FM 3-12

CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS



SEPTEMBER 2025

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes FM 3-12, dated 24 August 2021.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Foreword

Over the past several years, the global security environment has changed in ways once considered unthinkable in the post-Cold War world order. Where the Department of Defense once believed the future of warfare was antiterrorism and limited contingency operations, it is now clear that the prospect of large-scale combat against a regional peer is much more likely than once believed. In recent years, Russia has engaged in the largest land war in Europe of the past 80 years. China, with an economy nearly equal in size to ours, is fostering new international partnerships through its Belt and Road Initiative and building a world-class military to challenge the United States, its allies, and neighbors in the Pacific Rim, including in Taiwan. China and Russia, along with other regional peers, have heavily invested in and demonstrated formidable capabilities to challenge U.S. dominance in multiple domains, including cyberspace and the electromagnetic spectrum.

The Army's operating concept of multidomain operations anticipates the return of great power competition and large-scale combat operations and stresses the need to integrate and converge warfighting capabilities in all domains to achieve and press positions of relative advantage. At the same time, the Army's newest doctrine for information presents a new paradigm for how the Army views information in a military context. Data and information are central to command and control, for our adversaries as much as for ourselves. Advances in sensors, networking technologies, and global connectivity provide commanders an unprecedented amount of data and information to support informed decision making. These capabilities are almost wholly dependent on cyberspace and the electromagnetic spectrum. Peer threats continually attempt to infiltrate, exploit, and degrade access to and ability to use our networks and data. It is therefore vital that the Army not only protect its own information and cyberspace capabilities, but also deny our adversaries the use of similar capabilities.

Creating effects in cyberspace and the electromagnetic spectrum across the competition continuum is key to achieving relative advantages. To maximize these advantages, commanders must integrate and synchronize cyberspace operations and electromagnetic warfare with all other available military capabilities through a combined arms approach.

Competent leadership, informed by sound doctrine, is critical as the Army prepares for the complexities of modern warfare. We must actively assess and refine our approach to cyberspace operations and electromagnetic warfare through continuous learning, guided by lessons learned from the operational force. By embracing doctrinal principles and integrating military capabilities across all domains, we will enhance our ability to achieve relative advantages and ensure the Army remains ready to fight and win.

Forge and project power!



RYAN M. JANOVIC
MAJOR GENERAL, UNITED STATES ARMY
COMMANDING

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil) and the Central Army Registry Site (https://atiam.train.army.mil/catalog/dashboard).

Field Manual
No. 3-12

Headquarters
Department of the Army
Washington, DC, 17 September 2025

CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS

Contents

Page

Preface v
Introduction vii
CHAPTER 1 1
OVERVIEW AND THREAT 1
Section I – Context for Cyberspace and Electromagnetic Warfare Operations 1
Multidomain Operations 1
Challenges for Army Forces 5
Understanding an Operational Environment 10
The Cyberspace Domain 11
The Electromagnetic Spectrum 12
Section II – Threats and Hazards 13
Overview 13
Threat Activities in Cyberspace and the Electromagnetic Spectrum 14
State Threats 16
Peer Threat 16
Peer Threat Tactics 19
Hybrid Threat 20
Threat Information Warfare 20
Non-State Threats 21
Insider Threat 22
Hazards 22
Section III – Systems Analysis 25
Overview 25
Analysis Process 26
Output 27
CHAPTER 2 29

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes FM 3-12, dated 24 August 2021.

CYBERSPACE OPERATIONS 29
Joint and Army Networks 29
Cyberspace Defense 30
Cyberspace Offense 32
CHAPTER 3 35
ELECTROMAGNETIC WARFARE 35
Introduction 35
Electromagnetic Attack 35
Electromagnetic Protection 39
Electromagnetic Support 43
Electromagnetic Warfare Reprogramming 44
Synchronization with Signals Intelligence 45
Electromagnetic Warfare Forces at Echelons Division and Below 47
CHAPTER 4 49
CYBERSPACE ELECTROMAGNETIC ACTIVITIES 49
Overview 49
Cyberspace Electromagnetic Activities Roles by Echelon 49
Cyberspace Electromagnetic Activities in the Operations Process 52
Cyberspace Electromagnetic Activities in the Integrating Processes 60
Integration With the Joint Force 67
CHAPTER 5 73
CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS IN COMBINED ARMS 73
Section I – Convergence and Integration with the Joint Force 73
Converging Effects Across Domains 73
Supporting Joint Command and Control 74
Enabling Operations 74
Section II – Cyberspace and Electromagnetic Warfare Operations Across the Competition Continuum 76
Relative Weighting of Effort 76
Competition 77
Crisis 82
Armed Conflict 88
APPENDIX A 97
CYBER INCIDENT RESPONSE 97
APPENDIX B 111
CYBERSPACE ELECTROMAGNETIC ACTIVITIES PLANNING AND INTEGRATION 111
APPENDIX C 139
EFFECTS REQUESTS 139

APPENDIX D **149**
RECOGNIZING AND RESPONDING TO ELECTROMAGNETIC ATTACKS AND MALICIOUS CYBERSPACE ACTIVITY **149**
APPENDIX E **163**
MESSAGE FORMATS **163**
APPENDIX F **175**
ECHELONS ABOVE CORPS CYBER AND ELECTROMAGNETIC WARFARE ORGANIZATIONS **175**
APPENDIX G **183**
TRAINING **183**
APPENDIX H **187**
NETWORK HARDENING GUIDE **187**
APPENDIX I **203**
ARMY INTEGRATED REPROGRAMMING CYCLE **203**
Glossary **207**
References **215**
Index **219**

Figures

Figure 1-1. Domains and dimensions of an operational environment 10
Figure 1-2. Competition for available electromagnetic spectrum resources 13
Figure 1-3. Output of mission analysis 28
Figure 3-1. Synchronization of electromagnetic warfare with signals intelligence 47
Figure 3-2. Division electromagnetic warfare company 48
Figure 3-3. Brigade combat team electromagnetic warfare platoon 48
Figure 4-1. Tactical electromagnetic support reporting 50
Figure 4-2. Joint electromagnetic spectrum operations actions 68
Figure 4-3. Integration of Army targeting with the joint targeting cycle 71
Figure 5-1. Cyberspace and electromagnetic warfare across the competition continuum 77
Figure A-1. Cyber incident analysis 98
Figure A-2. Cyber incident response life cycle 98
Figure B-1. Example cyberspace and electromagnetic warfare running estimate 112
Figure B-2. Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of an operation plan or order 128
Figure C-1. Example joint tactical airstrike request 141
Figure C-2. Example electromagnetic attack request format 142
Figure C-3. Example electromagnetic attack brief 143
Figure C-4. Routing chain for offensive cyberspace operations support requests 144
Figure C-5. Routing chain for defensive cyberspace operations support requests 146
Figure E-1. Stop jamming message format 163
Figure E-2. Electromagnetic warfare frequency deconfliction message 164
Figure E-3. Electromagnetic warfare mission summary 165
Figure E-4. Electromagnetic warfare requesting/tasking message 166
Figure E-5. Meaconing, intrusion, jamming, and interference feeder report format 168

Figure E-6. Threat information message format 169
Figure E-7. Operational change request message format 170
Figure E-8. System impact message format 171
Figure E-9. Reprogramming impact message format 172
Figure E-10. Unit loading message format 173
Figure E-11. Army Reprogramming Analysis Team information message format 174
Figure I-1. Army integrated reprogramming cycle 203

Tables

Introductory table. Modified terms ix
Table 3-1. Emission control conditions 41
Table 3-2. Service and interagency electromagnetic warfare reprogramming roles 45
Table 4-1. Example emitter criteria table. 56
Table 4-2. Sample cyberspace electromagnetic working group activities 57
Table A-1. Cyber incident categories 105
Table A-2. Initial impact assessment table 106
Table A-3. Cyber incident severity schema crosswalk 107
Table B-1. Military decision-making process step 1—receipt of mission 115
Table B-2. Military decision-making process step 2—mission analysis 118
Table B-3. Military decision-making process step 3—course of action development 121
Table B-4. Military decision-making process step 4—course of action analysis and war-gaming 123
Table B-5. military decision-making process step 5—course of action comparison 124
Table B-6. Military decision-making process step 6—course of action approval 125
Table B-7. Military decision-making process step 7—orders production, dissemination, and transition 126
Table B-8. Sample information collection working group activities 133
Table B-9. Sample targeting working group activities at division or corps 135
Table B-10. Sample protection working group activities 137
Table C-1. Example airborne electromagnetic attack or electromagnetic support request tool 140
Table D-1. Common jamming signals 152
Table F-1. Elements of the Cyber Mission Force and their associated teams 179

Preface

FM 3-12 nests with and supports joint doctrine for cyberspace operations and joint electromagnetic spectrum operations and with higher-level Army doctrine. To understand and apply the doctrine in this publication, readers should be familiar with Army operations doctrine found in ADP 3-0 and FM 3-0. They should also be familiar with the information advantage framework outlined in ADP 3-13.

The principal audience for FM 3-12 is commanders and staffs at echelons theater army and below. The secondary audience is cyber and electromagnetic warfare professionals. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the competition continuum and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States, international, and in some cases host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of armed conflict and the rules of engagement. (See FM 6-27.) They also adhere to the Army ethic as described in ADP 6-22.

FM 3-12 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which FM 3-12 is the proponent publication (the authority) are italicized in the text and are marked with an asterisk (*) in the glossary. When first defined in the text, terms for which FM 3-12 is the proponent publication are boldfaced and italicized, and definitions are boldfaced. When first defining other proponent definitions in the text, the term is italicized and the number of the proponent publication follows the definition. Subsequent uses of the term are not italicized.

This publication applies to the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

The proponent for this publication is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Branch, United States Army Cyber Center of Excellence. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-OPD (FM 3-12), 419 B Street, Fort Gordon, GA 30905-5735, or e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@army.mil.

This page intentionally left blank.

Introduction

FM 3-12 provides Army doctrine for cyberspace operations, electromagnetic warfare, and cyberspace electromagnetic activities as part of a combined arms approach to achieve objectives across the competition continuum. FM 3-12 provides commanders and staffs an understanding of Army cyberspace operations, electromagnetic warfare, cyberspace electromagnetic activities, staff roles and responsibilities, and those echelons above corps organizations that support cyberspace and electromagnetic warfare operations.

FM 3-12 describes how personnel who conduct cyberspace electromagnetic activities plan, integrate, and synchronize cyberspace and electromagnetic warfare operations and how cyberspace electromagnetic activities sections integrate with other staff sections through various integrating processes and working groups throughout the operations process.

FM 3-12 contains five chapters and nine appendixes:

- **Chapter 1 – Overview and Threat**—begins with an overview of the context for cyberspace and electromagnetic warfare as part of a combined arms approach. It goes on to discuss threats and vulnerabilities. The chapter concludes with a discussion of systems analysis to support targeting and protection planning.
- **Chapter 2 – Cyberspace Operations**—describes how different portions of cyberspace may be controlled and operated by different entities, with users relying on systems they neither control nor operate. It goes on to discuss how Army forces protect against threat use of cyberspace and preserve friendly ability to use it. The chapter concludes with an explanation of the conduct of operations against threats in and through cyberspace as well as in the air and land domains based on their reliance upon cyberspace.
- **Chapter 3 – Electromagnetic Warfare**—introduces electromagnetic warfare and the divisions of electromagnetic warfare consistent with joint doctrine. It goes on to discuss the application of electromagnetic attack, electromagnetic protection, electromagnetic support, and electromagnetic warfare reprogramming in Army operations. The chapter then addresses the synchronization of electromagnetic warfare with complementary signals intelligence capabilities. The chapter concludes with a description of organic electromagnetic warfare forces at echelons corps and below.
- **Chapter 4 – Cyberspace Electromagnetic Activities**—describes the integration and synchronization of cyberspace and electromagnetic warfare operations into combined arms through the operations process—planning, preparation, execution, and assessment, the role of the cyberspace electromagnetic activities section in targeting. The chapter concludes with a discussion of integration with the joint force.
- **Chapter 5 – Cyberspace and Electromagnetic Warfare Operations in Combined Arms**—addresses the contributions of cyberspace and electromagnetic warfare operations in a combined arms approach. The chapter begins with a discussion of targeting, convergence, and integration with the joint force. It then discusses the contributions of cyberspace and electromagnetic warfare operations across the competition continuum.
- **Appendix A – Cyber Incident Response**—describes the types and severity of cyber incidents and the reporting processes and procedures for reporting cyber incidents to higher echelons and joint force authorities.
- **Appendix B – Cyberspace Electromagnetic Activities Planning and Integration**—discusses the cyberspace electromagnetic activities section's role in the military decision-making process and integrating processes.
- **Appendix C – Effects Requests**—introduces the forms and instructions for the cyber effects request format, the electromagnetic attack request format, and the joint tactical airstrike request.
- **Appendix D – Recognizing and Responding to Electromagnetic Attacks and Malicious Cyberspace Activity**—addresses the means to recognize and overcome threat malicious cyberspace activities and electromagnetic attacks in a contested environment. It includes an overview of peer

threat tactics, techniques, and procedures and methods to prevent, recognize, and counter threat electromagnetic attacks and malicious cyberspace activity.

- **Appendix E – Message Formats**—provides the formats and instructions for the various electromagnetic warfare messages.
- **Appendix F – Echelons Above Corps Cyber and Electromagnetic Warfare Organizations**—discusses the national, Department of Defense, and Reserve Components organizations that conduct or support cyberspace and electromagnetic warfare operations. This appendix also provides an overview of the United States Cyber Command and its subordinate joint organizations that deliver cyberspace operations and electromagnetic warfare support to Army commanders using cyber mission forces.
- **Appendix G – Training**—discusses training to prepare Soldiers to execute missions to shape operational environments, prevent conflict, and support large-scale combat operations against peer threats. This discussion includes institutional training, home-station training, combat training center rotations, and deployments.
- **Appendix H – Network Hardening Guide**—This guide should provide units a risk-based assessment of their network security posture and ultimately a more secure network. The network hardening guide organizes local network hardening procedures around four distinct but interrelated areas:
  - Domain management and security.
  - Network device management and security.
  - Network traffic monitoring and alerts.
  - Endpoint (host and server) security.
- **Appendix I – Army Integrated Reprogramming Cycle**—defines the future state Army reprogramming enterprise.

SUMMARY OF CHANGES

This is a major revision of FM 3-12. Significant changes in this revision include—

- **Operational focus**—this revision of FM 3-12 focuses on the application of available military capabilities at echelons theater army and below as part of a combined arms approach to create effects in cyberspace and the electromagnetic spectrum.
- **Information advantage**—describes how the employment of cyberspace operations and electromagnetic warfare contributes to relative information advantages as outlined in ADP 3-13.
- **Threat**—introduces the categories of threat—enemy, adversary, and insider threat—and their significance in cyberspace and the electromagnetic spectrum. Details cyberspace- and electromagnetic spectrum-relevant aspects of the most challenging state threats.
- **Hazards**—describes natural and manmade hazards that affect operations in the electromagnetic spectrum.
- **Systems analysis**—introduces the analysis of mission threads (systems of systems) to identify dependencies and vulnerabilities to support either targeting (threat systems) or mission thread defense (friendly systems).
- **Cyberspace electromagnetic activities**—FM 3-12 becomes the proponent for and modifies the term cyberspace electromagnetic activities. Details the cyberspace electromagnetic activities section's role in the military decision-making process, integrating processes, and working groups. Describes how cyberspace electromagnetic activities support the joint task force's cyberspace operations, joint electromagnetic spectrum operations, and joint targeting.
- **Synchronization with signals intelligence**—discusses the synchronization of electromagnetic support with signals intelligence to maximize their complementary capabilities.
- **Targeting**—describes the cyber electromagnetic warfare officer's participation in the targeting working group and targeting coordination board to identify and nominate targets in cyberspace and the electromagnetic spectrum and match the targets with available military capabilities to create desired effects in cyberspace and the electromagnetic spectrum.
- **Cyberspace and electromagnetic warfare across the competition continuum**—describes how commanders can leverage cyberspace and electromagnetic warfare capabilities with other available

military capabilities as part of a combined arms approach in competition below armed conflict, in crisis, and during armed conflict.

- **Cyber incident response**—outlines the procedures to recognize and respond to cyber incidents, restore network capabilities, and report incidents through command channels (see appendix A).
- **Effects requests**—describes how Army units at echelons theater army and below request cyberspace operations and electromagnetic warfare support from joint, theater-level, and national capabilities (see appendix C).
- **Electromagnetic warfare reprogramming**—implements electromagnetic warfare reprogramming messages (see appendix E) and discusses the Army integrated reprogramming cycle and future reprogramming enterprise (see appendix I).
- **Cyberspace operations and electromagnetic warfare training**—describes institutional and home-station training for cyber and electromagnetic warfare personnel; training exercises; and combat training center rotations.
- **Network hardening guide**—describes how cybersecurity personnel and local network defenders can strengthen the baseline security of the network against known threat tactics, techniques, and procedures (see appendix H).

The introductory table outlines changes to Army terminology promulgated in FM 3-12.

Introductory table. Modified terms

Term	*Action*
cyberspace electromagnetic activities	FM 3-12 becomes the proponent and modifies term

This page intentionally left blank.

Chapter 1
Overview and Threat

This chapter begins with an overview of the context for cyberspace and electromagnetic warfare operations as part of combined arms. It goes on to discuss operational environments, threats, and hazards. The chapter concludes with a discussion of systems analysis to support targeting and protection planning.

SECTION I – CONTEXT FOR CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS

1-1. The Army's primary responsibility is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. While operations in cyberspace or the electromagnetic spectrum might dominate military considerations in a specific, narrow context, conflicts are ultimately resolved on land because that is where people live and make political decisions and where the basis of national power exists.

1-2. Army forces achieve objectives through the conduct of operations. Operations change factors in the physical, information, and human dimensions of an operational environment. It is important to understand that cyberspace operations and electromagnetic warfare (EW) operations exist primarily in the larger context of combined arms operations.

1-3. Most Army operations occur either below the threshold of armed conflict or during limited contingencies. Cyberspace and EW operations play valuable roles in shaping operational environments to U.S. forces' advantage across the competition continuum. In addition, a wide range of state and non-state threats continually engage U.S. cyberspace networks during competition below armed conflict to collect information about friendly forces, steal or modify data, assess vulnerabilities, or plant malicious software in U.S. systems.

1-4. The United States always retains the option to employ greater levels of force when less coercive methods are ineffective, and when vital interests or national survival are at stake. This requires Army forces to be prepared for the most demanding and dangerous types of operations. Offensive and defensive cyberspace and EW capabilities are parts of the Army's combined arms approach to operations, both to protect itself and to create converged effects in multiple domains during large-scale combat operations.

MULTIDOMAIN OPERATIONS

1-5. All Army operations are multidomain operations. *Multidomain operations* are the combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders (FM 3-0). Multidomain operations are the Army's contribution to joint operations, which span the competition continuum. Army forces use all available combat power in each domain to accomplish missions at least cost. Cyberspace and EW operations contribute to operations by affecting conditions in an assigned area to create temporary windows of relative advantage in the air, land, maritime, space, and cyberspace domains and the electromagnetic spectrum. Refer to FM 3-0 for more information about multidomain operations.

COMBINED ARMS

1-6. Cyberspace and EW operations are key contributors to a combined arms approach. *Combined arms* is the synchronized and simultaneous application of arms to achieve an effect greater than if each element was used separately or sequentially (ADP 3-0). Leaders apply all relevant military capabilities—including cyberspace and EW capabilities—in complementary and reinforcing ways to amplify their effects. The combined arms approach to operations during competition, crisis, and armed conflict is foundational to exploiting capabilities across all domains.

1-7. Army operations take place as part of a larger joint or multinational effort. Commanders must understand not only their assigned forces and capabilities, but how they can leverage the forces or capabilities provided by higher echelon Army, joint, and multinational partners. As part of a combined arms approach, commanders integrate and employ organic capabilities with capabilities provided by higher headquarters to achieve objectives. Some multinational partners may offer greater capabilities to support a particular mission or operate under less restrictive rules of engagement. Integration of joint and multinational cyberspace and EW capabilities into operations increases the commander's ability to converge effects in multiple domains to achieve objectives.

1-8. Army forces also benefit from air, maritime, space, and cyberspace capabilities they do not control. Examples of this support include—

- Satellite-based positioning, navigation, and timing.
- Satellite communications.
- Intelligence, surveillance, and reconnaissance.
- Close air support.
- Over-the-shore logistics.
- Other Services' support.
- Multinational partners' support.
- Effects from joint offensive cyberspace operations.

1-9. Many supporting joint and multinational capabilities are integrated at the corps or field army to shape conditions in the deep area, though they may provide reinforcing support in the close area. Lower echelons may not always realize the opportunities created by higher echelons or other forces operating in other domains, but leaders should understand that the absence of those supporting capabilities affects their concepts of operations, decision making, and operational risk. Refer to FM 3-0 for more information about combined arms and FM 3-16 for more information about the Army in multinational operations.

Relative Advantages

1-10. A position of relative advantage is a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage. Relative advantages are characterized as human, information, or physical, and they complement each other. During operations, small advantages can have significant impacts on the outcome of the mission, particularly when they accrue over time. Creating and exploiting relative advantages are therefore necessary for all operations, and they become even more critical when opposing sides are evenly matched. The ability to plan, integrate, and synchronize space, cyberspace, and EW capabilities into combined arms at the most effective echelon expands options for creating relative advantages to exploit. Most maneuver commanders are skilled at creating positions of relative advantage using available combined arms capabilities. Commanders must integrate organic and supporting cyberspace and EW capabilities into their combined arms approach to protect friendly capabilities and affect threat sensing, decision making, and information warfare capabilities. Refer to FM 3-0 for more information about relative advantages.

Information Advantage

1-11. In addition to creating physical and human advantages, cyberspace and EW capabilities are key contributors to creating and exploiting information advantages. *Information advantage* is a condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior (ADP 3-13). While friendly forces seek information advantages, threat forces are doing the same. As such, an information advantage is something to gain, protect, and exploit across as many domains as possible. Commanders can achieve a relative advantage by making better and faster decisions than the enemy. Cyberspace and EW operations can protect and speed friendly decisions and degrade or slow enemy decisions to contribute to information advantage.

1-12. Army forces integrate all relevant military capabilities, including cyberspace and EW operations, through the planning and execution of information activities. An *information activity* is a collection of tasks linked by purpose to affect how humans and automated systems derive meaning from, use, and act upon, or are influenced by, information (ADP 3-13). Each information activity incorporates several tasks and subtasks

from the warfighting functions to achieve a variety of friendly and threat-based objectives. The information activities are—

- Enable.
- Protect.
- Inform.
- Influence.
- Attack.

1-13. Friendly actions in cyberspace and the electromagnetic spectrum may contribute to information advantage by—

- Enabling friendly decision making.
- Protecting friendly information.
- Defending networks and command and control information systems.
- Informing friendly audiences.
- Influencing threat and neutral actors.
- Attacking enemy command and control or information warfare capabilities.

Enable

1-14. The enable information activity includes tasks that enhance friendly command and control. The focus of this activity is to improve situational understanding, decision making, and communications. Cyberspace operations and electromagnetic support, augmented with intelligence support, contribute to a holistic understanding of an operational environment, including friendly, threat, and neutral use of cyberspace and the electromagnetic spectrum. Up-to-date situational understanding enables commanders' decision making and assists in targeting.

Electromagnetic Support

1-15. Electromagnetic support provides the ability to—

- See and understand friendly use of, and appearance within, the electromagnetic spectrum and identify friendly vulnerabilities in the electromagnetic spectrum.
- See and understand the threat's use of the electromagnetic spectrum and identify threat weaknesses to exploit through attack activities.
- Support rapid decision making and dynamic targeting by locating and characterizing threat emitters.

Electromagnetic Protection

1-16. Electromagnetic protection provides capabilities to—

- Ensure spectrum-dependent devices can operate effectively despite threat or environmental interference.
- Protect friendly electromagnetic emissions from threat interception, direction finding, or exploitation.

Cyberspace-Enabled Activities

1-17. Cyberspace-enabled activities support the ability to—

- Create conditions of shared situational understanding.
- Coordinate across echelons.
- Link sensors with decision makers and decision makers with lethal and nonlethal attack assets.

Intelligence Support

1-18. Units at echelons corps and below may have limited ability to gain situational understanding of threat and neutral use of cyberspace. Units may require augmentation from theater- or national-level intelligence elements to develop this understanding. Signals intelligence (SIGINT) elements can perform many of the same functions as electromagnetic support to improve commanders' understanding of friendly, neutral, and

threat use of the electromagnetic spectrum. SIGINT functions differ from EW beyond initial signals collection and geolocation.

Protect

1-19. In the cyberspace domain, the protect information activity includes tasks that secure friendly data, information, and networks. This activity focuses on denying threat access to friendly data and information while preserving friendly communications capabilities. Preventing threat access to friendly data and information not only protects the friendly force but hinders the threat's ability to accurately understand situations and make effective decisions. Information protection contributes to broader protection activities.

Defensive Cyberspace Operations and Cybersecurity

1-20. Defensive cyberspace operations and cybersecurity combine active and passive measures to secure friendly information resident on or transiting communications and information technology systems. See paragraph 2-8 for more information about defensive cyberspace operations. Refer to ATP 6-02.71 for more information about cybersecurity.

