may be software updates, hardware modifications, changes in TTP, or a combination of all three.

d. Implement the change. Transmit and implement the change (hardware, software, and TTP) to the system at the operator level. See ATP 3–13.10 for additional information on RSR processes.

3–3. Evolving Army practices

a. Warfare is rapidly moving into a new domain: cyberspace. This will affect warfighting in all domains, and the Army will take measures to adapt to the cyberspace environment. As doctrine and tactics evolve, so will practices for reprogramming EW and CEMA systems to make them more responsive to the Soldier. This increased responsiveness demands shortened timelines to combat enemy threats as they adapt to new technology and to new methods of employment. RSR will be required to become even more adaptive, automated, and integrated with weapons systems operating in the EMS. A vigorous research and development approach to provide timely mission software to the field with on-call data sets hosted on the network are required for use by the EWOs and AMSOs to counter anticipated threats. The intelligence community will be required to provide validated and verified threat information to the ARAT–PO more rapidly than in the past for specific regions of the world. Priorities for software updates will have to be identified by the TCM as early as possible to create and adjust mission data sets for users. The integration and cooperation required will demand attention by the entire CEMA community as part of a combined arms team in support of CEMA operations.

b. New EW and CEMA systems now in development will require continuous attention to detail and involvement of every command in the acquisition of new systems in an era of scarce resources to achieve the efficiencies required. Upfront involvement of sustainers in the early phases of the development cycle and acquisition decisionmaking will be of critical importance to achieve required goals in this environment.

c. Those EW and CEMA systems supported by RSR must be maintained whether they are in operational use or in depot storage. Current mission software products are readily accessible through ARAT–PO accounts on the secure internet protocol router network.

d. Under the CEMA tactical organizational construct, there is a CEMA element at all levels (corps through battalion) that serves as the commander's staff group for planning. The CEMA element is led by the unit EWO. The EWO serves as the commander's designated staff officer for the planning, integration, and synchronization of CEMA and uses other elements of the staff to integrate CEMA into the commander's scheme of maneuver in addition to the existing responsibilities for coordinating and implementing ongoing EW activities (see FM 3–38).

3–4. Commander's response to changes in threat-system electromagnetic parameters, procedures and modes of operation

See Chairman Joint Chiefs of Staff Instruction 3210.04A for guidance on this topic.

Appendix A
References

Section I
Required Publications

The following publication is available on the Army Publishing Directorate Web site (http://www.apd.army.mil).

AR 381–11
Intelligence Support to Capability Development (Cited in para 2–12*e*.)

Section II
Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 11–2
Managers' Internal Control Program

AR 25–30
The Army Publishing Program

AR 70–1
Army Acquisition Policy

AR 71–9
Warfighting Capabilities Determination

AR 95–1
Flight Operations

AR 380–5
Department of the Army Information Security Program

AR 525–22
U.S. Army Electronic Warfare

AR 530–1
Operations Security (OPSEC)

AR 750–1
Army Materiel Maintenance Policy

ATP 3–13.10
EW Reprogramming Multi-Service Tactics, Techniques, and Procedures for Reprogramming Electronic Warefare (EW) Systems

CJCSI 3121.01B (S)
Standing Rules of Engagement for U.S. Forces (U) (Available on SIPRNET.)

CJCSI 3210.04A (S)
Joint Electronic Warfare Reprogramming Policy (U) (Available on SIPRNET.)

CJCSI 3320.01D
Electromagnetic Spectrum Use in Joint Military Operations

CJCSM 3212.02D
Performing Electronic Attack in the United States and Canada for Testing, Training, and Exercises

CJCSM 3212.03
Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada

CJCSM 3320.01D
Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment

CJCSM 3320.02D
Joint Spectrum Interference Resolution (JSIR) Procedures

CJCSM 3320.04
Electromagnetic Warfare in Support of Joint Electromagnetic Spectrum Operations

DODD 3222.04
Electronic Warfare (EW) Policy (Available at http://www.dtic.mil/whs/directives.)

DODD 5250.01
Management of Signature Support within the Department of Defense (Available at http://www.dtic.mil/whs/directives.)

FM 3–38
Cyber Electromagnetic Activities

NDP–1
National Disclosure Policy (NDP–1, 1 Oct 1988) (Available at http://www.dtic.mil/whs/directives/corres/pdf/523011p.pdf.)