Electromagnetic Protection

1-21. Electromagnetic protection actions—including emission control (EMCON)—secure friendly information against threat intercept and analysis. Electromagnetic protection enables information protection and force protection by minimizing unnecessary electromagnetic energy to avoid threat detection and geolocation. Encryption, both communications security and transmission security, prevent threat forces from exploiting detected communications signals. For transmissions in the clear, the use of brevity codes according to signal operating instructions may provide short-term protection against exploitation. Electromagnetic protection activities include implementing techniques for—

- Low probability of intercept.
- Low probability of detection.
- Low probability of exploitation.
- Low probability of positioning.

1-22. Refer to ATP 3-12.3 for more information about electromagnetic protection. Refer to ATP 6-02.75 for more information about communications security and transmission security. Refer to ATP 1-02.1 for more information about brevity codes.

Inform

1-23. The inform information activity includes tasks that explain relevant military operations and activities to various audiences. The focus of this activity is to maintain the trust and confidence of internal audiences (Soldiers, Department of the Army Civilians, contractors, and family members) and external audiences (domestic and international audiences). Cyberspace and EW operations' primary contribution to the inform activity results from enabling and protecting the friendly network used to inform internal audiences.

Influence

1-24. The influence information activity includes tasks that affect the thinking and ultimately the behavior of threats and other foreign audiences. This activity focuses on reinforcing or changing how individuals and groups think, feel, and act in support of objectives. Actions in cyberspace can influence foreign audiences by delivering real or perceived impacts to the threat military or civilian population. Army forces deliberately plan actions and supporting messages to affect threat perceptions and behavior. As part of operations, commanders direct or coordinate for military deception, military information support operations, civil affairs operations, and Soldier and leader engagements to influence foreign relevant actors. EW elements can conduct electromagnetic deception to deceive threat commanders regarding friendly positions, disposition, and activities and cloud threat decision making. Refer to ATP 3-12.3 for more information about electromagnetic deception.

Attack

1-25. The attack information activity includes tasks that affect the threat's ability to exercise command and control. The focus of this activity is to affect the threat's physical capabilities used to communicate and conduct information warfare. Threat command posts, communications nodes, networks, information systems, and sensors—surveillance, target acquisition, and radar—are often high-payoff targets for Army forces. As part of the scheme of fires, Army forces attack these targets using all available fires, including lethal fires, electromagnetic attack, and offensive cyberspace operations to destroy or degrade the threat's command and control and information warfare capabilities. U.S. forces may also use offensive cyberspace capabilities to attack the threat data and information used to support decision making.

Degrade Threat Command and Control

1-26. Army forces can degrade threat command and control capabilities through movement and maneuver or lethal and nonlethal attack. Faced with degraded command and control capabilities, threat commanders will have difficulty synchronizing maneuver and lethal and nonlethal fires against friendly forces. Nonlethal capabilities used to attack threat command and control include electromagnetic attacks and cyberspace attacks. Electromagnetic support activities help identify and locate threat command and control nodes. The cyber electromagnetic warfare officer (CEWO) participates in the targeting working group and the targeting coordination board to nominate targets and pair the targets with the appropriate attack or delivery system. Refer to ATP 3-12.3 for more information about electromagnetic support techniques. See chapter 4 for more information about the CEWO's role in targeting.

Affect Threat Information Warfare Capabilities

1-27. Threat information warfare capabilities disrupt friendly networks, use of the electromagnetic spectrum, and use of information. Threat information warfare also includes deception and perception management. Many threat information warfare capabilities rely on cyberspace and the electromagnetic spectrum. While the purpose of attacking threat information warfare capabilities differs from attacking threat command and control, the means of targeting and attack are largely the same. Disrupting, degrading, or denying threat information warfare makes it difficult for threat commanders to conduct integrated malicious cyberspace activities, electromagnetic attack, and influence operations against friendly forces. See paragraph 1-125 for more information about threat information warfare.

CHALLENGES FOR ARMY FORCES

1-28. Trained and ready Army forces support joint force commanders in three strategic contexts—competition below armed conflict, crisis, and armed conflict. Within these contexts, Army forces shape operational environments, counter aggression on land during crisis, prevail during large-scale ground combat, and consolidate gains.

COMPETITION BELOW ARMED CONFLICT

1-29. During competition below armed conflict, adversaries may pursue political and military objectives through malign activities calculated to fall below the threshold which would trigger an armed U.S. response. These adversaries may conduct cyberspace surveillance and reconnaissance to collect intelligence and malicious cyberspace activity to disrupt U.S. command and control capabilities or critical infrastructure, or to corrupt data storage or weapon system software. Some adversaries have the ability and the will to conduct damaging malicious cyberspace activity against critical infrastructure and the economy in the homeland to extend the battlefield globally and prevent or disrupt deployment of U.S. forces from home station into an overseas theater. During competition, adversaries will likely employ cyberspace and EW capabilities covertly with limited attribution to remain below the level that might justify an armed response.

Note. The DOD cyberspace operations mission labels of Department of Defense information network operations (DODIN operations), defensive cyberspace operations and offensive cyberspace operations are based on commanders' objectives and intent. Because threat commanders' objectives and intent cannot be known with certainty, 'malicious cyberspace activity' generally describes all threat activities in cyberspace.

CRISIS

1-30. During a crisis, adversaries are not yet using lethal force as the primary means for achieving their objectives, but the situation may require a rapid response by forces prepared to fight to deter further aggression. When directed, the Army provides a joint force commander with forces to help deter further provocation and build sufficient combat power to maintain or reestablish conventional deterrence. Adversaries may attempt to conceal attribution for malicious cyberspace and EW activities to avoid provoking a military response. Under some conditions, adversaries may conduct some of these activities overtly to signal their resolve and discourage U.S. and allied forces while remaining below the level of armed conflict. Adversaries will likely use malicious cyberspace activities and electromagnetic attacks against friendly forces and critical civilian infrastructure to disrupt deployment of forces into theater.

1-31. The introduction of significant land forces demonstrates the will to impose costs, provides options to joint force and national leaders, and signals a high level of national commitment. As a crisis develops, the responsible joint force commander continues to employ capabilities from all Services to gain and maintain information advantages against the threat and set conditions in the operational area for success if the crisis transitions to armed conflict. Adversaries will attempt to penetrate U.S. networks, either to collect intelligence about U.S. capabilities, disposition, and intentions, or to plant malicious code to disrupt the friendly network. Adversaries will use electromagnetic sensing to determine forward deployed friendly forces' locations, strength, and disposition. Adversaries may use electromagnetic jamming to identify friendly tactics, techniques, and procedures to counter jamming effects.

ARMED CONFLICT

1-32. The employment of lethal force is the defining characteristic of armed conflict, and it is the primary function of the Army. Lethality's immediate effect is in the physical dimension—reducing the enemy's capability and capacity to fight. Lethality extends into the information and human dimensions where it influences the enemy's behavior, decision making, and their will to fight. During armed conflict, the enemy will use offensive cyberspace and EW capabilities to attack friendly communications, information, and data to affect friendly situational understanding and ability to exercise command and control. Army forces integrate cyberspace and EW operations into combined arms to—

- Counter the enemy's efforts to affect friendly command and control capabilities.
- Confuse, manipulate, or deceive enemy understanding and decision making.
- Degrade, deny, disrupt, corrupt, or destroy the enemy's command and control systems and their surveillance and reconnaissance capabilities.

PERSISTENT THREAT

1-33. Army forces must understand the persistent nature of threat cyberspace and EW activities as they prepare to conduct operations in competition below armed conflict, including in the United States. Army forces must account for being under constant contact in the cyberspace domain and the electromagnetic spectrum and the threat's ability to gain valuable information about the conditions, disposition, and capabilities of U.S. forces, wherever they are located. Army forces and individuals are in constant electromagnetic contact with adversaries who persistently probe and disrupt individual, group, and Army capabilities dependent on space, cyberspace, and the electromagnetic spectrum. Adversaries will attempt to establish persistent access to U.S. systems and wait to create an effect until the time and place of their choosing to maximize their strategic to tactical advantage. In some cases, the threat may maintain covert access to U.S. systems for years or decades before attempting to create an effect at the most impactful time and place.

SETTING THE THEATER

1-34. *Setting the theater* is the broad range of activities continuously conducted to establish conditions for the successful execution of operations in a theater (FM 3-0). Army forces—primarily the theater army—set the theater during competition below armed conflict to enable quick transitions during crisis and conflict. Setting the theater for cyberspace and electromagnetic warfare operations supports commanders' ability to—

- See themselves physically and virtually.
- See the threat and account for being under constant observation.
- Employ combinations of active and passive protection.

1-35. The theater army leverages theater-assigned and national-level capabilities to develop comprehensive understanding of—

- Friendly, adversary, and civilian use of cyberspace and the electromagnetic spectrum in theater.
- Adversary cyberspace and EW capabilities and activities.
- Friendly vulnerabilities in cyberspace and the electromagnetic spectrum.

1-36. Theater army efforts to set the theater may include collaboration with multinational partners to assess and improve their cyberspace and EW capabilities and defenses. The Army will likely depend on host nations for network support. These assessments may require support from cyber protection teams or national-level cyber defense forces.

CONTESTED DEPLOYMENT

1-37. Army forces cannot expect to deploy without being challenged by the threat. For decades, U.S. military forces have conducted uncontested and generally predictable deployments from home stations to operational theaters because threats could not significantly affect deploying units at home station or while in transit to a theater of operations. This is no longer the case. Peer threats have the capability and capacity to observe, disrupt, delay, and attack U.S. forces at any stage of force projection, including at home stations in the United States and overseas. Commanders and staffs must therefore assume friendly forces are always under observation and contact when planning and executing deployments. Threat activities to contest deployment begin with attacks at the home station and on critical infrastructure and continue through fort-to-port movement. See chapter 5 for more information about mitigating contested deployments and protecting deploying forces from fort to port.

EARLY AND INITIAL ENTRY

1-38. Army forces must be ready to deploy on short notice to austere locations and be capable of immediately conducting combat operations. During the initial phases of an operation, Army units may face numerically or qualitatively superior threats. The first deploying units must be able to defend themselves and collect information about threat activities so they can provide reaction time and freedom of maneuver for follow-on forces. During joint forcible entry, Army cyberspace and EW capabilities may provide critical support to the suppression of enemy air defenses and protection from enemy long-range fires to overcome enemy antiaccess and area denial. Forward-stationed forces may defend critical terrain with other multinational forces to delay enemy offensive operations. Some forward-stationed forces may defend joint bases and aerial and seaports of debarkation to enable flow of follow on forces and protect strategic and operational lines of communications. Electromagnetic protection is critical to the survival of forward-deployed Army forces as they fight in relative isolation in the early stages of combat operations.

PRECISION FIRES AND WEAPONS OF MASS DESTRUCTION

1-39. The likelihood an enemy will employ long-range precision fires and weapons of mass destruction increases during large-scale combat operations—particularly against command and control nodes, sustainment nodes, assembly areas, and critical infrastructure. Commanders should disperse forces as much as is tactically prudent to manage the risk that an enemy will locate friendly forces and engage them with long-range precision fires and weapons of mass destruction. Units should pay particular attention to reducing the electromagnetic signatures of command posts through EMCON to reduce the probability the enemy will locate the command post and target it with lethal fires. Dispersion increases the difficulty of both command and control and sustainment and may increase reliance on spectrum-dependent communications capabilities. Commanders should balance command post protection measures with the need for effective command and control and accept prudent risk. Operation plans should account for increased security, site defense, and EMCON requirements for dispersed forces.

CONGESTED ENVIRONMENT

1-40. Gaining and maintaining access to the electromagnetic spectrum is critical to achieving freedom of action in cyberspace in support of joint and Army operations. All U.S. forces and supporting agencies depend on a wide range of spectrum-dependent capabilities to enable and execute operations in the air, land, maritime, space, and cyberspace domains. Spectrum-dependent capabilities include—

- Communications.

- Information collection.
- EW.
- Precision-guided munitions.
- Aviation.
- Unmanned aircraft systems.
- Unmanned ground vehicles.
- Radars.
- Satellite-based positioning, navigation, and timing.
- Any system that transports data or voice communication through the electromagnetic spectrum.

1-41. Within the electromagnetic spectrum, joint forces contend with civil agencies, commercial entities, allied forces, and threats for use of a common electromagnetic spectrum resource. Competing for the finite available bandwidth sometimes results in an extremely congested electromagnetic spectrum, particularly when operating in developed nations.

1-42. Staffs plan communications and network capabilities to support all anticipated requirements in their assigned area. However, in a congested electromagnetic environment, there may be inadequate spectrum availability to support all missions. Staffs must deconflict EW and signal use of the electromagnetic spectrum in collaboration with the G-6 or S-6 spectrum manager, the G-2 or S-2, and SIGINT elements. Changes in the operational variables—political, military, economic, social, information, infrastructure, physical environment, and time or the mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations—METT-TC (I) could change spectrum requirements beyond the capabilities of assigned and attached forces. *Informational considerations* are those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information (FM 3-0). Refer to FM 5-0 for a more complete discussion of the operational and mission variables.

CONTESTED ENVIRONMENT

1-43. Enemies and adversaries may deliberately attempt to deny friendly use of the electromagnetic spectrum, space, cyberspace, and terrestrial systems. Due to heavy joint reliance on advanced communications systems, such an attack may be a central element of any enemy or adversary antiaccess and area denial strategy, requiring a higher degree of protection for friendly command and control systems and planning for operations in a denied or degraded environment.

1-44. Threat cyberspace and EW capabilities jeopardize U.S. freedom of action in cyberspace and the electromagnetic spectrum. Adversaries understand the extent of U.S. forces' reliance on communications and automated information systems. Because communications are key to the exercise of command and control, U.S. military communications and information networks present high-value targets for enemies and adversaries. In future conflicts, enemies and adversaries will contest U.S. capabilities in cyberspace and the electromagnetic spectrum to deny operational access and diminish the effectiveness of U.S. and allied forces.

1-45. An enemy can use radio frequency direction-finding equipment to locate radio frequency emitters. Once the enemy determines an accurate location, enemy forces can maneuver or direct lethal or nonlethal fires to destroy or degrade the capability. Vulnerable emitters include—

- Radios.
- Satellite communications terminals.
- Counter-improvised explosive device systems.
- Radars.
- Unmanned aircraft systems.
- Unmanned ground vehicles.
- Cell phones.

1-46. Implementing electromagnetic protection techniques based on current intelligence estimates may mitigate a threat's ability to find and attack key communications nodes or command posts. The G-2 or S-2 section defines the threat's electromagnetic order of battle. The CEWO's knowledge of threat EW capabilities and techniques helps inform communications and electromagnetic protection plans that limit the threat's effectiveness.

1-47. G-6 or S-6 section cybersecurity personnel must protect network capabilities by applying the DOD risk management framework and cybersecurity policies. Local network defenders must be prepared to defend the network in case of malicious cyberspace activity.

1-48. Synchronizing signal support with cyberspace, EW, intelligence, space, and other information activities is key to achieving and maintaining freedom of action in contested cyberspace and the electromagnetic spectrum while denying the same to threats. *Synchronization* is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 2-0). Synchronization provides the ability to execute multiple related and mutually supporting tasks in different locations at the same time, producing greater effects than executing each in isolation.

1-49. The cyberspace electromagnetic activities (CEMA) section plays an important role in several integrating processes and working groups, including—

- Intelligence preparation of the operational environment.
- Information collection.
- Risk management
- Targeting process.
- CEMA working group.
- Targeting working group.

1-50. Synchronization of capabilities across multiple domains and warfighting functions maximizes their inherently complementary effects in and through cyberspace and the electromagnetic spectrum. Planning for locations of automated systems and network transport must account for threat conditions. Planning must also support maneuver if attacked.

Degraded

1-51. The cyberspace and space domains grow in importance as global competitors, regional competitors, and non-state actors invest in capabilities to protect their access and disrupt or deny access to others. Although Army forces have grown accustomed to communicating freely without fear of jamming or interception, threats are likely to use technological advances in cyberspace and vulnerabilities in the electromagnetic spectrum to attack U.S. cyberspace and spectrum-dependent capabilities.

1-52. A broad array of threat actors will challenge the joint force's freedom of action in space, cyberspace, and the electromagnetic spectrum. For example, a threat that jams positioning, navigation, and timing satellites may degrade precision fires, situational understanding, and battlespace deconfliction. Army commanders must protect their own systems and disrupt the enemy's ability to operate while being prepared to operate with degraded communications and reduced access to cyberspace- and spectrum-dependent capabilities.

1-53. While threat action might cause a degraded environment, degraded capabilities may also occur because of insufficient resources to support all communications requirements. For example, inadequate electromagnetic spectrum availability in an operational area causes congestion and network latency. Unintentional electromagnetic interference may also cause degradation.

1-54. Careful operational planning can minimize disrupted operations in a degraded environment. The CEWO collaborates with the G-3 or S-3 and the G-6 or S-6 to develop electromagnetic protection plans to preserve spectrum-dependent capabilities. The commander's priority of effort includes priorities of service. The staff's prioritization of effort must support the commander's plan. Continuity of operations plans; primary, alternate, contingency, and emergency communication plans; and disciplined initiative under the mission command philosophy can mitigate the effects of degraded capabilities in cyberspace and the electromagnetic spectrum.

Denied

1-55. Threats may adopt an antiaccess and area denial strategy against U.S. forces. An enemy or adversary with the ability to field layered and fully integrated antiaccess and area denial capabilities may try to deny U.S. access to an operational area altogether. Defeating threat antiaccess and area denial to support joint forcible entry may depend heavily on effects in cyberspace and the electromagnetic spectrum.

1-56. Targeting in cyberspace to defeat threat standoff and layered air and missile defenses depends on targeting undertaken by the theater army and combatant command during competition and crisis in their efforts to set the theater. Offensive cyberspace effects to defeat threat antiaccess and area denial will likely be delivered by national-level cyber mission forces.

UNDERSTANDING AN OPERATIONAL ENVIRONMENT

1-57. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). For Army forces, an operational environment includes portions of the air, land, maritime, space, and cyberspace domains understood through three dimensions (human, physical, and information). The air, land, maritime, and space domains are defined by their physical characteristics. Cyberspace transits and connects the other domains. Figure 1-1 illustrates the relationship between the domains and the dimensions of an operational environment.

Note. Joint doctrine describes the components of an operational environment as the physical areas of the air, land, maritime, and space domains; the information environment (which includes cyberspace); the electromagnetic spectrum; and other factors. The Army does not use 'information environment' to understand, visualize, and describe an operational environment. Refer to JP 2-0 and JP 5-0 for more information about describing and analyzing an operational environment from a joint perspective and FM 3-0 for more information about the Army's approach to understanding operational environments.

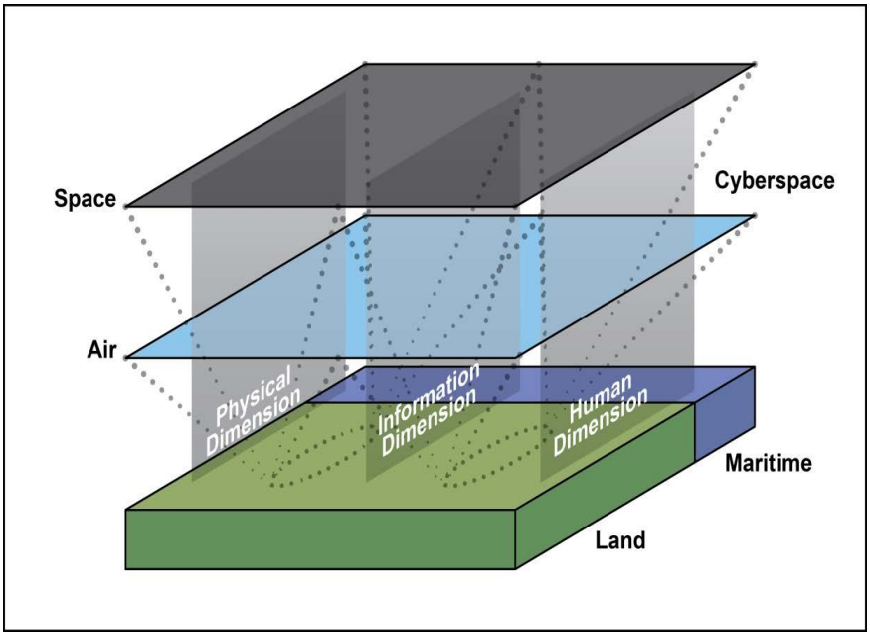


Figure 1-1. Domains and dimensions of an operational environment

1-58. Situational understanding of an operational environment accounts for all factors, circumstances, and conditions that impact the conduct of operations. Thorough understanding of the environment allows leaders to identify problems, anticipate outcomes, and understand the results of various actions and how these actions affect planned operations. The common operational picture enables situational understanding by helping commanders and staffs visualize their operational environment, including all the factors they need to consider in planning and conducting operations.

1-59. Understanding an operational environment requires continuous reconnaissance, surveillance, security, and intelligence operations to acquire information. Commanders gather information from multiple sources. EW and SIGINT elements conducting electromagnetic support in the close area are important reconnaissance assets. EW and SIGINT teams can use radio frequency direction finding to geolocate threat emitters, including radios, other communications systems, and radars. This location information can be used

immediately as combat information or may feed into intelligence channels for further processing and analysis as intelligence. *Combat information* is a report that is gathered by or provided to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence before being used to support decision making (FM 2-0).

Note. Despite its name, 'combat information' refers to all information of this type provided to tactical commanders across the competition continuum. It is not limited to armed conflict.

1-60. Commanders and staffs use all available relevant information, whether combat information or intelligence, to determine how the operational environment affects operations. This allows commanders to understand which courses of action are the most feasible, acceptable, and suitable. Commanders and staffs rely on integrated information collection throughout the course of operations to develop an accurate picture of their operational environment. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). EW elements conducting electromagnetic support are positioned to answer many critical information requirements and can provide time-sensitive combat information to support decision making and targeting. The CEMA section may refer some information collected through electromagnetic support activities to the G-2 or S-2 to feed into intelligence channels for further processing to meet intelligence requirements. Refer to FM 3-55 for more detailed discussion of information collection.

1-61. Operational environments undergo continual change due to the interactions between various friendly, threat, and neutral actors and as actors learn and adapt to conditions in the environment. Because operational environments are complex and dynamic, it is sometimes challenging to determine cause and effect relationships, leading to ambiguity. There are several tools, processes, and frameworks to assist commanders and staffs in understanding their operational environments. They include—

- Domains (refer to FM 3-0).
- Dimensions (refer to FM 3-0).
- Operational and mission variables (refer to FM 5-0).
- Running estimates (refer to ADP 5-0).
- The Army design methodology (refer to ATP 5-0.1).
- The military decision-making process—battalion and above (refer to FM 5-0).
- Troop leading procedures—companies and platoons (refer to FM 5-0).
- Pre-mission analysis of the operational environment (refer to FM 2-0).
- Intelligence preparation of the operational environment (see chapter 4).
- Sustainment preparation of the operational environment (refer to FM 4-0).

THE CYBERSPACE DOMAIN

1-62. For Army forces, the *cyberspace domain* is the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum (FM 3-0). The cyberspace domain crosses and connects all other domains. Friendly, enemy, adversary, and host-nation networks, communications systems, computers, cellular telephone systems, social media, and technical infrastructures are all parts of cyberspace. Cyberspace is congested, contested, and critical to successful operations. Operations in a geographic area may rely on data and analysis conducted elsewhere but connected through cyberspace. Planners must account for dependence on these reachback capabilities when making network and contingency plans.

1-63. Communications and information systems in cyberspace use links and nodes located in the air, land, maritime, and space domains for connectivity. Therefore, cyberspace is highly dependent on the other domains and the electromagnetic spectrum. At the same time, due to their interconnected nature, conditions and effects in cyberspace can affect the other domains. The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace and the electromagnetic spectrum, and a critical portion of cyberspace bandwidth can only be provided via satellite communications, which provide

a key global connectivity option for cyberspace operations. These interrelationships are important considerations during planning.

1-64. The Army conducts cyberspace operations and supporting activities as part of Army, joint, and multinational operations. Because cyberspace is a global communications and data-sharing medium, it is inherently a joint, interorganizational, and multinational shared resource with signal and intelligence organizations maintaining significant equities. Data sensed and collected during operations can be correlated with other data to generate relevant insight. Cyberspace capabilities enable decision making and protect friendly information.

1-65. Commanders can leverage cyberspace intelligence and reconnaissance capabilities from higher-level joint and national-level units to gain enhanced understanding of the threat situation. Cyberspace intelligence and reconnaissance can augment and enhance the understanding a commander gains from other forms of information collection and intelligence processes.

THE ELECTROMAGNETIC SPECTRUM

1-66. The electromagnetic spectrum consists of the entire range of wavelengths or frequencies of electromagnetic radiation extending from the longest radio waves to gamma and cosmic rays (the shortest wavelengths). The electromagnetic spectrum is a maneuver space that is essential for facilitating control within the operational environment and impacts all portions of the operational environment and military operations. Despite the wide range of the electromagnetic spectrum, the usable portions are a limited resource with competing demands from military, governmental, commercial, and personal users for communications and noncommunications purposes.

1-67. Because of the dependence on spectrum-dependent capabilities, Army forces have the imperative to own the electromagnetic spectrum. Military operations and training are executed in an environment complicated by increasingly challenging demands and constraints on the electromagnetic spectrum. Just as in the physical domains and in cyberspace, military forces maneuver and conduct operations within the electromagnetic spectrum to achieve tactical, operational, and strategic advantage. Freedom of maneuver and action within the electromagnetic spectrum are essential to U.S. and multinational operations. Spectrum use must be planned, deconflicted, and protected to support command and control, sensing, information collection, data sharing, and effects delivery at the right time and tempo to support combined arms operations.

1-68. In early use of the electromagnetic spectrum, military forces only relied on radio communications. In the early years of World War II, spectrum use expanded to extensive use of radar systems. Over the past several decades, military use of, and dependence on, the electromagnetic spectrum have increased greatly. In the modern world, nearly every vehicle, combat platform, and Soldier relies to some extent on one or more spectrum-dependent devices or capabilities, including—

- Communications and information systems.
- Positioning, navigation, and timing.
- Detection and monitoring.
- Precision fires.
- Radar.
- Air defenses.
- Unmanned aircraft systems or unmanned ground vehicles.

1-69. Nearly every person, civilian and military, relies on the electromagnetic spectrum for many of their everyday activities, including cellular communications, wireless Internet access, satellite navigation, and radio and television broadcast. Military users share the limited bandwidth in the electromagnetic spectrum with many other users, including other militaries (friendly and threat) and civilian users. Spectrum managers plan friendly use of the electromagnetic spectrum and perform host-nation coordination to deconflict with friendly military and civilian spectrum use. Preserving friendly civilian access to the electromagnetic spectrum has significant implications for quality of life and may contribute to, or degrade, civilian populations' support of U.S. military action. G-6 or S-6 spectrum managers also collaborate with the CEMA section and the G-2 or S-2 to deconflict frequency use with EW and SIGINT. Figure 1-2 on page 13 illustrates the competing friendly, threat, and neutral spectrum-dependent devices sharing the electromagnetic spectrum.

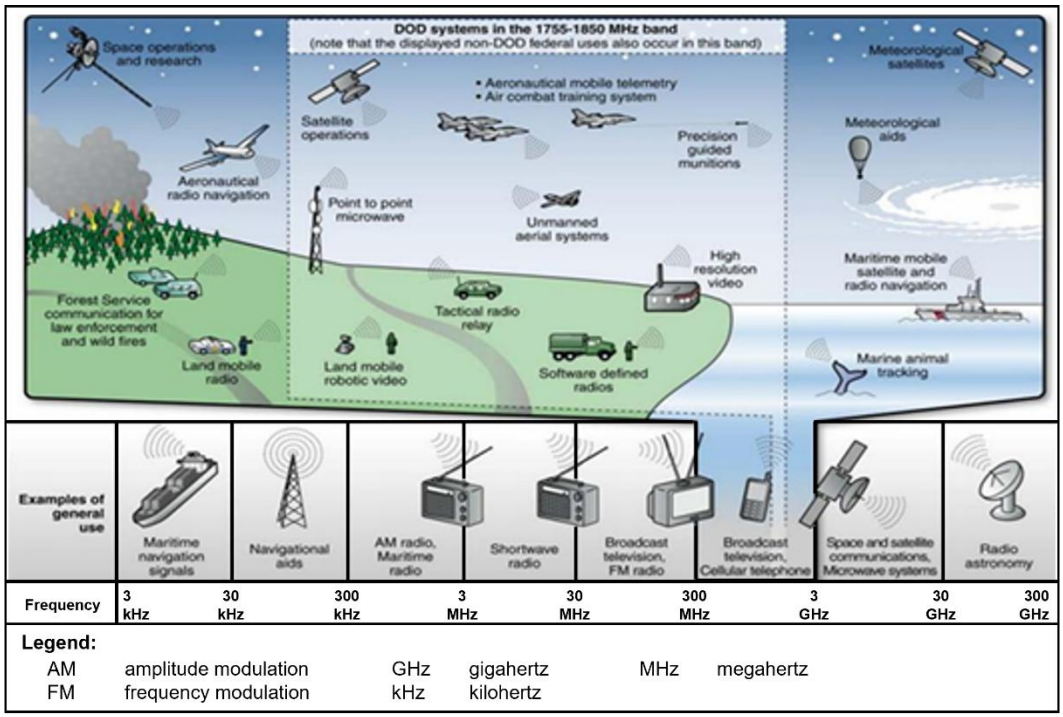


Figure 1-2. Competition for available electromagnetic spectrum resources

1-70. To preserve warfighting capabilities, commanders must take actions to maintain an operational advantage with freedom of action in the electromagnetic spectrum. EW capabilities enable commanders to achieve relative advantages in the electromagnetic spectrum when operating against peer threats who are equally reliant on spectrum-dependent devices. Electromagnetic support allows leaders to maintain situational understanding of friendly, threat, and neutral electromagnetic signatures to support protection planning and targeting. By protecting friendly information systems and signals from threat disruption or exploitation, a commander can ensure command and control and maintain operations security. Conversely, a commander might use electromagnetic attack to degrade an enemy's decision-making processes by disrupting enemy sensors, communications, or data processing. To achieve an information advantage, a commander must plan early to integrate EW activities into the overall scheme of maneuver.

SECTION II – THREATS AND HAZARDS

1-71. U.S. forces face a variety of threats and hazards through cyberspace and the electromagnetic spectrum. It is important for commanders and staffs to understand the nature and operational impact of these threats and hazards to mitigate their effects on operations.

OVERVIEW

1-72. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats can generally be categorized as adversaries, enemies, or insider threats. An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0). An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). Insider threats present unique challenges because they are trusted individuals with access to Army capabilities and sensitive operational information. Hazards are natural or artificial conditions that present risk to operations. The effects of hazards are considered neutral, since they affect friendly, threat, and neutral parties equally.

THREAT ACTIVITIES IN CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

1-73. Threats will likely have the advantage of initiative, delivery mechanisms, and timing of malicious cyberspace activity. Some state-sponsored threats commit significant resources to offensive cyberspace capabilities and follow less restrictive rules for employing these capabilities than U.S. forces. Developing, testing, and employing system patches and mitigating techniques to counter threat capabilities is time consuming. A threat exploiting a previously unknown cyberspace vulnerability has an asymmetric advantage and may significantly disrupt U.S. operations until defensive cyber forces can develop, test, and deploy a software patch or other mitigating technique. U.S. forces are sometimes heavily dependent on civilian network infrastructure that may or may not be properly secured against known vulnerabilities and exploits.

1-74. Setting the conditions for significant malicious cyberspace activity or electromagnetic attack can be very time consuming, but the speed of execution is fast and exceeds the reaction time and decision-making process of most tactical units. Commanders should recognize the factors U.S. forces will contend with in cyberspace and the electromagnetic spectrum. Commanders and staffs must maintain situational understanding of cyberspace and the electromagnetic spectrum to enable timely decision making.

THREAT ACTIVITIES IN CYBERSPACE

1-75. Threats can exploit system vulnerabilities to cause a loss of confidentiality, integrity, or availability of network and information technology system capabilities. Protecting the information on the Army network is essential to maintaining freedom of action in cyberspace.

1-76. The distinction between enemies and adversaries is clear in the air, land, maritime, and space domains, but less so in cyberspace. An adversary may well take hostile actions against U.S. interests in cyberspace without becoming an enemy that U.S. forces might engage in the other domains. For this discussion, 'threats' encompasses both adversaries and enemies.

1-77. U.S. networks and information systems, including the civilian infrastructure on which U.S. forces depend, face continuous risk from a variety of threats. Every day, these networks come under attack by threats including—

- Insider threats.
- Foreign intelligence entities.
- Military opponents.
- Geopolitical rivals.
- Terrorist groups.
- Non-state actors (criminal and activist organizations).

Note. While DOD cyber forces secure and defend the Department of Defense information network (DODIN), the Department of Homeland Security has the primary mission to defend federal civilian networks within the United States and engages state and local governments and the private sector to synchronize efforts to defend critical infrastructure.

1-78. Threats use many methods to disrupt, degrade, destroy, exploit, alter, or otherwise adversely affect the Army's use of cyberspace. Elements of the network reside across the physical domains, with different methods of communicating and varying levels of interconnectivity and isolation. Threats may seek to exploit any network node, communications link, or the data residing in or traversing the nodes and links. Connecting critical infrastructure to the network exposes it to the risk of malicious cyberspace activity.

1-79. Cyberspace allows threats to operate anonymously or to obscure their identity and location. This allows threats to pose as friendly actors and deceive individuals into divulging sensitive information or circumventing security measures—likely without realizing they have done so—through social engineering or phishing. Threat cyber forces can attack Army systems, networks, and information by manipulating unsecured systems.

Note. Social engineering uses techniques that rely on weaknesses in human nature rather than software. The goal is to deceive people into revealing passwords and other information that compromise the security of automated information systems and networks.

1-80. The same gateways that enable information exchange and allow legitimate outside users to access the network present attack vectors threats will attempt to exploit. Threat forces often use the same commercial networks as noncombatant civilian populations, complicating malicious cyberspace activity attribution and response.

1-81. The broad range of hostile actors in cyberspace increases complexity in securing and defending the Army network. The enduring nature of threat malicious cyberspace activities causes U.S. forces to expend considerable resources and effort securing DOD networks. Network-enabled operations are a force multiplier and a traditional strength of U.S. forces. However, network-enabled operations also create significant vulnerabilities. The extent to which U.S. forces rely on networked capabilities presents broad cyberspace and electromagnetic spectrum attack surfaces.

1-82. Failing to protect even one system can create a foothold into the network and place sensitive data, U.S. operations, and lives at risk. Even when cyberspace defenders discover and stop an attack, they might not be able to attribute it to a particular source. Following cybersecurity best practices, defending the network, and adhering to operations security guidelines help protect DOD networks and data.

1-83. Threats may undertake intelligence gathering in friendly networks, either to support their operations or to counter U.S. operations. Exploitation reveals information resident on, or transiting through, a system. Threat intelligence activities can compromise sensitive operational information.

1-84. Trusted insiders with legitimate access to systems pose one of the most difficult threats to counter. Insider threats arguably present the greatest risk to operations security because they can readily access sensitive information.

1-85. Threats will systematically and continuously combine all available means to attack U.S. and allied network capabilities. Peer threats will use deceptive tactics such as phishing attacks to gain access to Army networks for follow-on malicious cyberspace activities.

1-86. Commanders must recognize the proliferation of threat cyberspace capabilities and their impact on operations. Threat malicious cyberspace activities can disrupt friendly information systems and degrade joint command and control. Threat operations in cyberspace are often less encumbered by treaty, law, and policy restrictions than those self-imposed on U.S. forces. This may give threats an initial advantage in cyberspace. Army units must maintain an effective cybersecurity program, integrated with defensive cyberspace capabilities, to secure the network against threat malicious cyberspace activities.

1-87. Malicious cyberspace activity may originate from any of the categories of state and non-state threats; there is no way to quickly identify the source. This complicates understanding of the threat's intent, purpose, and objectives.

THREAT ACTIVITIES IN THE ELECTROMAGNETIC SPECTRUM

1-88. The Russo-Ukrainian War provides an undeniable lesson—mastery of the electromagnetic spectrum is no longer a luxury, but a prerequisite for success in large-scale combat operations. Russia's initial overwhelming use of EW, from crippling command and control networks to blinding Ukrainian defenses, underscored its potential as a decisive force multiplier. While Ukraine has adapted with commendable ingenuity, the conflict exposes a critical vulnerability for the Army—a potential gap in preparedness to fight and win in a highly contested electromagnetic operational environment.

1-89. In the electromagnetic spectrum, radio frequency transmitters used to jam radars and communications systems may also provide a transmission path to insert viruses and other malicious computer code into spectrum-dependent devices to spoof or disable them. Electromagnetic attacks applied from the air, land, maritime, or space domain by manned and unmanned systems can target humans, communications systems, radars, or other assets. Threat electromagnetic attacks can affect—

- Satellite-based positioning, navigation, and timing (spoofing or jamming).

- Satellite-based and terrestrial radio frequency communications (jamming).
- Precision guided munitions (spoofing or jamming).
- Radars (spoofing or jamming).
- Unmanned aircraft systems or unmanned ground vehicles (spoofing or jamming).

1-90. Any device that emits electromagnetic energy can be located through radio frequency direction finding. Once an enemy or adversary locates an emitter, they can exploit the information for combat information or target the emitter for intelligence collection or lethal or nonlethal fires. This has long been a vulnerability with peer threats; in recent years there has been a proliferation of relatively inexpensive commercial off-the-shelf equipment that can accomplish many of the same things. Even a relatively unsophisticated non-state threat can now locate U.S. communications systems and command posts with relative precision at low cost.

1-91. Any electromagnetic signature that is not common in the operational area will attract attention from the threat. Examples of electromagnetic signatures that stand out include—

- Single-channel radios operating in military-specific portions of the spectrum.
- Encrypted radio signals.
- X band satellite communications signals.
- Cell phones with U.S. subscriber identification modules in an overseas area.

1-92. If a threat locates a high density of emitters that are not common to the operational area, they might correctly assume they have pinpointed a military formation. Experience at combat training centers shows the radio frequency heat maps of military formations often allow the opposing force to determine position, disposition, and actions of command posts and maneuver formations. Metadata from government-issued cell phones sometimes identifies the user by role (for example, the commander, executive officer, or S-3), identifying them as high-value targets.

STATE THREATS

1-93. Traditionally, state threats pose the greatest threat in cyberspace and the electromagnetic spectrum due to their ability to match or exceed U.S. capabilities and resources. State threats assess that the Army's reliance on the electromagnetic spectrum is an exploitable weakness and strive to develop and field EW systems to disrupt current and projected U.S. capabilities. State threats typically employ broad cyberspace capabilities as coercive elements of great power competition. State threats design their activities to disrupt U.S. operations and undermine perceived U.S. technological advantages.

1-94. State agents continually probe U.S. networks to identify areas of weakness, attack to gain a foothold, and maneuver to a position of advantage so they can create an effect at the time and place of their choosing. The weakest link is the entry point. State threats employ a wide array of techniques ranging from phishing scams to insider threats to gain access to critical systems. Opportunistic states may also use coercive methods with allies or partners to obtain access to shared systems and data. Since state threats assess that they can conduct these operations with limited attribution and avoid a direct military response, these methods continue across the competition continuum.

1-95. Many state threats exercise strict control over communications and Internet infrastructure within their borders and their connections with global Internet. This strict state control offers a measure of sanctuary from U.S. cyberspace attacks in these nations.

PEER THREAT

1-96. Peer threats are adversaries or enemies with capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a region where they enjoy a relative advantage. Not all state threats are global or regional peers. Peer threats possess roughly equal combat power in geographic proximity to a conflict area with U.S. forces. Peer threats employ their resources across multiple domains to exploit perceived U.S. vulnerabilities.

1-97. Because peer threats can contest the force in all domains, Army forces must be prepared to defend themselves in all domains and continue to conduct operations when supporting capabilities are not available. For instance, under the mission command approach, subordinates can continue their missions, understanding the commander's intent when communications are disrupted. Units must be able to navigate using alternate

means, such as map and compass if space-based positioning, navigation, and timing capabilities are unavailable.

1-98. Peer threats have demonstrated advanced capabilities in long-range precision fires, integrated air defense, and EW. These threat capabilities demand changes to tactics, techniques, and procedures to counter the risks they present. Friendly command and control nodes and other electromagnetic emitters must displace frequently during large-scale combat operations to avoid destruction by enemy fires.

1-99. Peer threats consider U.S. communications, command and control nodes, massed formations, and critical infrastructure key targets during large-scale combat operations. Commanders should ensure as much dispersion of their formations as tactically prudent. Locating radio frequency emitters, such as satellite communications antennas and line of sight radio systems, away from major command posts minimizes loss of life and command and control capabilities if the enemy targets the communications systems with lethal fires. Global and regional peers include China, Russia, Iran, and the Democratic People's Republic of Korea (North Korea).

CHINA

1-100. China is the United States' most active strategic competitor, both militarily and economically, and will likely continue to challenge U.S. and partner nation strategic interests in the foreseeable future. While the United States can currently overmatch Chinese power projection capabilities, Chinese asymmetric attacks may place significant pressure on U.S. and partner nation command and control systems.

1-101. China presents a persistent cyber espionage risk to DOD networks with a growing ability to conduct malicious cyberspace activity against U.S. military and civilian critical infrastructure. Chinese state intelligence organizations may use third-party entities or criminal hackers to penetrate U.S. and partner nation critical infrastructure and networks prior to deployment or within the assigned area. A growing concern is China's improving ability to alter online information to shape the views of the U.S. public, which can present commanders a challenge in their attempts to gain an information advantage.

1-102. Chinese cyber actors can conduct localized, temporary disruptive effects on critical infrastructure, such as disrupting a natural gas pipeline for days to weeks. China has invested heavily in acquiring industrial control systems technology for domestic energy consumption. Tactical units located in areas where Chinese companies operate or have previously worked may be subject to additional risk to local industrial control systems as a result. China intends to dominate the commercial 5G network globally, which expands the challenges within the operational environment and presents an operations security concern in areas with a large Chinese telecommunications presence or where they operate the communications infrastructure. Chinese quasi-governmental ownership of the telecommunications infrastructure in entire countries or regions gives them the ability to collect intelligence information through the network or deny access to communications and Internet service at will.

1-103. Chinese activities in the electromagnetic spectrum intertwine with the commercial and military sectors. China will direct their efforts against friendly EW assets and communications (including satellite) networks to disrupt U.S. systems and gain qualitative advantages. Chinese EW capabilities will likely be more prevalent in a land-based operational environment and will likely participate in some capacity during naval campaigns. Airborne EW assets may take on a larger operational and tactical role during a naval campaign.

RUSSIA

1-104. Russia is proficient at executing cyber espionage, malicious cyberspace activity, influence operations, and EW operations down to the tactical level to achieve its political and military objectives. Russian cyber espionage is sophisticated and likely coupled with human intelligence gathering techniques. Tactical commanders can anticipate facing combinations of intelligence gathering, network disruption, and other information warfare activities.

1-105. Russia can execute malicious cyberspace activities that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting unsecured industrial control systems. Russian information warfare uses and manipulates social media platforms to gain public support and influence their opponents at the tactical level to obtain their preferred outcomes. Russian disinformation techniques span all

levels of operations, from national strategic, through the theater strategic, operational, and tactical levels to influence operations.

1-106. Russia may employ third-party operatives such as cyber criminals to conduct malicious cyberspace activities to affect tactical commanders while affording non-attribution and plausible deniability. These operatives may conduct malware-as-a-service or hacker-for-hire activities aimed at disrupting Army network capabilities.

1-107. Russia employs robust tactical EW capabilities with the ability to perform in the air, land, maritime, and space domains. Russian EW supports tactical units or special operations forces that leverage EW to mask movement or operations. A combination of malicious cyberspace activities and EW directed at telecommunications networks may drive friendly units to resort to redundant communications or, in the case of local civilians, onto an established network. Once there, Russian cyber units may collect intelligence or combat information for targeting with lethal or nonlethal capabilities. Russia does not observe the same restraints on cyberspace operations activities as the United States. Their less restrictive rules of engagement, coupled with the scope and scale of their malicious cyberspace activities, offers them an asymmetric advantage.

Note. Russian doctrine uses the term 'special purpose forces' for their special operations units. For clarity, this manual refers to 'special operations forces' when describing special operations units, whether employed by the United States, allies, adversaries, or enemies.

IRAN

1-108. Iran presents a cyber espionage and malicious cyberspace activity risk to the U.S. homeland as well as the Middle East region. Iranian military and cyberspace capabilities are improving and present direct risks to tactical operations and logistics support. Global dependence on fossil fuels produced in the Middle East provides the Iran regime financial resources and serves as an external focus for Iranian attacks against U.S. and allies' critical infrastructure. Iranian cyber actors have predominantly targeted Saudi Arabian and other regional infrastructure with disruptive and destructive malicious cyberspace activity. Iranian cyber campaigns have targeted various regional and U.S. government systems, political processes, financial institutions, and critical infrastructure.

1-109. Iran uses multiple social media platforms to target U.S. and allied audiences with pro-Iran messages. Iranian disinformation efforts, while limited in scale, seek to employ cyber-launched messages in conjunction with conventional military or proxy activities. Iran has the means to purchase malicious software and tools or employ malware-as-a-service to obfuscate their malicious cyberspace activities. Iran is hardening its internal telecommunications and cyber infrastructure since the highly publicized 2010 Stuxnet computer worm crippled Iranian nuclear centrifuges.

1-110. Iran generally retains EW capabilities at the operational level, primarily as a defensive asset to preserve the regime. However, Iran may be growing its tactical-level EW capabilities. Airborne EW delivery extends Iran's limited capabilities to the tactical level and may disrupt friendly actions.

1-111. The Iranian regime views the United States and its allies as its greatest existential threat and prefers non-attributable, asymmetric attacks to counter U.S. regional presence. Iran often uses regional proxy forces to execute operations against U.S. and allied forces. Iranian special operations forces and their proxies will exploit opportunities to physically attack U.S. forces within the region, typically as a coercive means to achieve a political or economic advantage.

NORTH KOREA

1-112. North Korea assesses that malicious cyberspace activity and EW can provide the regime an asymmetric advantage in warfare against the United States and the Republic of Korea. North Korea's Internet infrastructure and the regime's strict control over its use ensure that there are no rogue cyberspace actors. All North Korean government-sanctioned actors exercise careful security practices to prevent information leaks. This, coupled with the relative isolation of North Korea's Internet infrastructure, makes it difficult to develop cyberspace threat intelligence and attribution. North Korea's isolated networks and prioritization of resources

for military use provide a secure and structured base of operations from which they can conduct cyberspace operations.

1-113. For years, North Korean malicious cyberspace activities have mainly consisted of state-sanctioned cybercrime, such as ransomware attacks, to generate revenue for the regime in the face of international sanctions, industrial espionage, and intelligence collection. North Korean cyber intelligence collection largely focuses on the aerospace, defense, government, manufacturing, media, academic, and technology sectors. More recently, North Korean malicious cyberspace activity has begun to shift focus to critical infrastructure and industrial controls.

1-114. While the North Korean regime has used EW since the Korean War, after studying U.S. operations in the Gulf War they have increased their investment in advanced EW capabilities to create an asymmetric advantage against the United States and the Republic of Korea. North Korean EW and SIGINT operate as an integrated capability to simultaneously affect the electromagnetic spectrum and collect intelligence. North Korean electromagnetic spectrum capabilities employed at the Demilitarized Zone include electromagnetic sensors, radar, and SIGINT collection capabilities. Recent historical uses of electromagnetic attack by North Korea include electromagnetic jamming of—

- Military and commercial radio broadcast.
- Satellite-based positioning, navigation, and timing.
- Unmanned aircraft system controls.

PEER THREAT TACTICS

1-115. Peer threats use their capabilities to create lethal and nonlethal effects throughout an operational environment. Peer threat tactics relevant to cyberspace operations and the electromagnetic spectrum include sanctuary, systems warfare, and contested deployment. See paragraph 5-75 for more information about contested deployment.

SANCTUARY

1-116. Sanctuary is a threat method of putting their forces beyond the reach of friendly forces. It provides threat forces protection derived by some combination of political, legal, and physical boundaries and distance that restrict freedom of action by a friendly force commander. Peer threats will use any means available, including sanctuary, to protect key elements of their combat power from destruction, particularly by air and missile capabilities. The global reach of cyberspace operations may allow a state threat to launch malicious cyberspace activity from relative sanctuary. Because U.S. portions of the Internet and much of its critical infrastructure are freely connected to the global Internet, the United States has no sanctuary from threat malicious cyberspace activity.

1-117. The corps leverages long-range sensing capabilities of organic, other Service, and multinational partner EW elements to understand the locations, strength, and disposition of threat forces in the deep area. This understanding supports long-range targeting to reduce the protection threats seek to derive by operating from sanctuary.

SYSTEMS WARFARE

1-118. Peer threats view the battlefield, their own instruments of power, and an opponent’s instruments of power as a collection of complex, dynamic, and integrated systems composed of subsystems and components. Peer threats use systems warfare to identify critical capabilities for disruption or destruction to cause failure of a larger friendly system.

1-119. An example of systems warfare against friendly command and control is an enemy using radio frequency direction finding to locate a critical communications site. Once the enemy locates the communications site, they can confirm the location using unmanned aircraft systems and direct long-range precision fires from sanctuary to prevent counterattack. Targeting a critical communications asset has a more significant effect than destroying a typical single node in the network. Loss of the communications capability may disrupt critical functions or affect many radios across a wide section of the assigned area and disrupt command and control until the isolated elements can restore communication by an alternate, contingency, or emergency means. Refer to TC 7-100.2 for an in-depth discussion of threat systems warfare.

HYBRID THREAT

1-120. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects (TC 7-100). Some aspects of the hybrid threat, such as criminal or terrorist organizations, do not abide by the law of armed conflict. Hybrid threats seek to exploit asymmetric advantages over an adversary to avoid engaging in direct combat.