10 USC 2460
Definition of depot-level maintenance and repair (Available at https://www.law.cornell.edu/uscode/text.)

50 USC
War and National Defense (Available at https://www.law.cornell.edu/uscode/text.)

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
DA Forms are available on the Army Publishing Directorate Web site (http://www.apd.army.mil).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B
Internal Control Evaluation

B–1. Function
The function covered by this evaluation is Software Reprogramming for EW Systems.

B–2. Purpose
The purpose of this evaluation is to assist the organizations designated in chapter 2 in evaluating the key internal controls listed. It is not intended to cover all controls.

B–3. Instructions
Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, simulation, and so forth). Answers that indicate deficiencies must be explained and the

corrective action identified in the supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions

a. Are sensor-based weapons and EW systems developed using reprogrammable software? (ASA (ALT) only)

b. Are policies and procedures in place to enable RSR across the Army, Services, Joint community, and allies, as necessary? (All-ASCCs address inside their command only.)

B–5. Supersession

Not applicable.

B–6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to Deputy Chief of Staff, G–3/5/7 (DAMO–ODE), Washington, DC 20310–3200

Glossary

Section I
Abbreviations

AMC
U.S. Army Materiel Command

AMSO
Aviation Mission Survivability Officer

ARAT
Army Reprogramming Analysis Team

ARAT–PO
Army Reprogramming Analysis Team-Program Office

ARCYBER
U.S. Army Cyber Command

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

ASCC
Army service component command

ATEC
U.S. Army Test and Evaluation Command

CAR
Chief, Army Reserve

CCMD
combatant command

CECOM
Communications-Electronic Command

CEMA
cyber electromagnetic activities

CG
Commanding General

CIO/G–6
Chief Information Officer/G–6

CNGB
Chief National Guard Bureau

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DCS, G–4
Deputy Chief of Staff, G–4

DCS, G–8
Deputy Chief of Staff, G–8

EA
electronic attack

EMS
electromagnetic spectrum

EP
electronic protection

ES
electronic warfare support

EW
electronic warfare

EWO
electronic warfare officer

FORSCOM
U.S. Army Forces Command

INSCOM
U.S. Army Security and Intelligence Command

MES
Mission Enabling Software

MSP
mission software program (or product)

NDP–1
National Disclosure Policy–1

PEO
program executive officer

PM
program manager

PPSS
post-production software support

RSR
rapid software reprogramming

SEC
Software Engineering Center

TCM
TRADOC Capabilities Manager

TRADOC
U.S. Army Training and Doctrine Command

TTP
tactics, techniques, and procedures

WARM
wartime reserve mode

Section II
Terms

Cyber electromagnetic activities
Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the EMS, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.

Electromagnetic spectrum
The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands.

Electronic attack
Division of EW involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.

Electronic protection
Division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability.

Electronic warfare
EW is military action involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy. EW consists of three divisions: EA, EP, and ES.

Electronic warfare support
Division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.

Electronic warfare mission software
EW mission software is the element contained in an equipment software operating program to enable the detection of hostile threats while performing EA, EP, and electronic support functions. Specifically, EW mission software may contain a data library and operational profile of threat system operations. For example, the threat load set in an EW radio-controlled improvised explosive devices protection system will contain regional or area of operations specific threat parametric data in the library and platform operational ground profile characteristics of the system such as speed of travel, and on-board communications.

Mission Enabling Software
MES encompasses all other ARAT–PO products, for example, computer based training, system software support and maintenance, pattern developments, CEMA threat verification and validation, and future cyber products.

Mission software product
MSP include aviation survivability equipment software, mission data sets, and ground-based counter improvised explosive device software, known as threat load sets, and nonmission software products such as the ARAT survivability software loader development and distribution.

Operational flight program
The software program of an embedded computer system (that is, the Electronic Control Unit of the Common Missile Warning System) which enables that system to perform its interactive tasks as designed.

Operations security
A process of analyzing friendly action attendant to military operations and other activities to (1) Identify those actions that can be observed by adversary intelligence systems; (2) Determine indicators hostile intelligence systems might obtain that could be intercepted and pieced together to derive critical information in time to be useful to adversaries;(3) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to the adversary exploitation.

Rapid software reprogramming
Rapid software reprogramming is the deliberate alteration or modification of EW systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. These

changes may be the result of deliberate actions on part of friendly, adversary or third parties; or may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW system equipment. EW reprogramming includes changes to self-defense systems, offensive weapon systems, and intelligence collection systems.

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

Section III
Special Abbreviations and Terms
This section contains no entries.