1-121. In many ways, hybrid threat is not a new way of fighting a war; it is simply a new way of framing an operational environment. The Colonials in the American Revolution employed a hybrid strategy with a mixture of regular Continental troops, state militias, irregular partisans, and supportive local populations, along with publishers and pamphleteers sympathetic to the revolutionary cause. What has changed is the tools available to threats and the ability of some of these tools to create far-reaching effects outside the operational area. Enemies may employ malicious cyberspace activity and cyber espionage, electromagnetic jammers, and space-based capabilities, such as anti-satellite weapons, to disrupt U.S. communications; positioning, navigation, and timing; synchronization; and freedom of maneuver. A peer threat's ability to combine regular and irregular forces, robust information warfare capabilities, long-range precision fires, and massed lethal fires with the capacity to contest or achieve air superiority presents a formidable challenge.

1-122. The hybrid threat understands that the most challenging environment for U.S. forces is one where conventional military operations occur in concert with irregular warfare. The hybrid threat concept is not simply making do with what is available, but deliberately taking advantage of all tools at hand to create a complex operational environment.

1-123. Hybrid threats employ a wide variety of military, paramilitary, insurgent, criminal, and information warfare capabilities in concert with a robust antiaccess and area denial strategy and long-range precision fires to support their strategic and tactical objectives. Each component of the hybrid threat brings additional capabilities to bear. Commanders should not underestimate the synergy of these capabilities. Operational environments are inherently complex due to the operational variables—political, military, economic, social, information, infrastructure, physical environment, and time. The hybrid threat seeks to introduce additional complexity using an ever-shifting array of forces, technologies, and techniques. The hybrid threat may conduct a conventional military attack while simultaneously creating economic instability, fostering lack of trust in existing governance, attacking information networks, and conducting a propaganda campaign, perhaps while causing a humanitarian crisis.

1-124. Commanders facing a hybrid threat may have difficulty identifying and responding to specific challenges. If they faced these challenges individually, U.S. forces could readily isolate and defeat each aspect of the hybrid threat. However, because hybrid threats are agile and integrate these capabilities throughout an operational area, they can continue to shift effort and emphasis to make all U.S. choices seem poor ones. Threats can learn and adapt quickly, often unrestricted by rules or bureaucracy. The hybrid threat's continually shifting efforts may cause haphazard and incomplete change, but such rapid adaptation is difficult to counter. Ultimately, success goes to those who can act, react, and adapt their tactics quickly and creatively.

THREAT INFORMATION WARFARE

1-125. Information warfare refers to a threat's use of information activities, such as malicious cyberspace activity and EW, to gain an operational advantage. The threat construct of information warfare merges the disciplines of EW, deception, lethal fires, information protection, perception management, information attack, and computer warfare into a mutually supporting, integrated capability. Threat information warfare consists of—

- **EW.** Measures to control or deny friendly use of the electromagnetic spectrum while ensuring its use by the threat.
- **Deception.** Measures designed to mislead friendly forces by manipulation, distortion, or falsification of information to induce friendly forces to act in a manner prejudicial to their interests.
- **Physical destruction.** Measures to destroy critical components of friendly communications infrastructure.
- **Information protection.** Measures to protect the threat's information infrastructure and to deny friendly forces access to the threat's protected information.

- **Perception management.** Measures aimed at creating a perception of truth that best suits threat objectives. Perception management uses a targeted combination of true, false, and misleading information to sway public opinion in its favor or impact critical decision makers.
- **Information attack.** Attacks against the information resident on or transiting communications and information systems, rather than the systems themselves. Information attacks focus exclusively on the manipulation or degradation of the information to affect friendly decision making.
- **Computer warfare.** Threat malicious cyberspace activity ranging from unauthorized access (hacking) of information systems for intelligence collection purposes to the insertion of malware and deceptive information into friendly computer systems.

1-126. Because these elements share some of the same functions, means, and targets, the threat can formulate and execute a single, integrated information warfare plan. Despite the name information warfare, threats continually conduct these activities at every level of warfare across the competition continuum to set favorable conditions, protect their self-interests, and influence public opinion in an operational area.

1-127. Some threat information warfare capabilities, such as computer warfare and perception management, can reach far beyond the immediate operational area. A threat may perform strategic information warfare activities to create effects globally, including attacks on critical U.S. infrastructure, military deception, and perception management campaigns to influence public support. Refer to FM 3-53 for more information about military deception and perception management.

1-128. A threat may also conduct tactical maneuver to achieve information warfare objectives (such as influence or deception), rather than purely military ones. To some extent, managing, controlling, and disseminating information have always been critical to tactical success. This is especially true given the advances in information technology and U.S. reliance on network capabilities.

1-129. Threats recognize the advantages information warfare activities can provide their tactical commanders. Therefore, they strive to integrate information warfare planning and activities in all tactical missions and battles. Information warfare activities may degrade or deny U.S. communications and blur or manipulate the common operational picture. Information warfare may also help an enemy dictate the tempo of combat. By combining perception management, military deception, and EW, the enemy may be able to effectively slow or control the pace of battle. Traditional EW activities, such as jamming, also contribute to the tactical application of information warfare by disrupting U.S. command and control and challenging friendly forces' attempts to establish information advantage.

1-130. Threat information warfare also supports tactical counterreconnaissance. Threats constantly seek to attack, degrade, or manipulate U.S. intelligence, surveillance, reconnaissance, and security capabilities. Each U.S. and allied target acquisition system and sensor is a potential target.

1-131. Because threats integrate their information warfare capabilities, a coordinated and synchronized response is essential. The countermeasures to defend against these capabilities are a combination of signal, cyberspace operations, electromagnetic protection, space, counterreconnaissance, and other protection activities, along with intelligence and operations security support. Close collaboration between these elements ensures a more effective response. Refer to TC 7-100 for more information about hybrid threat and information warfare.

NON-STATE THREATS

1-132. Non-state cyber actors, including hacktivists and cyber criminals, pose a limited risk to tactical commanders. Hacktivists are often assessed to be nuisance threats, conducting unsophisticated distributed denial-of-service attacks and web page defacement. Organized crime or other non-state organizations often make sophisticated malware available for purchase or for free, allowing even unsophisticated threats to acquire advanced capabilities at little to no cost. U.S. forces may face a variety of non-state threats. Non-state cyber actors include—

- Criminal organizations.
- Insider threats.
- Violent extremist organizations.
- Cyber vigilantes.
- Individuals or small groups.

1-133. Non-state cyber actor disruption of operations in the information, human, and physical dimensions of an operational environment is a challenge for tactical commanders. A viral disinformation message released on social media can quickly galvanize local populations to side with threats, take up arms, riot, or exacerbate already volatile situations. Tactical commanders, already pressured by the situation on the ground, may have limited resources to deal with a viral story propagated by hostile groups. Military operations that impede criminal organizations, who might be connected to local political leaders, pose a significant challenge to engagements and force protection. Cybersecurity awareness, data literacy, and operations security are critical components to mitigating false narratives.

1-134. Non-state threats may attempt to discover personally identifiable information of U.S. participants. Spear phishing and watering holes attempt to lure unwitting victims to click links that download malware and corrupt U.S. networks. Non-state threats who gain network access may, in turn, sell that access to more sophisticated threats.

INSIDER THREAT

1-135. Insider threats present a significant risk to military operations. An *insider threat* is a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the department; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace (AR 381-12).

1-136. An insider threat does not necessarily need to be a military member or government employee. Third party vendors, contractors, and mission partners could pose a risk as well. The insider threat is especially dangerous because insider activity is generally the hardest to identify. Downloading or printing files to remove from secure areas may appear to be ordinary day-to-day activities. As with threat malicious cyberspace activity, a trusted insider can steal sensitive information to compromise operation plans, undermine partner relationships, or manipulate public opinion.

1-137. Past cases of insider threats have demonstrated that coworkers, associates, friends, and supervisors of those engaging in espionage or terrorist activity commonly overlook insider threat indicators. If these indicators had been reported and investigated, they might have minimized the damage to national security or saved the lives of U.S. personnel. The knowledge and participation of all Department of the Army personnel in threat awareness and reporting is essential to the success of the Army's warfighting mission and in protecting the lives of Soldiers. Army counterintelligence elements conduct aggressive and comprehensive investigations worldwide to detect, identify, exploit, and neutralize the foreign intelligence entity and insider threat to the Army and DOD. Refer to AR 381-12 for more information about the threat awareness and reporting program.

HAZARDS

1-138. Certain environmental hazards can significantly impact the electromagnetic spectrum, adversely affecting communications and other spectrum-dependent capabilities, including satellite-based positioning, navigation, and timing. These hazards include electromagnetic environmental effects, space weather phenomena, and environmental weather.

ELECTROMAGNETIC ENVIRONMENTAL EFFECTS

1-139. Various electromagnetic environmental effects impact the operational capability of military forces, equipment, systems, and platforms in the electromagnetic operational environment. Examples of electromagnetic environmental effects include—

- Electromagnetic compatibility.
- Electromagnetic interference.
- Electromagnetic pulse.
- Electromagnetic radiation hazards—
  - Hazards of electromagnetic radiation to personnel.
  - Hazards of electromagnetic radiation to ordnance.
  - Hazards of electromagnetic radiation to fuels.

- Space weather.

1-140. All spectrum-dependent devices are susceptible to electromagnetic environmental effects. When platforms, associated systems, and equipment (for example, avionics or ordnance) are exposed to an electromagnetic operational environment different from that for which they were designed and tested, the possibility of safety, interoperability, and reliability problems increases. A system is said to have an electromagnetic vulnerability if it is unable to perform its designated mission when exposed to a certain level of electromagnetic environmental effects. CEWOs must identify and quantify the possible impacts of electromagnetic environmental effects on operations.

Electromagnetic Compatibility

1-141. *Electromagnetic compatibility* is the ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response (JP 3-85). Spectrum manager adherence to the joint restricted frequency list will help ensure electromagnetic compatibility. Before units employ EW equipment, the CEWO conducts electromagnetic compatibility analysis to identify possible compatibility issues and ensure maximum usability of equipment.

Electromagnetic Interference

1-142. Electromagnetic interference to spectrum-dependent devices is a persistent, pervasive problem in military operations. Routine continued use of spectrum-dependent devices will inevitably result in electromagnetic interference affecting these devices. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment (JP 3-85). Electromagnetic interference may be either intentional or unintentional. Intentional sources of electromagnetic interference are threat electromagnetic attacks, including jamming, deception, and electromagnetic intrusion. Unintentional electromagnetic interference may be the result of—

- Friendly and threat use of the same frequencies.
- Other electronic, electrical, or electromechanical equipment, such as electric motors, power generators, and vehicle ignition systems.
- Atmospheric weather.
- Space weather.
- Equipment malfunction.

1-143. Electromagnetic interference requires mitigation action when it interferes with friendly use of the electromagnetic spectrum. Units incorporate techniques to identify, isolate, and mitigate electromagnetic interference. Techniques to resolve electromagnetic interference include—

- Moving equipment away from sources of electrical or electromechanical noise.
- Changing friendly frequencies as prescribed in the signal operating instructions or operation order.
- Implementing terrain masking techniques.
- Using directional antennas.
- Relocating transmitters and receivers.

Electromagnetic Pulse

1-144. An *electromagnetic pulse* is a strong burst of electromagnetic radiation caused by a nuclear explosion, energy weapon, or by natural phenomenon, that may couple with electrical or electronic systems to produce damaging current and voltage surges (JP 3-85). An electromagnetic pulse creates a permanent effect and destroys equipment, rendering it useless until maintainers repair or reconstitute the capability. An enemy can deliver electromagnetic pulse effects through either a high-altitude detonation of a nuclear weapon or using directed energy from an EW platform.

1-145. Hardened equipment, redundancy, passive techniques, and timely resupply can partially mitigate electromagnetic pulse effects. Electromagnetic pulse caused by a nuclear detonation introduces other survivability issues. Understanding electromagnetic pulse and its effects poses more defensive considerations than offensive. Commanders must be prepared to operate without digital systems if an enemy employs an

electromagnetic pulse weapon. Units at echelons theater army and below seeking to generate offensive electromagnetic pulse effects rely on strategic-level decisions and capabilities. Refer to FM 3-11 and ATP 3-72 for information about nuclear survivability.

Electromagnetic Radiation Hazards

1-146. High levels of electromagnetic radiation may create hazardous conditions. Throughout the planning process, the CEWO considers electromagnetic radiation hazards and advises the commander and staff on techniques to mitigate these hazards. The three categories of electromagnetic radiation hazards are—

- Hazards of electromagnetic radiation to personnel.
- Hazards of electromagnetic radiation to fuels.
- Hazards of electromagnetic radiation to ordnance.

Hazards of Electromagnetic Radiation to Personnel

1-147. Hazards of electromagnetic radiation to personnel is the danger to personnel from the absorption of electromagnetic energy by the human body. Personnel hazards are associated with the absorption of radio frequency energy above certain power levels in certain frequency bands for certain lengths of time. CEWOs evaluate risks make recommendations to mitigate hazards of electromagnetic radiation to personnel. Mitigation measures include establishing minimum safe distance from high power transmission systems, such as radars super high frequency and extremely high frequency satellite communications terminals, and electromagnetic jammers.

Hazards of Electromagnetic Radiation to Fuels

1-148. Hazards of electromagnetic radiation to fuels are associated with the possibility of igniting fuel or other volatile materials through radio frequency energy-induced arcs or sparks. It takes a certain amount of arc energy to ignite fuel. High powered transmission systems should not be operated near large stores of fuel, such as airfields, refueling points, and refueling on-the-move locations.

Hazards of Electromagnetic Radiation to Ordnance

1-149. Hazards of electromagnetic radiation to ordnance refers to the susceptibility of electro-explosive devices to radio frequency energy. Electro-explosive or electrically initiated devices are the control devices to detonate explosives, launch ejection seats, cut tow cables, or perform other similar functions. High power communications, EW, and radar transmitters can produce enough electromagnetic energy to trigger some of these devices. Planners should not locate communications, radar, or EW jamming sites near ammunition storage points.

SPACE WEATHER

1-150. Space weather disturbances can disrupt friendly, civil, commercial, and threat spectrum-dependent devices, including communications; radars; and satellite positioning, navigation, and timing. Most space weather events are predictable. Unit space staff officers, in collaboration with Air Force staff weather officers, provide space weather forecasts so units can prepare for disruptions and arrange backup means of communication. Space weather hazards include—

- Solar flares.
- Coronal mass ejections.
- Ionospheric scintillation.

Solar Flares

1-151. Solar flares cause interference with satellite communications, radar, and high frequency radio, causing shortwave fade. There is no mitigation for this effect; high frequency radio communication will be degraded until the solar flare dissipates. Solar flares may occur a few times per month to several times per day. In rare occasions, radio frequency interference from solar flares can significantly degrade operation of spectrum-dependent devices. The geomagnetic storms associated with solar flares can last from a few minutes to several hours, but the effects can linger in the Earth's magnetosphere and atmosphere for days to weeks.

Coronal Mass Ejections (Solar Radio Bursts)

1-152. When the magnetic field associated with a coronal mass ejection impacts the Earth's magnetic field, the resulting geomagnetic storm can last several days, with storm effects continuing 1–2 days more. The coronal mass ejection's electromagnetic energy disrupts the ionosphere's reflectivity, adversely impacting broadcast radio signal transmissions. In rare instances, a coronal mass ejection can damage power grids. This disruption can also affect satellite positioning, navigation, and timing signals, interfering with satellite-based guidance systems for long-range precision munitions, and the satellite timing reference used by communications systems.

Ionospheric Scintillation

1-153. Severe scintillation conditions can prevent a satellite positioning, navigation, and timing receiver from locking onto a satellite signal and can make it impossible to calculate a position. This causes similar positioning, navigation, and timing disruptions to those of coronal mass ejections. Ionospheric scintillation effects are more prevalent at low and high latitudes—far North and far South—and much less frequent at middle latitudes (such as the continental United States). These effects can last from a few minutes to several hours. Refer to FM 3-14 for more information about space weather phenomena.

Atmospheric Weather

1-154. The primary atmospheric weather source of electromagnetic interference is lightning. Lightning is formed by electrostatic discharge between two electrically charged regions, either both in the atmosphere or one in the atmosphere and one on the ground. Lightning releases an intense burst of electrical noise that can temporarily interfere with spectrum-dependent devices. Electromagnetic interference from lightning is easy to isolate, since it coincides with the natural phenomenon. This type of electromagnetic interference is normally of short duration and resolves when the electrical storm clears.

SECTION III – SYSTEMS ANALYSIS

1-155. The interactions among cyberspace, the electromagnetic spectrum, and other aspects of the physical environment create opportunities and vulnerabilities that may not be readily apparent. Targets that are otherwise secure in one domain may be directly or indirectly vulnerable through system interactions and dependencies in other domains. This section provides a high-level overview of systems analysis for the purpose of protection planning (friendly systems) or targeting (threat systems).

OVERVIEW

1-156. A *system* is a functionally, physically and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole (JP 3-0). Changes or effects on one element influence other elements as well as the output or function of the system. By analyzing systems, Army forces gain understanding of these interactions, their external dependencies, and their implications for military operations. The CEWO's systems analysis identifies mission-relevant terrain in cyberspace—those system dependencies that rely on cyberspace capabilities. Mission-relevant terrain in cyberspace may identify friendly capabilities to protect through mission thread defense (see paragraph 2-18) or threat capabilities to nominate during the targeting process (see chapter 4).

1-157. Commanders and staffs apply systems analysis during mission analysis, throughout operations, and outside of operations. Systems analysis is an iterative process used to assess both friendly and threat capabilities and inform protection planning and targeting. Given a targeted function or capability, staffs analyze the system used to perform the function so they can identify its critical characteristics. These characteristics can be targeted to cause indirect effects on the primary target.

Example Operational Application

Operational objective: Prevent the enemy reserve from affecting the main effort.

Targeted function or capability (system): The employment of the reserve.

Potential targets:
- Drawbridge controls along the route.
- Transmission and reception of the activation command.
- Navigation systems of the reserve force.
- Vehicle functioning or maintenance.

ANALYSIS PROCESS

1-158. Staffs may focus their analysis on a capability or function as an asset to protect or as a target for effect. This approach to systems analysis involves understanding the processes, dependencies, components, and interactions through which the system accomplishes its overall function. This requires analyzing all dimensions of the operational environment—the physical dimension with its technological underpinnings, the information dimension regarding the content of the interactions, and the human dimension with its associated organizational context.

1-159. During systems analysis, planners must consider the links between physical equipment (such as a radar, radio, or network device) and the capability it offers or the information it provides in the human dimension. This will assist in protection planning or targeting by ensuring both the system and its function are accounted for as options to shape the operational environment.

1-160. The analysis process reveals critical links, nodes, and additional systems that may be selected for protection or targeting to yield a desired effect through indirect or non-obvious approaches. Systems analysis is applicable when—
- There is a function, capability, or task to be affected or protected.
- The relevant system to accomplish the function uses or depends on cyberspace or the electromagnetic spectrum.
- Direct methods to affect the system do not exist or may impose excessive cost on an attacker.

1-161. The steps of the analysis process are—
- Define the system—task, function, capability, or mission—for analysis.
- Describe the functioning and implementation of the system.
- Assess the system's limitations and vulnerabilities.
- Refine.

DEFINE

1-162. During this step the staff identifies the task, function, capability, or mission being assessed and the process or activities through which it is accomplished. They identify how the major elements combine to perform the function. The define step includes enumerating the subtasks or actions that contribute to the function, the major actors—personnel, equipment, or subsystems—and the generalized inputs and outputs of each step. Critical to this step is understanding the overall process and its key aspects to focus subsequent analysis. The result of this step should be a high-level process diagram.

1-163. The define step identifies mission-relevant terrain in cyberspace as it relates to the task, function, capability, or mission the staff is analyzing. Mission-relevant terrain in cyberspace includes all devices, internal and external links, operating systems, services, applications, ports, protocols, hardware, and software on servers required to enable the function of a critical asset or the completion of a mission. Some mission-relevant terrain may exist external to DOD-controlled cyberspace. The define step also requires identifying the mission thread's reliance on spectrum-dependent capabilities.

DESCRIBE

1-164. The second step is to describe the implementation of the process. For each step in the targeted process, the staff identifies the actors and their tasks or purposes along with any objects of the actions or performance criteria. They identify how components interact, capturing where information flows between components and requirements such as those for timing, synchronization, or format. Throughout this step, the staff identifies any additional dependencies on external and shared resources or assumptions about the state of the system, such as available power, satellite connectivity, or electromagnetic spectrum access requirements.

ASSESS

1-165. The assess step identifies critical links and nodes and their interactions across domains and dimensions within the operational environment to gain a systems perspective. After defining the key components and describing the system interactions, staffs assess the system's limitations and vulnerabilities. The perspective in which a link or node is critical may differ from the domain in which it is most vulnerable or in which the ultimate effect is desired. For example, a communications site is critical for its function in cyberspace but is most vulnerable to a physical or electromagnetic attack. Weighted ranking based on a system's criticality, accessibility, recuperability, vulnerability, effect, and recognizability can be applied to friendly and hostile networks and systems analysis. The results of the assessment step may be sufficient to inform targeting or for incorporation into protection planning. Refer to ATP 2-33.4 for more details on weighted ranking analysis.

REFINE

1-166. The analysis process is iterative. Staffs continue to refine their analysis to account for a changing operational environment, to increase understanding, and to support requirements for increased levels of detail. The level of detail needed is often driven by requirements for target engagement and subsequent reassessment. This refinement includes performing further systems analyses of components of the system, accounting for redundancies or mitigations in the system, and adjusting for changing disposition of forces.

1-167. Systems are often composed of other systems. The analysis process can be applied to each layer of systems. Comprehensive, in-depth understanding requires significant analysis effort. Units focus their analysis on functions, systems, components, or a set of these associated with an operation plan. The determination of this focus comes from mission analysis and the commander's priorities.

OUTPUT

1-168. The output of the analysis process (see figure 1-3 on page 28) may include—

- Effects chains.
- Short-, medium-, and long-term approaches.
- Actions to target an element of the system in any or all domains or dimensions of the operational environment.
- Actions involving physical attacks on supporting components.
- Converged effects using a combination of lethal and nonlethal actions on multiple system components in different domains.
- Actions or effects outside the defined physical or organizational boundaries.

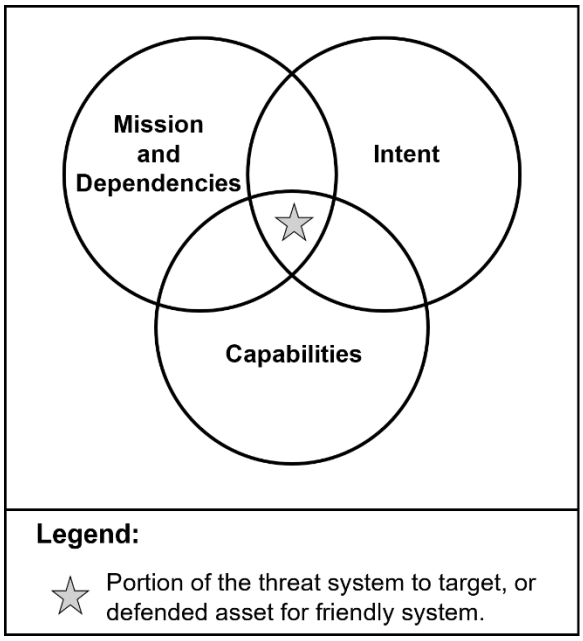


Figure 1-3. Output of mission analysis

Chapter 2
Cyberspace Operations

This chapter describes how different portions of cyberspace may be controlled and operated by different entities, with users relying on systems they neither control nor operate. It goes on to discuss how Army forces protect against threat use of cyberspace and preserve friendly ability to use it. The chapter concludes with an explanation of the conduct of operations against threats in and through cyberspace as well as in the air and land domains based on their reliance upon cyberspace.

JOINT AND ARMY NETWORKS

2-1. Cyberspace is a manmade domain. Its components are built and operated for certain purposes. Cyberspace includes enterprise and tactical networks, civilian cell phones, telecommunications infrastructure, other components of critical infrastructure, and weapon systems. Among other devices, as parts of cyberspace, information technology systems perform networking, information processing, and other tasks typically associated with home computers and the Internet. The DODIN comprises the entire portion of DOD cyberspace.

DEPARTMENT OF DEFENSE INFORMATION NETWORK

2-2. The *Department of Defense information network* is the set of information capabilities and associated processes owned or leased by the Department of Defense for collecting, processing, storing, disseminating, and managing information, whether interconnected or stand-alone (JP 6-0). The DODIN includes common enterprise service networks, intelligence networks operated by the DOD components, stand-alone mission and weapon systems, other special-purpose networks, DOD-owned smartphones, radio frequency identification tags, industrial control systems, isolated laboratory networks, and platform information technology operated by or on behalf of the DOD components.

2-3. The DODIN interacts with and provides connections to national and global cyberspace. The DODIN encompasses the Service-specific enclaves of the Army, Navy, Air Force, Marine Corps, and Space Force combined with joint capabilities provided by the Defense Information Systems Agency. The DODIN provides access to Defense Information Systems Network services, including SECRET Internet Protocol Router Network, Nonclassified Internet Protocol Router Network, and classified mission partner networks.

DEPARTMENT OF DEFENSE INFORMATION NETWORK-ARMY

2-4. The *Department of Defense information network-Army* (DODIN-A) is an Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide (ATP 6-02.71). The DODIN-A includes all Army automated information systems and networks, including stand-alone networks supporting intelligence, sustainment, medical, Army National Guard, and United States Army Reserve.

SIGNAL SUPPORT

2-5. Signal units have effectively integrated communications capabilities across the air, land, maritime, space, and cyberspace domains for decades. The DODIN-A and the services it extends enable collaboration and synchronization across domains and among mission partners. Signal support is a key enabler for Army operations. Signal Soldiers install, operate, maintain, and secure the DODIN-A in locations where both friendly and threat cyberspace operations occur.

2-6. Given the high risk to the network, signal operators and information system users must continuously manage risk and secure their respective portions of the DODIN-A. Signal planners and cybersecurity personnel assess cybersecurity risk during network design, mitigate risk in software employment, and continuously monitor for signs of malicious activity within the network. Individual users must maintain cybersecurity awareness and learn to identify signs of malicious cyberspace activity. While cybersecurity efforts cannot prevent every intrusion, commanders and their staffs must take steps to identify, prioritize, and

secure their most important networks and data. See appendix D for more information about recognizing and responding to malicious cyberspace activity. Refer to FM 6-02 and ATP 6-02.71 for more information about signal support and DODIN operations in Army networks.

CYBERSPACE DEFENSE

2-7. *Cyberspace defense* is actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures (JP 3-12). Cyberspace defense includes actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. Cyberspace defense is a shared mission between cyberspace defense forces, local network defenders, and cybersecurity service providers.

DEFENSIVE CYBERSPACE OPERATIONS

2-8. *Defensive cyberspace operations* are missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity (JP 3-12). Corps, division, and brigade commanders can gain important tactical advantages through cyberspace if they understand the nature and potential of the cyberspace domain. During planning, the CEMA section identifies mission-relevant terrain in cyberspace to support both targeting and protection planning. Assets identified as friendly mission-relevant terrain in cyberspace contribute to the critical asset list and the defended asset list.

Note. Joint doctrine for cyberspace operations makes use of the colloquial terms blue, gray, and red cyberspace. The Army refers to these portions of cyberspace respectively as friendly, neutral, and threat cyberspace.

2-9. Networks inherently make it difficult to detect and identify malicious activity where the avenues of approach are wide. Furthermore, threat forces move at the speed of the network. Defense involves building or changing the terrain, consolidating information, and restricting routes. Developing named areas of interest and target areas of interest in terms of system nodes and links (which may include temporary denial to friendly systems) is necessary for effective cyberspace defense. Further necessary actions include vulnerability assessments to understand the attack surface and threat avenues of approach and inform defensive planning. Because many cyberspace nodes exist in other domains (primarily land and space), defending friendly cyberspace requires active defense in other domains. Because many capabilities in the air, land, maritime, and space domains depend on cyberspace, those capabilities require cyberspace defense as well as defense in their respective physical domains.

2-10. Defensive cyberspace operations are further categorized based on mission, intent, and the location of the actions in cyberspace as—

- Defensive cyberspace operations-internal defensive measures.
- Defensive cyberspace operations-response actions.

Defensive Cyberspace Operations-Internal Defensive Measures

2-11. *Defensive cyberspace operations-internal defensive measures* are a defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace (JP 3-12). The defended portion of cyberspace for the Army is typically considered to be the DODIN-A, which provides classified and nonclassified voice, data, and video connectivity and is a network extending from the strategic level to as low as individual Soldiers.

2-12. At the brigade, commanders are primarily concerned with cybersecurity activities to harden their respective portions of the network and ensure the general confidentiality, integrity, and availability of command and control information systems. These actions are informed by configuration guides, best practices, and general knowledge of cyberspace vulnerabilities, agnostic of threat activities or tactics, techniques, and procedures. In the event of suspected malicious cyberspace activity affecting brigade assets, personnel are expected to report these activities in accordance with the unit standard operating procedure (SOP) for remediation by local network defenders or higher headquarters. See appendix A for cyber incident reporting procedures.

2-13. The division secures and defends its portion of the network and provides defensive cyberspace operations support to subordinate brigade combat teams. For example, the division cyber team may have intelligence indicating a threat is targeting the unit and take steps to counter the indicated activity.

2-14. At the corps, the CEWO and CEMA section maintain direct dialog with the joint cyberspace center and Joint Force Headquarters-Cyber as required to track requests for cyberspace effects and to enable shared understanding of designated cyberspace.

Defensive Cyberspace Operations-Response Actions

2-15. *Defensive cyberspace operations-response actions* are a defensive cyberspace operations mission executed external to the defended network or portion of cyberspace without the permission of the owner of the affected system (JP 3-12). Defensive cyberspace operations-response actions consist of the same cyberspace actions as offensive cyberspace operations (cyberspace exploitation and cyberspace attack) but are undertaken for defensive purposes to prevent a threat from conducting malicious cyberspace activity against friendly networks. Defensive cyberspace operations-response actions missions are undertaken by cyber mission forces under USCYBERCOM authorities and rules of engagement.

Cyberspace Defense Missions and Functions

2-16. The combatant command, Service, or DOD agency that provides or operates the network is generally authorized to take steps to harden their portion of the network and manage risk. These organizations take cyberspace defense actions except in cases where those actions would negatively impact networks or systems outside of their responsibility. Cyber protection teams may reinforce local network defenders to undertake cyberspace defense actions. DOD Cyber Defense Command directs and synchronizes all defensive actions that impact more than one combatant command or have impacts outside the responsibility of the network owner.

Analytic Support to Defensive Cyberspace Operations

2-17. Analytic support enables the movement, processing, and analysis of data to build real-time network situational understanding and enhance cyberspace defense. Data analytics are an essential function for defensive cyberspace operations. Analytics provide the means to understand the cyberspace environment and to detect and characterize threat cyberspace activity. Refer to TC 3-12.2.4.1 for more information about analytic support to defensive cyberspace operations.

Mission Thread Defense

2-18. In DOD usage, mission thread refers to a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities. The mission thread includes all tasks to carry out a mission and satisfy a defined objective. Threads define the task execution sequence in a chain of events of how systems, people, data, methods, tactics, timing, and interfaces interact to complete necessary tasks to achieve a mission objective. Examples of mission threads include kill chains (lethal) or effects chains (nonlethal). Mission thread defense is a change from traditional point defenses in cyberspace that failed to account for mission, network, and data interdependencies. Defensive cyber forces conduct mission thread analysis (systems analysis) as described in chapter 1 to identify the critical capabilities and dependencies for a mission thread, identify defended assets, and plan appropriate defenses. Refer to TC 3-12.2.90 for more information about mission thread defense.

Hunt Operations

2-19. Defensive cyber forces conduct hunt operations with the assumption that threats may already be present in friendly networks and may have the initiative. Depending on operational objectives, hunt operations may be analogous to reconnaissance, counterreconnaissance, or movement to contact in the air, land, or maritime domain as cyber defenders seek to answer reconnaissance objectives, counter threat presence, or establish contact with the threat. Refer to TC 3-12.2.98 for more information about hunt operations.

Hunt Forward Operations in Ukraine

U.S. joint forces, in close cooperation with the government of Ukraine, conducted defensive cyberspace operations alongside Ukrainian Cyber Command personnel from December 2021 to March 2022 as part of a wider effort to enhance the cyber resiliency of critical Ukrainian national networks.

In late 2021, with the consent of Ukraine, USCYBERCOM deployed its largest hunt forward team yet. The joint team of Navy and Marine Corps cyber operators hunted for malicious cyberspace activity on Ukrainian networks. The operation persisted until days before Russian forces launched a wide-scale invasion of the nation.

The Ukrainian government provided the hunt forward teams with access to multiple networks. Sitting side-by-side, Ukrainian and U.S. cyber professionals began a meticulous, multi-pronged hunt looking for suspected malicious cyberspace activity. This mission postured Ukrainian cyber professionals to identify and address vulnerabilities on their networks and mitigate them in order of severity.

CYBERSPACE OFFENSE

2-20. *Offensive cyberspace operations* are missions intended to project power in and through cyberspace (JP 3-12). Offensive cyberspace operations missions are executed by direction of Commander, USCYBERCOM to support combatant commander objectives or other national security objectives.

2-21. Cyber mission forces conduct offensive cyberspace operations outside of DOD networks by conducting cyberspace surveillance and reconnaissance and cyberspace effects operations to expose threat infrastructure to risk in support of a commander's objectives. Commanders must integrate offensive cyberspace operations planning throughout the operations process to support the combined arms scheme of maneuver.

2-22. The Army provides cyber forces to the joint force, trained to perform offensive cyberspace operations across the competition continuum. Cyber mission forces may conduct offensive cyberspace operations to support commanders at echelons corps and below through the joint targeting process in response to requests for support. Targets identified for cyberspace effects require extended planning time, target development, extended approval time, synchronization, and deconfliction with other mission partners. See chapter 4 for a detailed discussion of targeting considerations in cyberspace.

CYBERSPACE SURVEILLANCE AND RECONNAISSANCE

2-23. Cyberspace surveillance and reconnaissance is a cyberspace exploitation action conducted on behalf of the joint force commander, authorized by an execute order and conducted by a military cyber unit that has been given direct support authority by Commander, USCYBERCOM. Cyberspace surveillance and reconnaissance includes activities in cyberspace conducted to gather information required to support planning and execution of current and future offensive cyberspace operations. Cyberspace surveillance and reconnaissance focuses on tactical and operational information and on identifying and mapping threat cyberspace to support planning. Army units conducting cyberspace surveillance and reconnaissance operate as part of the joint force supporting cyberspace operations missions.

CYBERSPACE EXPLOITATION

2-24. Cyberspace exploitation requires forces trained to a standard that prevents compromise of related operations. Cyberspace exploitation is conducted pursuant to military authorities and must be coordinated and deconflicted with other U.S. Government departments and agencies. Cyberspace exploitation actions include—

- Access creation.
- Intelligence activities.
- Maneuver.

- Information collection.
- Other enabling actions required to prepare for future military operations.

2-25. Cyberspace exploitation includes actions to gain and maintain cyberspace superiority and support intelligence preparation of the operational environment for current and future operations through activities such as—

- Gaining and maintaining unauthorized access to threat networks, systems, and nodes of military value.
- Maneuvering to positions of advantage.
- Positioning cyberspace capabilities to enable follow-on actions, such as a cyberspace attack.

2-26. Cyberspace exploitation supports current and future operations through collection of information, including—

- Mapping threat and neutral cyberspace to develop situational understanding.
- Discovering threat cyberspace vulnerabilities.
- Enabling—
  - Joint intelligence preparation of the operational environment.
  - Threat warning.
  - Joint target development.
- Supporting the planning, execution, and assessment of military operations throughout the operational environment.

CYBERSPACE ATTACK

2-27. *Cyberspace attack* consists of actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires (JP 3-12). Cyberspace attack may be conducted for offensive cyberspace operations (see paragraph 2-20) or defensive cyberspace operations-response actions (see paragraph 2-15).

2-28. Cyberspace attack actions may limit a threat's ability to use cyberspace to harm the United States and its allies. For example, a cyberspace attack that targets a threat's critical infrastructure to disrupt their ability to exercise command and control over hostile forces and deny the transfer of information residing on, or in transit between, computers or mobile devices.

2-29. Cyberspace attacks provide commanders a way to degrade, disrupt, or destroy the threat's freedom of action in cyberspace. Preserving friendly freedom of action through cyberspace defense while denying the same to threats through cyberspace attack offers commanders an operational advantage.

2-30. The Army provides forces trained to conduct offensive cyberspace operations. Cyber mission forces may only conduct offensive cyberspace operations when delegated the appropriate authorities by the combatant command and USCYBERCOM.

2-31. Cyberspace operations can create both lethal and nonlethal effects. It is important for commanders to understand offensive cyberspace operations can create desired effects from the strategic level (influence and deterrence) to the tactical level (disruption or destruction of a threat capability), destroying or otherwise denying the threat's ability to tactically maneuver. The requesting unit submits a cyber effects request format (CERF) to their higher headquarters articulating the desired effect along with other coordinating instructions. When the CERF reaches the joint force headquarters, the cyberspace operations integrated planning element further develops the target through the joint targeting cycle and enters a request for service in the USCYBERCOM request for service portal. If offensive cyberspace operations support is approved, the capabilities used to produce the desired effects must be resourced by the higher headquarters or national-level cyber forces.

2-32. Cyberspace attacks are conducted by joint force commanders with the mission and authority to create offensive effects in or through cyberspace after having deconflicted them with Commander, USCYBERCOM. Targeting for cyberspace generally follows the processes and procedures used for traditional targeting but must account for the unique nature of cyberspace as compared to the air, land, maritime, and space domains and the unique requirements for matching cyberspace capabilities to targets in cyberspace. Combatant command staffs develop targets according to combatant commander priorities and

forward them to USCYBERCOM for validation and possible action. Refer to JP 3-12 for more information about joint targeting in cyberspace.

Cyberspace Offense at Battalion and Below

2-33. Effects in cyberspace at echelons battalion and below are likely to be delivered by available lethal and nonlethal fires capabilities. Offensive cyberspace operations support is unlikely to be approved and resourced at these echelons. The commander's targeting guidance describes the desired effects to be generated by lethal fires, maneuver, cyberspace attack, electromagnetic attack, or other nonlethal capability. Targeting enables the commander to leverage lethal and nonlethal attack capabilities (within fire control measures) to produce the desired effects in support of operations. If the scheme of maneuver requires effects in cyberspace, the commander either engages the target with organic lethal or nonlethal fires capabilities or requests this support from higher echelons through the brigade combat team. If the brigade combat team, division, or corps cannot meet the battalion's support requirements, the support may be provided by joint, theater, or national-level assets. See chapter 4 for more information about targeting in cyberspace and appendix C for instructions for the CERF.

Chapter 3
Electromagnetic Warfare

This chapter introduces electromagnetic warfare and the divisions of electromagnetic warfare. It goes on to discuss the application of electromagnetic attack, electromagnetic protection, electromagnetic support, and electromagnetic reprogramming in Army operations. The chapter then addresses the synchronization of electromagnetic warfare with complementary signals intelligence capabilities. The chapter concludes with a description of organic electromagnetic warfare forces at echelons corps and below.

INTRODUCTION

3-1. Since the beginning of the 20th century, EW has played an ever-increasing role in shaping the outcomes of various military conflicts around the globe. *Electromagnetic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-85). The divisions of EW are—

- Electromagnetic attack.
- Electromagnetic protection.
- Electromagnetic support.

3-2. Electromagnetic warfare reprogramming is a separate function of EW. While not classified as a division of EW, electromagnetic warfare reprogramming supports electromagnetic attack, electromagnetic protection, and electromagnetic support.

ELECTROMAGNETIC ATTACK

3-3. *Electromagnetic attack* is the division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). Electromagnetic attack methods include—

- Electromagnetic countermeasures.
- Electromagnetic deception.
- Electromagnetic intrusion.
- Electromagnetic jamming.
- Electromagnetic probing.

3-4. Defensive electromagnetic attack protects friendly personnel and equipment by degrading the threat's ability to employ weapons that use radio frequency-activated triggers. Defensive electromagnetic attack measures include radar jammers, counter-unmanned aircraft systems, and counter radio-controlled improvised explosive device electromagnetic warfare systems.

ELECTROMAGNETIC COUNTERMEASURES

3-5. The Army uses electromagnetic countermeasures to mitigate threat EW sensing and attack activities. Countermeasures can be active or passive and used preemptively or reactively. Countermeasure devices and techniques include infrared flares, chaff, radar jammers, counter radio-controlled improvised explosive device electromagnetic warfare systems, and decoys. The devices and defensive techniques are permissible without restrictions since they serve as protection and are responses to enemy engagements.

ELECTROMAGNETIC DECEPTION

3-6. Electromagnetic deception involves radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy to convey misleading information to a threat or to threat spectrum-dependent devices, thereby degrading or neutralizing the threat's capability. Deception in an EW context presents enemy operators and higher-level processing functions erroneous inputs, either directly

through the sensors or through spectrum-dependent network capabilities, such as voice communications or data links.

> ***Note.*** Electromagnetic deception should not be confused or conflated with military information support operations or military deception, which are often used to present false messages to high-level threat decision makers. The distinction is important because the required legal authorities governing electromagnetic attack differ from those governing military information support operations or military deception.

3-7. EW supports both strategic and tactical deception, using electromagnetic means and scaling appropriately for the desired effect. Electromagnetic deception can increase or decrease ambiguity, affecting the situational understanding of threat decision makers. Deception measures can indicate to a threat commander the certainty of a course of action or create sufficient confusion to disrupt decision making. When planning electromagnetic deception, EW planners consider activities that support the current friendly operation, as well as those that will support the deception mission, integration, and deconfliction.

3-8. Electromagnetic deception techniques support information advantage. The G-3 staff (specifically the G-39) develops plans and supervises deception missions. The CEWO prepares the EW portion of the deception plan. Integration of electromagnetic deception with other information activities is necessary when conducting deception missions. Time is a critical factor in deception planning. The more extensive the deception, the greater the planning and coordination effort required. Regardless of the duration, the longer the deception goes on, the more unintended effects may occur.

3-9. Planners should consider that each spectrum-dependent device exhibits a unique electromagnetic signature. Electromagnetic deception must present realistic decoy signatures to threat sensors. The intent of electromagnetic deception is to cause the threat to draw incorrect conclusions about friendly locations and activities. The three types of electromagnetic deception are—

- Simulative.
- Manipulative.
- Imitative.

Simulative

3-10. Simulative electromagnetic deception attempts to represent friendly notional or actual capabilities to mislead threat forces. Simulative deception requires extensive command and staff collaboration to present a believable deception plan. What the threat detects electronically should be consistent with other information sources. That is, a threat is more likely to be deceived by simulative techniques if the signals they detect are consistent with what they expect. Simulative electromagnetic deception transmissions require close attention.

Manipulative

3-11. Manipulative electromagnetic deception seeks to convey misleading indicators of friendly intentions. Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit will attack when it is really planning to withdraw, the unit might transmit false plans and requests for ammunition. Units use manipulative electromagnetic deception to mislead the enemy to misdirect their electromagnetic attack and electromagnetic support assets, while interfering less with friendly communications.

Imitative

3-12. Imitative deception mimics threat emissions with the intent to mislead them. Imitative electromagnetic deception, if recognized by the enemy, can compromise friendly SIGINT efforts. Imitative deception normally requires approval from higher-echelon commands.

3-13. An example of imitative electromagnetic deception includes entering the threat's communication nets by using their call signs and radio procedures and giving threat commanders instructions to initiate actions that are advantageous to friendly forces. Refer to ATP 3-12.3 for more information about electromagnetic deception techniques.

ELECTROMAGNETIC INTRUSION

3-14. *Electromagnetic intrusion* is the intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion (JP 3-85). Electromagnetic intrusion techniques are discrete and tailored to specific target systems, as opposed to more broad techniques such as spot, sweep, or barrage jamming. An example of electromagnetic intrusion would be radio transmissions simulating air traffic control communications and giving false instructions to a pilot.

ELECTROMAGNETIC JAMMING

3-15. *Electromagnetic jamming* is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability (JP 3-85). CEWOs direct the use of jamming techniques to disrupt the threat's ability to effectively receive or process electromagnetic signals.

3-16. Successful jamming requires understanding available jamming techniques and overpowering threat receivers with higher-power transmissions. The primary effects of jamming persist as long as the jammer is within range of the target and emitting. Jamming effects may be observable through threat actions during or following an electromagnetic jamming attack. Jamming techniques include—

- Standoff jamming.
- Escort jamming.
- Spot jamming.
- Barrage jamming.
- Sweep jamming.
- Follower jamming.

3-17. Depending on mission objectives, the different jamming techniques each have certain advantages and disadvantages. The CEWO advises commanders of the available jamming techniques and the benefits and risks of each technique. Ultimately the commander assumes an acceptable level of risk to achieve mission objectives. All jamming techniques can interfere with friendly systems if not used properly. If targeted threat systems operate in frequencies near those in use by friendly forces, some level of degraded friendly capabilities is possible. The CEMA spectrum manager deconflicts frequencies used for jamming with the G-6 or S-6 spectrum manager to minimize the risk of degraded friendly capabilities. The relatively high radio frequency power used for electromagnetic jamming puts EW teams at risk of threat geolocation and lethal fires.

Standoff Jamming

3-18. A standoff jamming mission projects from a protected location within an assigned area. Due to the distance involved, standoff jamming requires high power and large antennas to reach threat positions. This jamming technique requires precise technical information about threat frequencies and receiver locations to maximize jamming effects.

Advantages

3-19. Standoff jamming affords maximum protection for EW professionals and the systems they deploy from threat actions. It also creates windows of opportunity for Army and joint forces to conduct maneuver.

Disadvantages

3-20. Standoff jamming allows an enemy to identify, geolocate, and target the jammer through radio frequency direction finding. The greater the distance between the jamming site and the enemy, the greater the likelihood the attack will unintentionally interfere with friendly systems. This is colloquially referred to as frequency fratricide.

Escort Jamming

3-21. Escort jamming is a defensive electromagnetic attack that protects maneuver forces from threat weapons systems that use radio frequency triggers. Escort jamming uses a jamming platform that

accompanies maneuver forces to implement electromagnetic countermeasures, such as counter radio-controlled improvised explosive device electromagnetic warfare. Escort jamming requires precise intelligence regarding threat frequency use. Escort jamming usually does not require the same level of power or large antennas as standoff jamming. Depending on the mission, escort jamming does not necessarily require EW Soldiers to operate the equipment performing this mission. EW personnel perform pre-combat checks to verify programming and operation of the equipment which can be operated by general-purpose users.

Advantages

3-22. Escort jamming is highly mobile and has low vehicle power requirements. Escort jammers can use similar vehicle configurations of maneuver vehicles to screen them from visual identification.

Disadvantages

3-23. Escort jamming capabilities are typically employed during tactical movement, increasing the likelihood of attack. While some escort jammers can be carried on foot (dismounted), the usability of dismounted escort jamming systems is limited due to high battery consumption.

Spot Jamming

3-24. Spot jamming is a technique to jam a discrete frequency. Spot jamming is the least intrusive form of electromagnetic jamming, as it does not jam adjacent, untargeted frequencies. To plan spot jamming, the CEWO needs accurate intelligence regarding the targeted threat system's characteristics, such as frequency, transmit and receive power, and the antenna height and type.

Advantages

3-25. Spot jamming achieves a high jamming-to-signal ratio because it concentrates the available transmit power on the targeted frequency, so threats are unlikely to overcome the jamming without changing to another frequency.

Disadvantages

3-26. Spot jammers are not effective for agile frequency transmission, such as frequency hopping radios. Frequency hopping radios do not use a discrete frequency but change frequency continually across a relatively wide frequency range.

Barrage Jamming

3-27. Barrage jamming is the jamming of all frequencies within a specified portion of the electromagnetic spectrum at the same time. Barrage jamming techniques apply less power to each jammed frequency because the power spans the targeted frequency range.

Advantages

3-28. Multiple frequencies can be targeted by a single jammer simultaneously.

Disadvantages

3-29. Barrage jamming achieves a lower jamming-to-signal ratio than spot or sweep jamming, because the available transmit power is spread over a wider bandwidth. Barrage jamming generally requires the electromagnetic attack platform to be closer to the targeted receivers; this increases the likelihood of detection and geolocation by the threat. Barrage jammers require high radio frequency power to affect a broad frequency range.

Sweep Jamming

3-30. Sweep jamming is the jamming of a specified portion of the electromagnetic spectrum by sweeping a defined frequency range at a predetermined rate. Sweep jamming may use less transmit power than barrage jamming but gives a higher jamming-to-signal ratio because the jamming power is spread over a narrower bandwidth at any given time as with spot jamming. Sweep jamming may be the most appropriate technique when the electromagnetic order of battle provides a frequency range but not the precise frequency in use.

Advantages

3-31. Sweep jamming will allow the electromagnetic attack asset to operate further from the intended target than barrage jamming.

Disadvantages

3-32. The greater the distance between the jamming site and the enemy, the greater the likelihood the jamming will interfere with friendly systems (frequency fratricide).

Follower Jamming

3-33. Follower jamming is a form of electromagnetic attack to target receivers automatically when the system detects a threat transmission. Follower jamming remains passive until a targeted transmitter emits a signal. Follower jamming uses a combination of spot, barrage, and sweep jamming techniques; this is useful against frequency hopping receivers. EW professionals program the jammer to attack either a discrete frequency or a range of frequencies. The G-2 or S-2 compiles the electromagnetic order of battle and determines the frequencies employed by the threat and when a particular type of emitter is being used by the threat. The electromagnetic order of battle feeds the cyberspace and EW running estimate. The G-2 or S-2, G-6 or S-6, and the CEWO track the electromagnetic order of battle in their running estimates and update it as needed. The CEWO clarifies and expands the electromagnetic order of battle before briefing during course of action comparison.

Advantages

3-34. Because the jamming system does not continuously transmit, the follower jamming technique allows a jammer to maximize its resources against a target while minimizing the threat's ability to sense and geolocate the jammer.

Disadvantages

3-35. Sometimes the threat's capability is too agile and the jamming system response too slow. If the threat system is too sophisticated, it can outpace the follower jammer's responsiveness and render the jamming ineffective.

Electromagnetic Probing

3-36. *Electromagnetic probing* is intentional radiation designed to be introduced into the devices or systems of an adversary for the purpose of learning the functions and operational capabilities of the devices or systems (JP 3-85). Electromagnetic probing aims to penetrate and exploit threat systems and operations. Division and below units do not typically have organic electromagnetic probing capabilities. Units can request electromagnetic probing effects by submitting an electromagnetic attack request format through their higher echelon CEMA section. See appendix C for instructions for submitting the electromagnetic attack request format.

ELECTROMAGNETIC PROTECTION

3-37. *Electromagnetic protection* is the division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). Electromagnetic protection is a preemptive and constant function where the CEWO introduces operational approaches and plans to ensure the unit is prepared to defend spectrum-dependent devices from threat actions. Not all units have

electromagnetic attack or electromagnetic support capabilities. However, all units are required to train and maintain readiness for electromagnetic protection. While not part of electromagnetic protection, spectrum management operations support all electromagnetic protection actions. Electromagnetic protection actions include—

- EMCON.
- Electromagnetic masking.
- Electromagnetic compatibility.
- Electromagnetic hardening.
- Wartime reserve modes.

EMISSION CONTROL

3-38. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan (JP 3-85). EMCON reduces the likelihood of detection by threat sensors and direction-finding systems and helps conceal the locations of friendly forces.

3-39. The CEWO advises the G-6 or S-6 in developing communication plans that provide a low probability of threat detection of friendly communications. This can be accomplished by attempting to hide the unit's communications in plain sight—blending into the background electromagnetic environment. A common analogy for this is hiding a needle in a haystack, but hiding a needle in a haystack may not be effective if the threat has a metal detector. Perhaps the more appropriate analogy is hiding a needle in a stack of needles. The more a unit's use of the electromagnetic spectrum parallels what is already used by local governments and civilian populations in the operational area, the more difficult it is for a threat to identify and locate friendly emissions.

3-40. An EMCON plan contributes to a reduced electromagnetic signature by providing progressively more restrictive measures to limit electromagnetic emissions based on the tactical situation and threat. At the least restrictive EMCON condition (EMCON 1 [green]), operation of all spectrum-dependent devices continues with basic security precautions. At the highest threat level (EMCON 5 [black]), units remove most electromagnetic emitters from operation until the tactical situation allows return to a less restrictive EMCON condition. Units should exercise the established EMCON plan, including transitions between EMCON conditions, during all unit training and exercises to ensure they know the correct procedures and can transition between EMCON conditions quickly. Table 3-1 on page 41 summarizes EMCON conditions.

Table 3-1. Emission control conditions

EMCON Condition	*Description*
EMCON 1 Green	Describes a situation where there is no apparent hostile activity against friendly emitter operations. *Operational performance of all spectrum-dependent devices is monitored; password and encryption systems provide a layer of protection.*
EMCON 2 Yellow	Describes an increased risk of attack after detection. *Increased monitoring of all EMS activities is mandated. End users ensure their systems are secure, encrypted, power levels monitored, and transmissions limited. EMS use may be restricted to certain emitters. Rehearsal for elevated EMCON conditions is recommended.*
EMCON 3 Amber	Describes when a risk has been identified. *Encryption, frequency hop, and directional antennas on important systems are a priority; the CEWO's alertness is increased. All unencrypted systems are disconnected.*
EMCON 4 Red	Describes when an attack has taken place, but the EMCON system is not at its highest alertness. *Non-essential emitters may be taken offline; alternate or contingency means of communication may be implemented; and modifications are made to standard lower EMCON conditions (power levels and antenna types).*
EMCON 5 Black	Describes when attacks are taking place. *The most restrictive electromagnetic protection methods are enforced. Any compromised systems are isolated from the rest of the network.*
Legend:	
CEWO	cyber electromagnetic warfare officer
EMCON	emission control
EMS	electromagnetic spectrum

3-41. Commanders should consider EMCON 3 (amber) as the baseline for operations in the field. Units should routinely execute transitions to EMCON 4 (red) and EMCON 5 (black) during training exercises and armed conflict. Commanders, assisted by the CEWO, should carefully evaluate the minimum required capabilities to support operations during more restrictive EMCON conditions and discontinue use of unnecessary systems. Some methods to limit emissions during restrictive EMCON conditions include—

- Implementing radio silence—trusting in the disciplined initiative of subordinate leaders within the commander's intent under the mission command approach.
- Disconnecting certain emitters (such as blue force tracking).
- Employing wire, runners, couriers, and liaison officers to deliver messages instead of transmitting over radios.

3-42. The most basic EMCON measure to prevent threat detection is good radio discipline. Radio discipline involves—

- Reducing transmitter power.
- Radio antenna placement.
- Antenna masking and shielding.
- Minimizing how often radios emit a signal.
- Reducing transmission times (short messages and brevity codes).
- Using directional antennas, when available.

3-43. Techniques to minimize transmissions include—

- Transmitting only when necessary.
- Preplanning messages before transmitting them.
- Transmitting quickly and precisely using equipment capable of data burst transmission.
- Alternate means of communication.

Note. Refer to ATP 6-02.53 for techniques to minimize transmissions and ATP 1-02.1 for brevity codes.

ELECTROMAGNETIC MASKING

3-44. *Electromagnetic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-85). Electromagnetic masking disguises, distorts, or manipulates friendly electromagnetic radiation to conceal critical information or present false perceptions to threat commanders. Electromagnetic masking is an essential component of military deception, operations security, and signals security. Electromagnetic masking techniques include terrain masking and camouflage net masking.

Terrain Masking

3-45. Transmitters placed on hilltops, mountaintops, or buildings are vulnerable to threat direction-finding and jamming. Known transmitter locations allow a threat to jam the receivers, listen to transmissions, collect information such as friendly battle rhythm and duration of friendly transmissions, or attack using lethal fires. To mitigate these vulnerabilities, the CEWO and the G-6 or S-6 advise the commander and staff on optimal site selection to implement terrain masking. System operators implement terrain masking by placing antennas on the side of a mountain, hill, or building to place the terrain between friendly emitters and threat formations and optimize friendly use of the antenna while preventing threat detection and exploitation. Terrain masking for command posts and communications sites requires close coordination with the G-6 or S-6. Using terrain to mask maneuver formations' emissions requires further coordination with the G-3 or S-3 when selecting movement routes.

Camouflage Net Masking

3-46. Units use radio frequency reflective camouflage material to cover communications assemblages and power generators. While it is difficult to visually conceal large communications assemblages, radar reflective camouflage netting is an effective means of blocking stray electromagnetic radiation from directional antennas. Camouflage netting placed to the sides and back of a line of sight or satellite communications antenna ensures only the main beam of the antenna radiates a detectable signal. The CEWO and G-6 or S-6 planners consider minimum safe distance from line of sight and satellite communications transmitters when planning for camouflage net masking to minimize radio frequency interference and mitigate hazards of electromagnetic radiation to personnel (see chapter 1).

ELECTROMAGNETIC HARDENING

3-47. *Electromagnetic hardening* is action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-85). The CEWO and the G-6 or S-6 mutually develop SOPs and inspect the configurations of unit equipment, such as the proper grounding of communications assemblages, serviceability of cable shielding, and adequacy of cable connectivity. These actions protect friendly communications and noncommunications emitters from threat identification, lethal and nonlethal attack, and exploitation.

WARTIME RESERVE MODES

3-48. *Wartime reserve modes* 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 (JP 3-85). Threats search for available information that reveals friendly EW vulnerabilities, such as technical articles, magazines, news programs, and web pages that are available on the public Internet to develop and test EW measures. The Army prevents public access to wartime reserve modes and, as the term suggests, holds them in reserve strictly for wartime use so threats cannot preplan exploits to overcome the friendly capability.

ELECTROMAGNETIC SUPPORT

3-49. *Electromagnetic support* is the division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations (JP 3-85). Electromagnetic support gathers information about friendly and threat electromagnetic emissions to support the commander's situational understanding and decision making. Both EW and SIGINT elements may perform electromagnetic sensing to characterize friendly and threat electromagnetic emissions. SIGINT forces do not further process electromagnetic support data on friendly emissions into intelligence products. Understanding friendly electromagnetic signatures helps commanders and CEMA staff plan electromagnetic protection measures to protect friendly personnel and systems. Understanding threat capabilities and locations helps commanders plan operations, manage operational risk, and seize the initiative.

3-50. The information gathered through electromagnetic support enables threat recognition and supports current and future operations, targeting, protection, and electromagnetic attack planning. Electromagnetic support enhances rapid decision making and targeting by supplying combat information about threat emitter locations, disposition, and concentrations. Some information gathered through electromagnetic support may simultaneously feed into intelligence channels for further processing into intelligence products.

3-51. Detected electromagnetic signatures, when compared with the electromagnetic order of battle, can assist in determining whether SIGINT activities have already characterized the signal. This information informs the refinement of the electromagnetic order of battle and electromagnetic protection plans. The CEMA section should pass unknown or uncharacterized signatures detected through electromagnetic support to the G-2 or S-2 for SIGINT analysis.

3-52. The CEWO and the G-2 or S-2 mutually develop SOPs and battle drills for the unit to plan, integrate, and synchronize electromagnetic support and SIGINT activities. Integration takes advantage of similar equipment capabilities and synchronizes EW and SIGINT resources to increase flexibility. Using both EW and SIGINT systems for direction finding increases the available number of sensors to enable more accurate geolocation of threat systems to support targeting. Integration enables immediate sharing of information and reduces delays in targeting.

ELECTROMAGNETIC RECONNAISSANCE

3-53. *Electromagnetic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-85). EW and SIGINT elements conduct electromagnetic reconnaissance to understand the types of threat emissions in their assigned area. EW and SIGINT teams classify signals by detecting and recognizing emission characteristics through system functions and cross-referencing the signal characteristics with the electromagnetic order of battle. SIGINT elements further cross reference detected signals with intelligence libraries and databases. The information obtained from electromagnetic reconnaissance helps shape the operational environment by providing the commander with situational understanding to support decision making. Information from electromagnetic reconnaissance can lead to the implementation or modification of electromagnetic protection plans or identify possible targets for lethal or nonlethal fires.

THREAT WARNING

3-54. *Threat warning* is the urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources (JP 2-0). Threat warning helps characterize threat communications and noncommunications emitters. Threat warning enables the commander and staff to quickly identify immediate risks to friendly forces and implement appropriate countermeasures, including lethal and nonlethal attacks. EW and SIGINT sensors can detect, intercept, identify, and locate threat electromagnetic signatures and provide early warning of imminent or possible hostile activities. EW personnel report the detected emissions to the CEWO or directly to formations in accordance with orders and established procedures. The CEWO nominates threat systems for targeting through the targeting working group. Commanders may need to make an intelligence gain-loss decision when approving targets, balancing the value of SIGINT collection on a targeted emitter versus the tactical utility of eliminating the threat capability.

DIRECTION FINDING

3-55. EW teams use electromagnetic support equipment to conduct direction finding. Direction-finding activities allow EW teams to accurately geolocate threat emitters to support situational understanding and targeting. The CEMA section coordinates support from the G-2 or S-2 for SIGINT resources to sense threat emitters, gather information, and determine the locations of specified emitters of interest. The CEMA section shares the information gathered during direction-finding activities with the G-2 or S-2 to aid in ongoing intelligence preparation of the operational environment, and the targeting working group to support dynamic targeting.

3-56. For direction-finding missions, due to signal loss and interference, the further the receiver is from the transmitter the greater the error associated with the intercept angle. Geolocation is more accurate when using more sensing sites, increasing the distance between sensing sites, or both. Combining EW sites and SIGINT sites' sensors increases the number of direction-finding baselines and helps determine more accurate threat emitter locations. Refer to ATP 3-12.3 and ATP 2-22.6 for detailed information about direction finding and geolocation.

ELECTROMAGNETIC WARFARE REPROGRAMMING

3-57. *Electromagnetic warfare reprogramming* is the deliberate alteration or modification of electromagnetic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment (JP 3-85). The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW equipment and target sensing systems when threats change their tactics, techniques and procedures or the technical characteristics of their communications and EW systems. When EW or SIGINT forces observe that the threat has changed frequencies for communications or there are other changes in the electromagnetic environment, the CEWO ensures the reprogramming of EW systems or target sensing systems or updates to employment techniques.

3-58. EW reprogramming includes changes to self-defensive systems, offensive weapons systems, and other electromagnetic systems. The CEWO informs the G-6 or S-6 spectrum manager of the changes to EW requirements to coordinate the adjustment in mission parameters and may recommend friendly communications frequency changes. Units are responsible for reprogramming their own EW equipment. However, units should be aware of other reprogramming efforts in the assigned area when operating with joint and multinational forces. EW reprogramming examples include—

- Changing target frequencies for jamming.
- Updating joint restricted frequency lists.
- Changing locations of electromagnetic sensors due to environmental changes or interference.
- Installing the most up-to-date software, firmware, and hardware for EW equipment.

3-59. The four phases of the Army integrated EW reprogramming cycle are—

- Determine the requirement.
- Determine the response.
- Create the response.
- Implement the response.

3-60. Responsibilities for the phases of the reprogramming cycle vary based on requirements, the affected theater, and whether the requirement is a joint or single-Service requirement. Service reprogramming efforts include coordination with the joint electromagnetic spectrum operations cell to ensure reprogramming requirements are identified, processed, deconflicted, and implemented in a timely manner by all affected friendly forces. The Army Reprogramming Analysis Team Program Office is the Army's Service reprogramming center.

3-61. The Army is building a methodology to enable the Army to rapidly build and deliver electromagnetic countermeasures effective against threat signals of interest to support large-scale combat operations. ARCYBER will be the Army's Service reprogramming center for the future rapid EW reprogramming enterprise. Table 3-2 on page 45 shows the Service and interagency roles for EW reprogramming. Organizations to accomplish the future state reprogramming enterprise are shown in italics in the table.

Table 3-2. Service and interagency electromagnetic warfare reprogramming roles

<table>
<tr><th colspan="8">Service and Interagency Electromagnetic Warfare Reprogramming Roles</th></tr>
<tr><td></td><td colspan="3">Determine requirement</td><td rowspan="2">Determine response</td><td rowspan="2">Create response</td><td colspan="2">Implement response</td></tr>
<tr><td></td><td>Collect data</td><td>Identify change</td><td>Validate change</td><td>Distribute change</td><td>Implement change</td></tr>
<tr><td>Joint Services and interagency organizations</td><td>NSA, DIA, SPCs, CCMDs</td><td colspan="3">NSA, DIA, SPC, SRCs</td><td>SRCs</td><td>SRCs</td><td>Other Service tactical units</td></tr>
<tr><td rowspan="2">Army organizations</td><td rowspan="2">ECTs, theater armies and theater intel elements</td><td colspan="5">ARAT-PO
ARCYBER</td><td rowspan="2">Tactical units</td></tr>
<tr><td colspan="2">Army IEW organizations</td><td>Theater armies; Army capability managers; ARAT-PO</td><td colspan="2">Future Reprogramming Enterprise</td></tr>
</table>

Legend:

ACM	Army capability manager
ARAT-PO	Army Reprogramming Analysis Team Program Office
CCMD	combatant command
DIA	Defense Intelligence Agency
ECT	expeditionary cyberspace electromagnetic activities team
IEW	intelligence and electromagnetic warfare
intel	intelligence
NSA	National Security Agency
SPC	Service production center
SRC	Service reprogramming center

3-62. Refer to JP 3-85 for more information about EW reprogramming. See appendix E for electromagnetic warfare reprogramming message formats. See appendix F for more information about the Army Reprogramming Analysis Team Program Office. See appendix I for more information about the future Army reprogramming enterprise.

SYNCHRONIZATION WITH SIGNALS INTELLIGENCE

3-63. SIGINT elements may also perform electromagnetic support activities with proper training. SIGINT teams and EW teams often use the same or similar capabilities and may be tasked to simultaneously collect information that meets both electromagnetic support and intelligence requirements. The integration of EW and SIGINT capabilities and activities provides a holistic approach that reduces duplication of effort, enables additional information collection, and provides flexibility in employing EW and SIGINT resources. The CEWO and CEMA section exercise technical control over assigned EW forces and coordinate with the G-2 or S-2 to synchronize EW with SIGINT operations.

COMPLEMENTARY CAPABILITIES

3-64. EW and SIGINT teams performing similar electromagnetic support activities provide more complete coverage of an operational area. EW and SIGINT teams collaboratively use direction-finding techniques to locate threat emitters more accurately. Combining the capabilities of EW and SIGINT sensors and spreading them throughout the assigned area provides more direction-finding baselines to locate targeted emitters more accurately.

DISTINCTIONS BETWEEN ELECTROMAGNETIC WARFARE AND SIGNALS INTELLIGENCE

3-65. Though EW and SIGINT are complementary, there are important distinctions between them. Legal considerations distinguish EW and SIGINT activities and the authorities for each to support operations that, if not followed, can complicate and delay the execution of EW and SIGINT operations. Commanders and

CEMA sections should collaborate closely with the G-2 or S-2 and the staff judge advocate or legal advisor to ensure compliance with SIGINT policies when planning EW activities.

3-66. EW and SIGINT employ the same or similar electromagnetic sensing and direction-finding capabilities; the task and purpose are the main factors when deciding whether to use SIGINT or EW capabilities. Army EW personnel are authorized to conduct electromagnetic support under the inherent authority of a military commander, including activities to search for, intercept, identify, locate, and localize sources of intentional or unintentional radiated electromagnetic energy for indications and warning, situational awareness, and targeting. The commander may also use electromagnetic support data to support targeting for electromagnetic attack, if delegated electromagnetic attack control authority.

3-67. Both EW and SIGINT sensors can provide combat information to support electromagnetic protection, immediate threat recognition, targeting, assessment, and planning of future operations. SIGINT elements perform sensing support activities when used to provide immediate threat intelligence including threat warnings, avoidance, and targeting. When SIGINT sensors intercept, identify, and localize sources of electromagnetic energy for intelligence purposes, they are supporting a SIGINT mission under National Security Agency SIGINT authorities. These distinctions are identified by determining—

- Who tasks or controls the sensors (G-2 or S-2 versus G-3 or S-3).
- What the sensors are tasked to provide (intelligence versus combat information).
- The purpose of the task that drives the employment of the sensors (intelligence collection versus threat warning).

3-68. Units may also transfer select data gathered through electromagnetic support activities to the United States SIGINT System for further analysis and processing into foreign intelligence. The CEWO and the G-2 or S-2 staff develop an SOP for exchange of electromagnetic support information.

Limitations of Electromagnetic Support

3-69. EW teams conduct sensing activities to locate signals of interest from the electromagnetic order of battle. When sensors detect a signal, electromagnetic support capabilities can measure or determine the signal frequency and modulation type and compare them with the electromagnetic order of battle to identify known signals of interest. The electromagnetic support sensors can also determine the direction to the transmitter (line of bearing). The EW team reports the identified signal of interest and line of bearing to the CEMA section. The CEMA section uses lines of bearing from multiple EW teams to geolocate the threat transmitter. This geographic location is combat information that supports either situational understanding or targeting. EW teams and CEMA sections should pass unknown detected signals for further analysis by SIGINT elements.

Additional Capabilities Provided by Signals Intelligence

3-70. SIGINT teams and equipment can perform the same electromagnetic support functions as EW teams, but their primary mission and purpose align with their ability and legal authorities to perform intelligence-specific functions:

- Transcription.
- Decryption of radio signals.
- Traffic analysis.
- Reporting into the United States SIGINT system.
- Target package analysis.
- Comparison of signal characteristics with SIGINT databases.

3-71. Based on the mission variables of METT-TC (I), commanders may task-organize SIGINT teams in the close area to augment electromagnetic support capabilities during a critical phase of an operation. Employing dispersed EW and SIGINT teams across the assigned area provides more complete sensor coverage. While they are tasked in this way, the SIGINT teams will not be able to perform their primary intelligence mission. Task-organized SIGINT teams can provide—

- Additional lines of bearing for more accurate geolocation.
- Immediate threat warning.
- Combat information to support protection and targeting.

3-72. Figure 3-1 illustrates the arrangement of EW and SIGINT elements and their respective technical control channels at the division and brigade combat team.

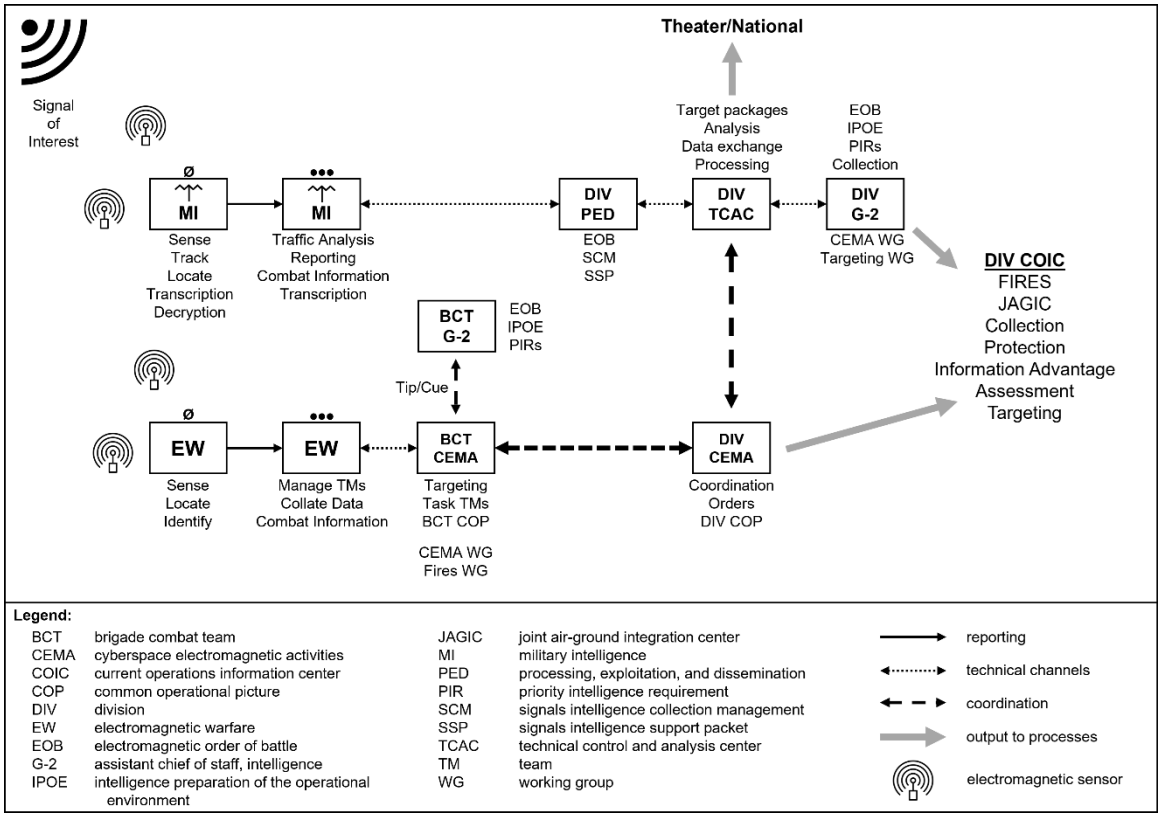


Figure 3-1. Synchronization of electromagnetic warfare with signals intelligence

ELECTROMAGNETIC WARFARE FORCES AT ECHELONS DIVISION AND BELOW

3-73. Maneuver units at echelons division and below are assigned organic EW forces and capabilities. This section describes organic EW formations at the division and brigade combat team.

DIVISION

3-74. The division EW company (see figure 3-2 on page 48) provides layered, long-range sensing and electromagnetic attack capabilities in the division deep area and downward reinforcement to brigade combat teams in the close area. The company's electromagnetic support capabilities can detect, recognize, locate, and identify threat signals of interest and assist the commander, G-3, CEWO, and G-6 in formulating electromagnetic protection plans. The company employs electromagnetic attack capabilities to disrupt enemy spectrum-dependent devices.

3-75. While electromagnetic support mainly enables situational understanding, decision making, and targeting, the CEMA section also coordinates with the G-2 to ensure electromagnetic support data from the EW company reaches the appropriate analysts for processing into intelligence, as necessary. Early designs of capabilities support the intent of the company to deliver radio frequency-enabled offensive cyberspace operations payloads while also enabling military information support operations, military deception, and other information advantage activities.

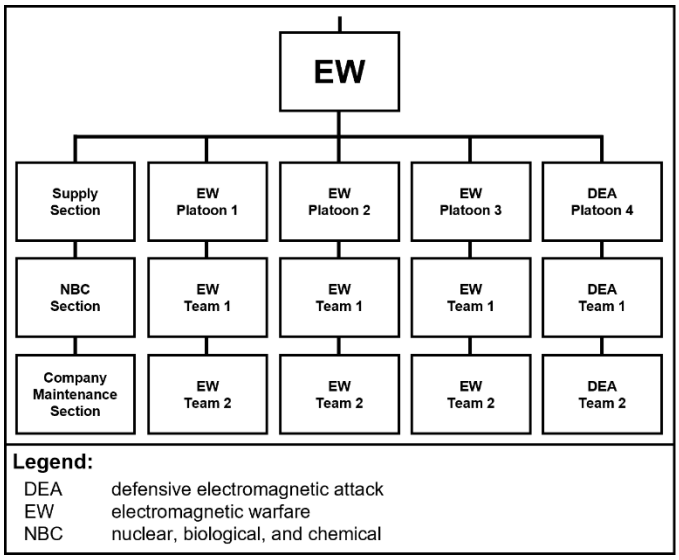


Figure 3-2. Division electromagnetic warfare company

Note. Division EW companies are authorized in unit tables of organization and equipment but are in the initial stages of resourcing in the operational force. References to the division EW company in the text reference capabilities and functions of the unit as designed and authorized.

BRIGADE COMBAT TEAM

3-76. The brigade combat team EW platoon (see figure 3-3) operates under the operational control of the brigade S-3. The brigade CEMA section controls EW taskings for the teams through technical channels. Technical channels are the chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities. The EW platoon supports the commander's ability to engage targets with lethal and nonlethal attack capabilities. The platoon detects and locates communications and noncommunications emitters in the brigade's assigned area using its organic electromagnetic support capabilities. The platoon reports the locations of enemy emitters to the CEMA section for situational awareness and targeting. The CEMA section forwards unidentified signals detected to the S-2 for further analysis. Because brigade combat team EW elements operate in close contact with enemy forces, they may be positioned to answer some commander's critical information requirements by direct observation. EW teams must be aware of collection requirements; unit SOPs should include reporting requirements. Refer to ATP 3-12.4 for detailed information about the composition and capabilities of EW companies and platoons.

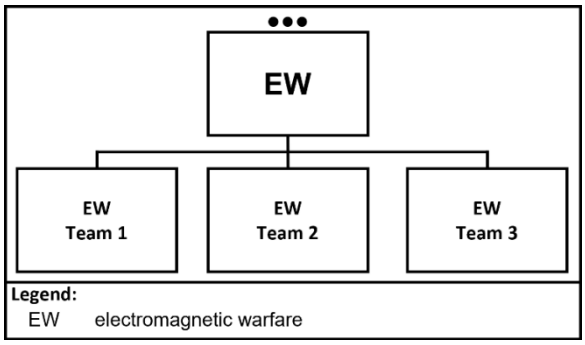


Figure 3-3. Brigade combat team electromagnetic warfare platoon

Note. There is a pending force design update to restructure the brigade combat team EW platoon from three EW teams to six EW teams.

Chapter 4

Cyberspace Electromagnetic Activities

This chapter discusses cyberspace electromagnetic activities. It begins with an overview, followed by a discussion of cyberspace electromagnetic activities roles by echelon. The chapter continues with a discussion of cyberspace electromagnetic activities through the operations process—planning, preparation, execution, and assessment—and the integrating processes. The chapter ends with a discussion of integration with the joint force.

OVERVIEW

4-1. The use of cyberspace and the electromagnetic spectrum are critical to successful operations. U.S. and threat forces alike rely heavily on cyberspace- and spectrum-dependent capabilities for—

- Command and control.
- Information collection.
- Situational understanding.
- Navigation.
- Target acquisition.
- Attack.

4-2. Achieving positions of relative advantage in cyberspace and the electromagnetic spectrum significantly contributes to the achievement of military objectives. By integrating cyberspace and EW operations into combined arms operations, commanders can limit the threat's available courses of action, diminish their ability to gain momentum, degrade their command and control, and affect their ability to operate effectively in the other domains.

4-3. Commanders leverage cyberspace and EW capabilities with other capabilities in a combined arms approach to seize, retain, and exploit the initiative. They do this through CEMA. ***Cyberspace electromagnetic activities*** **are the planning, integration, and synchronization of cyberspace and electromagnetic warfare operations as part of a combined arms approach through the operations process.** Integrating and synchronizing cyberspace and EW operations into the concept of operations contributes to mission success.

4-4. CEMA sections at echelons theater army through brigade play an important role in planning combined arms operations. They do this through the operations process, the integrating processes, and in working groups and boards.

CYBERSPACE ELECTROMAGNETIC ACTIVITIES ROLES BY ECHELON

4-5. CEMA sections are made up of cyber warfare officers, EW technicians, EW specialists, and spectrum managers. The grade levels within the CEMA section vary by echelon; higher echelons are staffed by more senior grades. CEMA sections at echelons corps and below plan, integrate, and synchronize cyberspace and EW operations across the competition continuum. The key activities of CEMA sections at echelons corps and below are—

- Developing and seeking approval of high-priority target lists, target nominations, collection priorities, and risk mitigation measures.
- Synchronizing cyberspace and EW operations with other lethal and nonlethal capabilities.
- Deconflicting frequency use with G-6 or S-6 spectrum managers.

4-6. Along with joint and multinational partners, Army forces use cyberspace and EW operations to support engagement, counter threat narratives, and conduct deception to create uncertainty within a threat's decision-making process. CEMA sections at all echelons exercise technical control over organic EW elements. In this role, the CEMA sections control electromagnetic support taskings and issue electromagnetic attack guidance within delegated electromagnetic attack control authority. The corps conducts shaping operations in the deep

area, coordinates with tactical elements operating in the close area, and integrates operations with the theater army.

4-7. Figure 4-1 illustrates tactical electromagnetic support reporting. CEMA sections issue electromagnetic support taskings to EW platoons in the close area. EW platoons conduct electromagnetic support sensing and report to the CEMA section through technical channels. The CEMA section integrates electromagnetic support into the operations process through coordination with other staff sections:

- Targeting working group (identifying and locating targets; triggers for fires; assessment).
- G-2 or S-2 (update electromagnetic order of battle; refer signals for processing into intelligence).
- G-3 or S-3 (combat information for decision support).
- G-6 or S-6 spectrum manager (frequency deconfliction; update joint restricted frequency list).

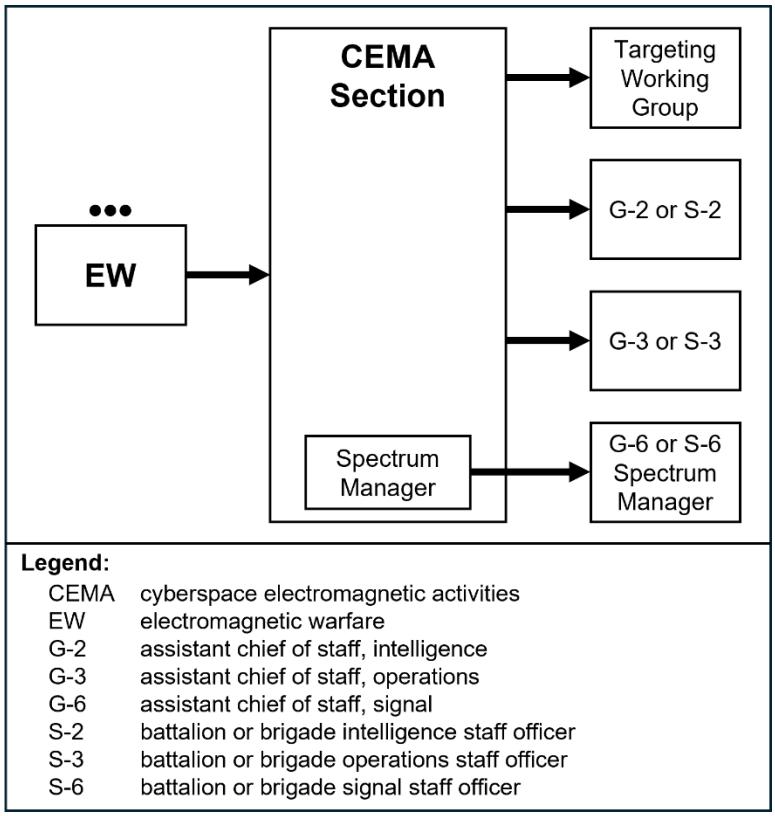


Figure 4-1. Tactical electromagnetic support reporting

Note. The content on the corps' CEMA responsibilities in this manual is based on the corps operating as a tactical echelon or ARFOR headquarters. If the corps is designated as a joint task force headquarters, the commander and staff refer to joint doctrine for their responsibilities for cyberspace operations and joint electromagnetic spectrum operations.

CORPS

4-8. The corps is the primary integrating echelon for multidomain convergence. The corps CEMA section integrates subordinate divisions and brigade combat teams' cyberspace and EW activities and CEMA reporting. The corps CEMA section reports through the theater army to the joint task force joint cyber center (for cyberspace operations) and the joint electromagnetic spectrum operations cell (for EW and spectrum use). During crisis and armed conflict, the corps CEMA section participates in the targeting process to nominate cyberspace and EW targets in the corps deep area and validate target nominations from subordinate divisions.

4-9. The corps CEMA section integrates cyberspace and EW operations into the corps commander's concept of operations. The CEMA section leads the CEMA working group (see paragraph 4-42) to assist in planning, development, integration, and synchronization of cyberspace and EW operations into combined arms operations through staff collaboration and shared understanding.

4-10. The CEWO participates in the targeting working group to nominate, vet, and process possible targets received from subordinate units and targets developed by the corps staff for effects in cyberspace and the electromagnetic spectrum. The CEWO—

- Assists the staff in integrating and synchronizing cyberspace and EW operations into combined arms.
- Advises the commander and staff on the effects of cyberspace and EW capabilities, including rules of engagement, impacts, and constraints.
- Develops and maintains a consolidated cyberspace and EW targeting synchronization matrix and assists in nominating cyberspace and EW targets in collaboration with the targeting working group.
- Monitors and assesses measures of performance and effectiveness while maintaining updates on cyberspace and EW effects on the operational environment.
- Requests and coordinates for offensive cyberspace operations and electromagnetic attack support through the combatant command while integrating received cyber mission forces and other Service EW capabilities into operations.
- Coordinates with joint and multinational partners for cyberspace and EW capabilities that complement or increase the unit's organic capabilities.
- Coordinates and deconflicts cyberspace and EW activities, including frequency deconfliction, with the G-2 and the G-6.
- Develops and implements cyberspace and EW home-station training.

Note. Planning for EW home-station training at all echelons includes collaboration with the G-6 or S-6 spectrum manager for frequency assignments and frequency deconfliction.

DIVISION

4-11. The division CEMA chief is the primary advisor to the division commander on cyberspace and the electromagnetic spectrum. The division CEMA section—

- Plans operations for organic cyberspace and EW capabilities.
- Prepares requests for external cyberspace and EW support.
- Integrates effects.
- Deconflicts spectrum use with the G-6 spectrum manager.
- Assesses cyberspace and EW effects in the division's assigned area.

4-12. Divisions do not have an assigned capability to plan and integrate all aspects of cyberspace operations, in particular future operations. The division CEMA section may be augmented with support from the corps or theater army to plan, coordinate, integrate, and synchronize cyberspace and EW operations into combined arms. The CEMA section vets and processes targets nominated by subordinate units for cyberspace effects. The CEMA chief leads the CEMA working group (see paragraph 4-42) when required to synchronize and integrate cyberspace and EW operations into the concept of operations.

BRIGADE COMBAT TEAM

4-13. The brigade EW platoon conducts electromagnetic support to understand friendly, threat, and neutral use of the electromagnetic spectrum in the brigade's assigned area. Understanding friendly spectrum use informs electromagnetic protection efforts, including EMCON plans. The EW platoon is normally under operational control of the S-3 and technical control of the CEMA section. The commander may task-organize the EW platoon with other elements and establish other command relationships to meet the brigade's requirements. The platoon reports the locations of enemy emitters to the CEMA section to support situational understanding and targeting.

4-14. The brigade combat team CEWO is the primary advisor to the brigade commander on cyberspace and the electromagnetic spectrum. The CEWO leads the CEMA section in—

- Planning operations for the EW platoon.
- Preparing requests for external cyberspace and EW support.
- Integrating effects.
- Assessing cyberspace and EW effects in the assigned area.

4-15. The CEMA section plans, coordinates, and integrates cyberspace and EW operations in support of the commander's intent and concept of operations. The CEMA section collaborates with all staff sections and subordinate units to meet the commander's operational objectives and desired end state. The CEMA section plans, synchronizes, and integrates cyberspace and EW operations through the operations process and through integrating processes and working groups, and deconflicts spectrum use with the S-6 spectrum manager.

4-16. The brigade CEMA section participates in the targeting process to nominate cyberspace and EW targets to support the maneuver plan. The CEMA section provides technical control of organic EW teams during operations. Though the CEMA section aligns cyberspace and EW operations with the operations process, they must collaborate with the S-3 to task EW platoons in support of brigade operations through the orders process. When required, the CEWO may form and lead a CEMA working group (see paragraph 4-42) to synchronize and integrate cyberspace and EW operations in a combined arms approach.

4-17. Data and information gathered through electromagnetic support provide the commander with critical combat information. The CEMA section uses combat information from the EW platoon to develop situational understanding and support targeting. The CEMA spectrum manager uses electromagnetic support data from the EW platoon to develop and update electromagnetic spectrum information in the common operational picture. The CEMA section also reports unknown signals detected to the S-2 to for processing into intelligence.

CYBERSPACE ELECTROMAGNETIC ACTIVITIES IN THE OPERATIONS PROCESS

4-18. The CEMA section, supported by the CEMA working group, integrates and synchronizes cyberspace and EW operations during planning, preparation, execution, and assessment. The CEMA section provides representatives to the plans, future operations, and current operations integrating cells as required to ensure cyberspace and EW operations are integrated and synchronized into the concept of operations in accordance with the commander's intent.

4-19. The CEMA section works closely with other members of the CEMA working group to ensure unity of effort to meet the commander's objectives. Integration and synchronization of cyberspace and EW operations—

- Ensure information collected in cyberspace and the electromagnetic spectrum is routed to the appropriate staff to support the commander and staff's situational understanding of the operational environment.
- Ensure the effective use of cyberspace and EW assets for information collection and targeting.
- Ensure appropriate coordination between Army and joint forces, multinational partners, and host nations before employing offensive cyberspace or EW capabilities.
- Minimize unintended interference (frequency fratricide) with friendly spectrum-dependent capabilities.

PLANNING

4-20. Planning is a continuous activity of the *operations process*—the major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0). Commanders use the operations process to drive the conceptual and detailed planning necessary to understand an operational environment; visualize and describe the operation's end state and operational approach; make and articulate decisions; and direct, lead, and assess operations. Refer to ADP 5-0 for fundamentals of the operations process.

Operation Plans

4-21. Plans and orders come in many forms and vary in the scope, complexity, and length of time they address. Generally, commanders and staffs develop an operation plan well in advance of execution; the operation plan is not executed until directed in an operation order (see paragraph 4-31). Commanders and staffs may develop operation plans through the Army design methodology if the military problem and situation are not well-defined. The conceptual operation plan must be integrated with the detailed planning typically associated with the military decision-making process to produce executable operation orders. Refer to ATP 5-0.1 for detailed information about the Army design methodology.

Information Requirements

4-22. During planning, commanders and staffs determine their information requirements to support decision making and protection. The CEWO participates in the definition of information requirements including—

- Commander's critical information requirements.
- Priority intelligence requirements.
- Friendly force information requirements.
- Essential elements of friendly information.

Commander's Critical Information Requirements

4-23. A *commander's critical information requirement* is specific information identified by the commander as being essential to facilitate timely decision making (JP 3-0). A commander's critical information requirement is directly tied to a decision that supports the successful execution of military operations. Commanders designate critical information requirements based on likely decisions and their visualization of the operation. A commander's critical information requirement may support one or more decisions. During planning, staffs recommend information requirements for commanders to designate as critical information requirements. Information requirements may be selected based on considerations in cyberspace or electromagnetic spectrum.

4-24. Commander's critical information requirements related to cyberspace and EW may include information relating to friendly, civilian, and threat use of, and activity in, cyberspace and the electromagnetic spectrum. Refinement of the commander's critical information requirements is continuous throughout operations. During preparation and execution, staffs recommend changes to commander's critical information requirements based on their running estimates. Indicators in cyberspace or the electromagnetic spectrum may aid in answering commander's critical information requirements. For example, the CEMA section may assist in answering information requirements relating to enemy composition, disposition, strength, and activity. The detection of a certain radio or radar emission may reveal the enemy course of action or the location of a high-payoff or high-value target.

Priority Intelligence Requirements

4-25. A *priority intelligence requirement* is the intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support (JP 2-0). Priority intelligence requirements identify the information about the enemy and other aspects of an operational environment that the commander considers most important. Intelligence about civil considerations may be as critical as intelligence about the enemy.

4-26. Priority intelligence requirements may include the location and electromagnetic signature of enemy command and control nodes, radar systems, or jamming assets. Cyberspace and EW priority intelligence requirements may also include information about the enemy electromagnetic order of battle, such as cyberspace and EW capabilities, spectrum-dependent devices, or electromagnetic signatures of key enemy systems. Cyberspace and the electromagnetic spectrum may provide key indicators that answer priority intelligence requirements, for example—

- Location of a threat signal of interest may indicate the position of an enemy command post.
- Locations of threat radar systems may reveal the presence of enemy fires or air defenses in the assigned area.
- Social media activity may reveal an upcoming civil disturbance.

- Open source data from navigation applications may reveal congestion.
- Software application content and metadata may reveal operations security vulnerabilities.

Friendly Force Information Requirements

4-27. A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0). Friendly force information requirements identify the information about the mission, troops and support available, and time available for friendly forces that the commander considers most important. Examples of friendly force information requirements relevant to cyberspace and EW operations include—

- Targeting of personnel or dependents via cyberspace.
- The capture of sensitive hardware.
- The suspected jamming of positioning, navigation, and timing systems.

Essential Elements of Friendly Information

4-28. An *essential element of friendly information* is a critical aspect of a friendly operation that, if known by a threat, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection (ADP 5-0). Essential elements of friendly information establish the information friendly forces need to protect from unauthorized disclosure. Identifying essential elements of friendly information is the first step in the operations security process and central to the protect information activity. Examples of essential elements of friendly information relevant to cyberspace and EW operations include—

- Critical passwords.
- Cryptologic keys.
- Classified waveforms.
- Existence or functionality of wartime reserve modes.

4-29. In addition to cyberspace and EW essential elements of friendly information, the CEMA section plays an important role in protecting other friendly tactical information, such as—

- Locations of critical command and control nodes (electromagnetic protection).
- The fact that a certain operation is a deception (realistic electromagnetic decoys).

4-30. Refer to JP 3-55 for more information about the joint operations security process. Refer to ADP 3-13 for more information about information advantage activities.

Operation Orders

4-31. An operation plan becomes an operation order when directed for execution based on a specified time or event. The commander and staff produce operation orders through the military decision-making process. This planning also involves various integrating processes and working groups to integrate and synchronize combined arms planning. See paragraphs 4-62 through 4-100 for more information about the CEMA section's role in the integrating processes and appendix B for information on the CEMA section's role in preparing operation orders.

Military Decision-Making Process

4-32. The commander and staff integrate cyberspace and EW operations with combined arms maneuver through the military decision-making process. The CEWO and CEMA section either produce or contribute to multiple portions of the operation order during the military decision-making process. See appendix B for detailed information about the CEWO's key inputs, substeps, and outputs for each step of the military decision-making process.

Emission Control Plans

4-33. During planning, the CEWO develops EMCON plans in conjunction with the G-3 or S-3 and the G-6 or S-6. A well-constructed EMCON plan contributes to reduced electromagnetic signatures by providing progressively more restrictive measures to control electromagnetic emissions based on the tactical situation.

It specifies operating procedures for emitters based on terrain, threat, and the scheme of maneuver. It is integrated into the execution checklist and decision support templates. At the least restrictive EMCON condition (EMCON 1 [green]), normal operation of all spectrum-dependent devices continues with basic security precautions. At the most restrictive level (EMCON 5 [black]), units may cease operation of all electromagnetic emitters until the tactical situation allows return to a less restrictive EMCON condition. Restrictive EMCON conditions may require maneuver elements to maintain extended periods of radio silence, relying on disciplined initiative of subordinate commanders within the commander's intent under the mission command approach. Terrain, assigned mission, or other factors may result in elements within a unit operating under different EMCON conditions.

4-34. Creating an EMCON plan involves defining operational requirements for the use of emitters, determining the operating criteria for each type of emitter, and determining triggers for transition between EMCON conditions. The EMCON plan should be published in Tab D to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of the operation order. A complete EMCON plan requires—

- Integration with the scheme of maneuver.
- Operating criteria for emitters, by EMCON condition.
- Triggers for transition between EMCON conditions.

4-35. When developing EMCON plans, it is important for the CEWO and the G-6 or S-6 to understand the background electromagnetic environment in their assigned area. It is difficult to maintain a low probability of detection in remote areas where there is little background radio frequency noise. In these cases, a very restrictive EMCON plan may be necessary to provide a reasonable measure of electromagnetic protection. In more populated areas where the background radio frequency noise floor is typically much higher, planners may be able to effectively hide the signals within the higher background noise if the signal is not discernable as a military communications system.

4-36. G-3 or S-3 participation is critical in the development of EMCON plans. Electromagnetic signatures can reveal the locations of command posts, exposing them to risk of lethal fires. Experience at combat training centers shows that the opposing force can determine the location, size, disposition, and direction of travel of maneuver formations based on their electromagnetic emissions. Considering EMCON in selection of movement routes may allow the unit to take advantage of manmade and natural terrain to mask electromagnetic emissions from threat detection. EMCON plans may include maneuver elements observing radio silence on a movement to contact to prevent revealing the operation to the enemy. Implementing such restrictive EMCON measures requires commanders to trust in the disciplined initiative of subordinates under the mission command approach.

Integration With the Scheme of Maneuver

4-37. During mission planning, the staff should determine the minimum required capabilities for each phase of the operation. Knowing which emitters are necessary to conduct operations enables the CEWO, the G-3 or S-3, and the G-6 or S-6 to create an EMCON plan that minimizes the unit's electromagnetic signatures while ensuring the availability of critical command and control capabilities.

Emitter Criteria

4-38. The CEWO assists the G-3 or S-3 and the G-6 or S-6 in determining operating criteria for each type of emitter for each EMCON condition. Detailed planning helps inform the commander's risk decisions and ensures smooth transitions between EMCON conditions. The emitter criteria specify the operating procedures for a particular emitter type across the EMCON conditions and the triggers for removing the emitter from operation. To build a complete EMCON plan, the staff builds an emitter criteria table for each type of emitter in the formation. Table 4-1 on page 56 illustrates an example of emitter criteria for single-channel ground and airborne radio system by EMCON condition.

Table 4-1. Example emitter criteria table.

Emitter	*Emitter Criteria by EMCON Condition*				
	EMCON 1 (Green)	**EMCON 2 (Yellow)**	**EMCON 3 (Amber)**	**EMCON 4 (Red)**	**EMCON 5 (Black)**
SINCGARS	Use system as prescribed in the technical manual	Must encrypt systems for operation	Must encrypt and operate in frequency hop mode	Must encrypt and operate in frequency hop mode. Do not exceed 10 watts transmit power. Use directional antennas if available	DO NOT USE
Legend:					
EMCON	emission control				
SINCGARS	single-channel ground and airborne radio system				

Triggers for Transition Between Emission Control Conditions

4-39. It is important when building an EMCON plan to establish conditions- or event-based triggers to transition between EMCON conditions. Triggers for transitioning between EMCON conditions can occur at any level and should be based on the mission variables of METT-TC (I). The EMCON plan may specify transition to a more restrictive condition based on enemy EW activity. Prominent terrain features between friendly and enemy formations may temporarily allow transition to a less restrictive EMCON condition. A unit beginning an assault may choose to transition to a very restrictive EMCON condition, ceasing operation of all emitters besides the tactical radios needed to exercise command and control over assaulting troops. Significant enemy maneuver, lethal fires, or EW activity might trigger an immediate change from EMCON condition 3 (amber) to EMCON condition 5 (black) until the threat level reduces. The CEWO, with the assistance of the G-3 or S-3 and the G-6 or S-6 will make recommendations on what triggers should prompt transitions between EMCON conditions based on identified risks and the electromagnetic operational environment in the assigned area. Units should rehearse the EMCON plan, including triggers for transition during rehearsals.

Working Groups

4-40. A headquarters' battle rhythm consists of a series of meetings (to include working groups and boards), briefings, and other activities synchronized by time and purpose. The battle rhythm is a deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations. The chief of staff or executive officer oversees the unit's battle rhythm. The chief of staff or executive officer sequences activities logically so that the output of one activity informs inputs to other activities. This is important not only within the headquarters, but also in the unit's battle rhythm as it nests with the higher echelon headquarters.

4-41. During periods of high operating tempo, the chief of staff and the staff principals may combine working groups to synchronize efforts and increase efficiencies while minimizing requirements on the staff. Examples include combining the civil-military operations working group, information operations working group, and CEMA working group to streamline coordination prior to the targeting working group. Refer to FM 6-0 for more information about boards and briefings in the command posts.

Cyberspace Electromagnetic Activities Working Group

4-42. The CEMA section is the staff lead for the CEMA working group. The CEMA working group is not a formal working group that requires dedicated staff members from other sections. When needed, the G-3 or S-3 convenes and chairs a CEMA working group to assist in synchronizing and integrating cyberspace and EW operations into the concept of operations. The CEMA section normally collaborates with key

stakeholders during staff meetings established as part of the unit's battle rhythm and throughout the operations process. Membership in the CEMA working group varies based on mission requirements.

4-43. If scheduled, the CEMA working group must be integrated into the staff's battle rhythm. The CEMA working group coordinates with higher, subordinate, and adjacent units to support operations and assist the fire support element throughout the execution of an operation. Generally, the CEMA working group is comprised of staff representatives with equities in CEMA. These stakeholders typically include—

- The G-2 or S-2.
- The G-3 or S-3.
- The G-6 or S-6.
- The G-6 or S-6 spectrum manager.
- The G-39 officer or representative.
- The fire support officer or a fire support element representative.
- The staff judge advocate representative.
- Liaison officers.

4-44. Table 4-2 shows sample CEMA working group activities.

Table 4-2. Sample cyberspace electromagnetic working group activities

General information	***Participants***
Title: CEMA working group **Purpose:** Coordinate for and integrate cyberspace and EW operations in support of the concept of operations. **Frequency:** Daily. **Duration:** One hour. **Location:** Main command post briefing area. **Medium:** Face-to-face, Microsoft Teams.	**Staff lead:** CEMA section. **Chair:** G-3 or S-3. **Members:** G-2 or S-2, G-3 or S-3, G-5, G-6 or S-6, G-39 officer or representative, fire support officer or fire support element representative, staff judge advocate representative, liaison officers, and others as required.
Inputs and Outputs	***Agenda (Responsible Party)***
Inputs: • Higher headquarters orders, directives, and policy. • Commander's guidance. • Outputs from the targeting and information working groups. • Running estimates. • Subordinate cyberspace or EW effects requests. **Outputs:** • Recommended requests for cyberspace and EW capabilities and resources. • Approval of information working group input. • Approval of targeting working group input. • Approval of recommended changes to the current operation order.	• Roll call (CEWO). • Intelligence update (G-2 or S-2). • Operations update (G-3 or S-3). • Cyberspace operations update (CEWO). • EW update (CEWO). • Spectrum management update (G-6 or S-6 spectrum manager). • Target nominations (CEWO). • Cyberspace and EW capabilities requests recommendation (CEWO). • Guidance (G-3 or S-3).

Legend:

CEMA	cyberspace electromagnetic activities	G-5	assistant chief of staff, plans
CEWO	cyber electromagnetic warfare officer	G-6	assistant chief of staff, signal
EW	electromagnetic warfare	S-2	battalion or brigade intelligence staff officer
G-2	assistant chief of staff, intelligence	S-3	battalion or brigade operations staff officer
G-3	assistant chief of staff, operations	S-6	battalion or brigade signal staff officer
G-39	assistant chief of staff, information plans and operations		

Other Working Groups

4-45. The CEWO and CEMA section are key participants in other staff working groups. See appendix B for detailed information about the CEWO and CEMA section's roles in other working groups, including—

- Information collection working group.
- Targeting working group.
- Targeting coordination board.
- Protection working group.
- Assessment working group.

PREPARATION

4-46. Preparation consists of those activities performed by units and Soldiers to improve their ability to execute an operation. Preparation creates conditions that improve friendly forces' opportunities for success and includes activities such as—

- Rehearsals—including EMCON plan and triggers.
- Training.
- Pre-combat checks and pre-combat inspections.

4-47. Preparation requires commander, staff, unit, and Soldier actions to ensure the force is ready to execute operations. The CEMA section's role in preparation focuses on contributions to collection management, information collection, target development, and protection tasks. The CEWO or CEMA chief participates in unit rehearsals to prepare for operations. The CEMA section continues to host the CEMA working group and participates in other scheduled working groups. See paragraph 4-67 for more information about information collection. See paragraph 4-77 for more information about the CEMA section's role in targeting. See appendix B for information about the CEMA section's role in the protection working group.

EXECUTION

4-48. Planning and preparation accomplish nothing if the command does not execute effectively. *Execution* is the act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0).

4-49. Throughout execution, commanders, supported by their staffs, assess the operation's progress, make decisions, and direct the application of combat power to seize, retain, and exploit the initiative or counter threats. Major activities of execution include—

- Assessment—monitoring current operations and evaluating progress and variances.
- Decision making—making decisions to exploit opportunities or counter threats.
- Directing action—applying combat power and resources at decisive points and times.

4-50. During execution, the CEMA section—

- Ensures cyberspace and EW operations are aligned and sequenced with the scheme of maneuver.
- Directs the activities of organic EW platoons.
- Requests cyberspace and EW support as needed from higher echelons and joint and multinational forces.

Frequency Deconfliction

4-51. The CEMA spectrum manager deconflicts frequency use for EW with the spectrum management operations conducted by the G-6 or S-6 spectrum manager. The G-6 or S-6 spectrum manager maintains a local database of all known emitters and receivers in the assigned area and provides input for the joint restricted frequency list through the chain of command to the joint task force joint electromagnetic spectrum operations cell. The joint electromagnetic spectrum operations cell prepares the joint restricted frequency list based on coordinated inputs from the J-2, J-3, and J-6 staffs and input from subordinate commands. The *joint restricted frequency list* is a time and geographically oriented listing of TABOO, protected, and guarded functions, nets, and frequencies and limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives (JP 3-85).

- ***TABOO frequencies*** are any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies (JP 3-85).
- ***Protected frequencies*** are friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electromagnetic warfare operations are directed against hostile forces (JP 3-85).
- ***Guarded frequencies*** are a list of time-oriented, enemy frequencies that are currently being exploited for combat information and intelligence or jammed after the commander has weighed the potential operational gain against the loss of the technical information (JP 3-85).

4-52. Using frequencies employed by other friendly forces in the same area may cause undesirable electromagnetic interference or frequency fratricide. Transmitting on guarded frequencies may disrupt friendly SIGINT operations. Knowing the purpose of spectrum resources and their characteristics allows the G-6 or S-6 spectrum manager and the CEMA spectrum manager deconflict friendly frequency use with EW operations and assists with preparation of electromagnetic protection plans.

Support to Intelligence Operations

4-53. The CEMA section shares electromagnetic support data from EW teams operating in the close area with the G-2 or S-2 for possible further processing into intelligence information. The CEWO and CEMA section exercise technical control over assigned EW forces and coordinate with the G-2 or S-2 to synchronize EW with SIGINT operations.

Electromagnetic Attack

4-54. During execution, EW teams in the close area may conduct electromagnetic attack activities. The CEMA section exercises technical control over the EW teams and provides electromagnetic attack guidance based on approved targets within delegated electromagnetic attack control authority. See chapter 3 for details about electromagnetic attack methods.

Responding to Enemy Malicious Cyberspace Activity and Electromagnetic Attacks

4-55. During execution, units may experience enemy malicious cyberspace activity and electromagnetic attacks. All personnel in the unit need to be able to recognize attack indicators and prepared to respond to malicious cyberspace activity and electromagnetic attacks. See appendix D for more information about recognizing and responding to malicious cyberspace activity and electromagnetic attacks.

Cyberspace Effects

4-56. During execution, units at echelons corps and below may create effects in cyberspace using available military capabilities. Units may also request cyberspace effects from theater- or national-level cyberspace forces based on approved targets. Units submit the CERF (see appendix C for instructions for completing the CERF).

ASSESSMENT

4-57. *Assessment* is determination of the progress toward accomplishing a task, creating a condition, or achieving an objective (JP 3-0). During assessment, the commander and staff compare intended outcomes from the operation plan or order and commander's intent with actual events to determine whether the unit is effectively employing its forces. Based on ongoing assessments, commanders refine plans and orders, and issue updated guidance to subordinates.

4-58. Assessment is a continuous process where the staff observes and evaluates the operational environment and the impact of friendly unit actions against their mission to better inform the commander. Successful staffs conduct assessments using existing staff elements, supported and coached by the assessment team. The staff may use indicators in cyberspace and the electromagnetic spectrum to aid in their assessments. For example, civilian activity on social media may contribute to assessing the effectiveness of messaging campaigns. The location and volume of enemy radio traffic may corroborate the effectiveness of a feint. The staff incorporates

assessment into their planning of cyberspace and EW operations. Refer to ATP 5-0.3 for more information about operational assessment.

Cyberspace and Electromagnetic Warfare Effects

4-59. The CEWO collaborates with fires elements and the G-2 or S-2 to support battle damage assessment for cyberspace and EW effects. This includes when lethal fires or other military actions are used to create an effect in cyberspace or the electromagnetic spectrum. Cyberspace and EW effects are usually difficult to observe directly. Assessments may rely heavily on measures of performance and may require inference and second order observations to evaluate measures of effectiveness. For example, a unit may assess the effectiveness of jamming by observing the enemy's transition to an alternate communication method. Assessment of EW effects may be enhanced by coordination with the G-2 or S-2 and SIGINT elements. Assessment of cyberspace effects may require support from theater- or national-level intelligence organizations. Understanding the method for assessment and the associated controlling organization is a key planning task such that coordination is required during execution.

Protection

4-60. The protection working group monitors and evaluates the progress of current operations to validate assumptions made in planning and to continually update changes to the situation. The protection working group continually meets to monitor threats to protection priorities, and recommend changes to the protection plan, as required. They also monitor the conduct of operations, looking for variances from the operation order that affect their areas of expertise. Units assess the impact protection actions have on operational objectives. As an example, overly restrictive EMCON measures may reduce operational effectiveness while overly permissive EMCON reduces survivability. Assessment determines whether implementation of these controls meets or fails to meet established measures of performance and effectiveness.

4-61. Units may also test the effectiveness of their protection plan. They may attempt to perform unauthorized actions on the network to assess cybersecurity or deploy sensors to measure the effectiveness of EMCON or other electromagnetic protection actions. Enemy actions offer an alternate perspective to assess friendly protection. Poor EMCON may result in the rapid engagement of units by enemy indirect fires. Assessment based on enemy activity generally requires the ability to correlate effective reporting and may trigger planned or hasty response actions.

CYBERSPACE ELECTROMAGNETIC ACTIVITIES IN THE INTEGRATING PROCESSES

4-62. The CEMA section plays critical roles in some of the integrating processes and shares some interaction with the rest of the integrating processes. The integrating processes in which the CEMA section participates are—

- Intelligence preparation of the operational environment.
- Information collection.
- Targeting.
- Risk management.
- Knowledge management.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

4-63. *Intelligence preparation of the operational environment* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (FM 2-0). The G-2 or S-2 leads intelligence preparation of the operational environment. Intelligence preparation of the operational environment begins at the start of the military decision-making process, is synchronized with planning, and continues throughout the operations process.

G-2 or S-2 Role

4-64. During intelligence preparation of the operational environment, the G-2 or S-2 supports cyberspace and EW operations by providing the commander and staff with all-source intelligence on the operational and

mission variables in an area of interest to determine conditions relevant to those operations. This information assists the commander and staff in understanding the operational environment, identifies opportunities for cyberspace and EW operations, and helps in course of action comparison and approval during the military decision-making process. During intelligence preparation of the operational environment, the G-2 or S-2 provides critical planning inputs to the rest of the staff, including—

- Threat doctrine, tactics, equipment, capabilities, vulnerabilities, and intent.
- Threat systems.
- Threat characteristics, including the electromagnetic order of battle.
- Identification of areas of interest and areas of influence.
- Terrain analysis.
- Threat courses of action (number driven by time available or directed by the commander).

Cyberspace Electromagnetic Activities Section Role

4-65. The CEMA section provides subject matter expertise on cyberspace and electromagnetic spectrum aspects of the operational environment, threat, and impacts to the operational environment, including—

- Civilian use of cyberspace and the electromagnetic spectrum in the assigned area.
- Cyberspace- and electromagnetic spectrum-related infrastructure in the assigned area.
- Threat cyberspace and EW doctrine, tactics, equipment, capabilities, vulnerabilities, and intent.
- Threat use of cyberspace and the electromagnetic spectrum.
- Known or templated locations for threat cyberspace and EW assets (this includes facilities for national and law enforcement).
- Ground-based, airborne, and functional EW employment considerations, including line of sight analysis. This supports the G-2 or S-2 development and refinement of the electromagnetic order of battle.

4-66. The CEMA section's subject matter expertise may be augmented or enhanced by access to cyberspace and electromagnetic support capabilities to support information collection. Refer to ATP 2-01.3 for more information about intelligence preparation of the operational environment.

INFORMATION COLLECTION

4-67. Information collection helps the commander understand and visualize the operation by aligning reconnaissance, surveillance, security, and intelligence assets to collect information about identified information gaps. It begins early in planning and continues throughout the operations process. Information collection is directly linked to intelligence preparation of the operational environment and supports planning, targeting, risk management, and decision making throughout the operations process.

4-68. The CEWO coordinates with the collection manager and the technical control and analysis cell to coordinate how and when in time and space the CEMA section and EW elements can answer information requirements with organic assets. This coordination includes priority intelligence requirements and friendly force information requirements. See appendix B for more information about the CEMA section's role in the information collection working group.

Collection Management

4-69. Collection management is a coordinated staff effort led by the G-2 or S-2. Collection management involves—

- Analyzing information and collection requirements
- Evaluating available collection assets (internal and external)
- Recommending taskings for information collection assets to the operations staff
- Submitting requests for information for adjacent and higher echelon collection support
- Assessing the effectiveness of the information collection plan.

4-70. The CEWO participates in the information collection working group to support collection management. Refer to ATP 2-01 for more information about collection management.

Information Collection Plan

4-71. The G-3 or S-3 collaborates with the G-2 or S-2 to develop the information collection plan based on the analysis performed by the entire staff. Through analysis, the staff determines the best way to satisfy each information requirement. The staff receives information collection tasks and requests for information from subordinate and adjacent units and higher echelon headquarters. The information collection plan aligns assets to collection tasks. Additionally, the plan provides coordinating instructions to ensure adequate coverage in the assigned area.

4-72. As the tactical situation changes, staffs adjust the overall information collection plan to synchronize collection. This optimizes collection and exploitation capabilities. The staff continually updates requirements to ensure information collection efforts synchronize with current operations and support future operations planning. As the information collected answers the commander's information requirements, the staff updates the information collection plan.

4-73. The CEWO is a key participant in the information collection working group led by the G-2 or S-2. During planning, the information collection working group develops the unit's collection plan to ensure effective use of collection assets. See appendix B for details about the CEWO's role in the information collection working group.

Combat Information

4-74. EW teams in the close area collect combat information through electromagnetic support. EW sensors survey the electromagnetic spectrum and conduct direction finding to provide combat information to support electromagnetic protection, immediate threat recognition, targeting, assessment, and planning for future operations. SIGINT teams also conduct electromagnetic support sensing for direction finding, geolocation, and decision support. Combining the capabilities of EW and SIGINT teams in the close area provides greater coverage of the assigned area and more accurate direction finding.

Decision Support

4-75. EW teams in the close area may be positioned to provide combat information through both electromagnetic support and direct observation. This combat information helps commanders understand enemy strength, position, and disposition to support decision making. The CEMA section exercises technical control of EW teams and reports combat information to support decision making to the G-3 or S-3.

Targeting

4-76. EW teams conduct direction finding to locate enemy emitters and report this information to the CEMA section and the G-2 or S-2. Locating enemy emitters of interest and characterizing their activities supports the CEMA section's role in targeting. This includes either deliberate targets based on the approved target list, or dynamic targeting—prosecuting targets of opportunity based on the tactical situation.

TARGETING PROCESS

4-77. CEMA sections play a critical role in the targeting process at echelon. They provide key insights about a target's criticality in cyberspace, its accessibility in cyberspace and the electromagnetic spectrum, and its vulnerability to existing cyberspace and EW capabilities. They assess the ability to engage targets through cyberspace and the electromagnetic spectrum in the short, medium, and long term and request the development of new capabilities to posture for future operations. The CEMA section uses systems analysis to identify additional effects chains to meet the commander's intent.

Targeting Guidance

4-78. The commander's targeting guidance must be articulated clearly and simply to enhance understanding. The guidance must be easily understood by all staff sections. Targeting guidance focuses on essential threat capabilities and functions that could interfere with the achievement of friendly objectives.

4-79. The commander's targeting guidance describes the desired effects to be generated by lethal fires, physical attack, cyberspace attack, electromagnetic attack, or other available capabilities. Targeting enables

the commander to produce desired effects through various lethal and nonlethal capabilities. Capabilities associated with one desired effect may also contribute to other desired effects. For example, a delay can result from disrupting, diverting, or destroying enemy capabilities or targets.

4-80. The desired effects for cyberspace and electromagnetic attacks generally affect systems or transmissions between systems rather than units and formations. As a result, certain effects terms and tactical tasks are generally more applicable than others for describing cyberspace and electromagnetic attack effects. For example, units may employ omnidirectional jamming to deny the enemy use of the electromagnetic spectrum, or an attack may trigger a system reboot in a radar system to temporarily neutralize enemy air defense. Through convergence with other combined arms actions, these attacks may contribute to compound effects on enemy units and actions.

4-81. When multiple terms could apply to a given attack, the targeting guidance should use the terms best aligned with the commander's intent. Cyberspace and EW capabilities may target transmission media, enemy systems, or enemy units.

Transmission or Medium-Focused Effects

Interdict—a tactical mission task where a unit prevents, disrupts, or delays the enemy's use of an area or route in any domain (FM 3-90). It is an offensive action that desynchronizes the enemy.

Deny—task to hinder or prevent the enemy from using terrain, space, personnel, supplies, or facilities. (ATP 3-21.20).

Example: Use of omnidirectional jamming to interdict enemy radio communications or deny the use of a particular portion of the electromagnetic spectrum.

System-Focused Effects

Suppress—a tactical mission task in which a unit temporarily degrades a force or weapon system from accomplishing its mission (FM 3-90).

Neutralize—a tactical mission task in which a unit renders the enemy incapable of interfering with an operation (FM 3-90).

Destroy—a tactical mission task that physically renders an enemy force combat ineffective until it is reconstituted (FM 3-90).

Deceive—a unit may provide specific input or otherwise manipulate a system to create an inaccurate or misleading interpretation of conditions. The target of the deception may include the system itself, the operator of the system, or enemy decision makers.

Examples:

- Jamming an enemy radar system to suppress integrated air defenses.
- Using directed energy to destroy an unmanned aircraft system or cause it to crash.

Unit-Focused Effects

Disrupt—a tactical mission task in which a unit upsets an enemy's formation or tempo and causes the enemy force to attack prematurely or in a piecemeal fashion (FM 3-90).

Delay—when a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on enemy forces without becoming decisively engaged. (ADP 3-90)

Fix—a tactical mission task in which a unit prevents the enemy from moving from a specific location for a specific period. (FM 3-90)

Defeat—to render a force incapable of achieving its objectives. (ADP 3-0)

Deceive—The target of the deception may include a system, the operators of a system, or enemy decision makers. The deception may be undertaken to achieve a specific result or to support a larger deception operation.

Example: Denying enemy positioning, navigation, and timing or communications to delay or disrupt their movement or delay the enemy advance.

Note. Unit-focused effects are generally achieved by employing cyber or EW capabilities in conjunction with other combined arms capabilities such as lethal fires or maneuver to create mutually supporting or compound effects.

4-82. The commander can direct a variety of nonlethal actions or effects separately or in conjunction with lethal actions or effects. The commander can also provide restrictions as part of targeting guidance. Targeting restrictions fall into two categories—the no-strike list and the restricted target list. The no-strike list consists of objects or entities protected by—

- The law of armed conflict.
- International laws.
- Rules of engagement.
- Other considerations.

4-83. A restricted target list is a list of valid targets with identified restrictions such as—

- Limit collateral damage.
- Preserve select ammo for final protective fires.
- Do not strike during daytime.
- Strike only with a certain weapon.
- Proximity to protected facilities and locations.

Note. Refer to FM 3-57, FM 3-84, FM 6-27, JP 2-0, JP 3-57, and JP 3-60 for additional information about legal considerations and targeting restrictions.

The Targeting Process

4-84. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). It is a continuous analytic process used to identify, prioritize, develop, and affect high-value and high-payoff targets to meet commanders' objectives. Targeting provides planners access to detailed target information, supported by the nominating component's analytic reasoning. The targeting working group uses this information to select targets and pair them with

capabilities to deny, degrade, disrupt, destroy, or manipulate the target's ability to perform its primary functions.

4-85. The targeting process should align sensors, decision makers, and effects delivery platforms for validation by the commander to align the necessary resources to shape the operational environment and set conditions for mission success. The CEMA section's participation in the targeting process helps align EW sensors and electromagnetic attack capabilities to possible targets.

4-86. Cyberspace and EW operations support provide timely and accurate targeting information for lethal or nonlethal attack. Cyberspace and EW assets may be able to detect threats well ahead of visual or direct contact. The CEWO is a key participant in the targeting working group and targeting coordination board to identify spectrum-dependent and cyberspace-dependent capabilities used by threat forces, aid in selecting targets, and align effects options that can provide a tactical advantage to support the scheme of maneuver. See appendix B for more information about the CEWO and CEMA section's role in the targeting working group.

Targeting Restrictions

4-87. Commanders, leaders, and personnel must understand and apply targeting restrictions regarding—

- The basic principles of the law of armed conflict.
- Rules of engagement.
- General restrictions.
- Precautions in attack.
- Separation of military activities.
- Special protections.
- National sovereignty.
- Environmental considerations.

4-88. Targeting restricted areas, civilian populations, and civilian or protected infrastructure is prohibited under the law of armed conflict. Civilians enjoy protected status unless they participate or take a direct part in combat, singularly or as a group. Likewise, protected infrastructure that harbors combatants loses its protected status. Staffs conduct target analysis and direct the application of information attack, possibly including cyberspace and EW effects.

4-89. Commanders must take positive steps and precautions to avoid excessive incidental civilian casualties and damage to civilian property. Targeting team members should ensure sound intelligence and vetting are used during target development and in selecting enemy objectives, not civilian objects, for attacks. Attacks against installations containing structures that affect natural resources—including dams, dikes, and power generation facilities—must be carefully considered due to the possibility of catastrophic collateral damage.

Deliberate and Dynamic Targeting

4-90. The targeting process breaks down into deliberate and dynamic targeting. Deliberate targets are either scheduled or on-call. Dynamic targeting is used to prosecute targets of opportunity (unscheduled or unanticipated targets).

Deliberate Targeting

4-91. Deliberate targeting prosecutes planned targets. These targets are known to exist in the assigned area and have actions scheduled against them. Examples range from targets on target lists in the applicable plan or order, to targets detected in sufficient time to be placed in the joint air tasking cycle, mission type orders, or fire support plans. Deliberate targeting produces preplanned, scheduled, and on-call targets for operations. The targeting process is scalable and tailorable to fit the operational need and planning horizon of the executing command. Deliberate targeting is used to engage—

- **Scheduled targets**—planned targets upon which fires or other actions are scheduled for prosecution at a specified time.
- **On-call targets**—planned targets upon which fires or other actions are determined using deliberate targeting and triggered when detected or located using dynamic targeting.

Dynamic Targeting

4-92. When planned targets must be adjusted, dynamic targeting provides a methodology for managing changes. Dynamic targeting prosecutes targets not scheduled for action in deliberate targeting or that emerge during an operation. Dynamic targeting provides commanders flexibility for generating effects against targets during an execution period within a compressed timeline. Dynamic targeting may also be employed to create lethal and nonlethal effects against on-call targets. Dynamic targeting prosecutes targets of opportunity, which are categorized as—

- **Unscheduled targets**—targets that are known to exist in the assigned area, but not deliberately included in the targeting schedule for a given time period. As an example, EW elements may detect a fire finding radar placed closer to the forward edge of the battle area than the enemy doctrinal template predicted. The radar might be prosecuted as an unscheduled target.
- **Unanticipated targets**—targets that are neither known nor expected to exist in the assigned area. An unanticipated target could be a known enemy unit assigned to a different theater of operations showing up in the deep area or an enemy air defense radar not known to be employed in the operational area. Refer to ATP 3-60.1 for more information about dynamic targeting.

Targeting in Cyberspace and the Electromagnetic Spectrum

4-93. When nominating targets in cyberspace, it is important to note that the targeting process focuses on targets and desired effects over capabilities. This methodology provides flexible employment of combined arms where multiple capabilities may offer a desired effect. Like any other target, the targeting working group should focus on what effect would achieve the commander's desired end state, and when the effect is needed to support operations. Targeting in cyberspace should match the target and desired effect with available military capabilities. The denial, degradation, disruption, destruction, or manipulation effects can be created through lethal or nonlethal attack capabilities—the delivery mechanism is less important compared to target nomination and validation.

Cyberspace and Electromagnetic Warfare Effects

4-94. When requesting or considering delivering effects through cyberspace or the electromagnetic spectrum, the targeting working group must ensure they integrate closely with their higher joint command. Attacks through cyberspace may have second- and third-order effects outside of the assigned area or theater of operations which require coordination with other combatant commands. The use of an offensive cyberspace capability may preclude its future use against either that target or against any other targets. The attacks may require high-level approvals to evaluate their military utility relative to the value of ongoing intelligence operations and planned future operations and the risk of collateral damage to civilian infrastructure.

4-95. The CEMA section uses electromagnetic support data from organic EW forces to identify targets in the electromagnetic spectrum. These can either be prosecuted as deliberate targets based on the phase of an operation, or as targets of opportunity through dynamic targeting.

4-96. The CEMA section identifies key terrain in cyberspace during intelligence preparation of the operational environment and mission relevant terrain in cyberspace through systems analysis and nominates cyberspace targets through the Army targeting methodology. Key terrain in cyberspace must meet the same criteria as key terrain in the land domain; it must provide a marked advantage to whichever force holds that terrain. This includes cyberspace terrain owned by friendly forces—if the enemy gains control of host-nation cellular or Internet infrastructure, that is an advantage to them—if friendly forces maintain control of the host-nation infrastructure, the advantage lies with the multinational force.

Risk Management

4-97. The CEWO is a key participant in risk management throughout the operations process and as a member of the protection working group. The CEMA section provides subject matter expertise on cyberspace and electromagnetic risk and electromagnetic radiation hazards during operations. Units incur risk by using cyberspace and spectrum-dependent devices and relying on cyberspace or EW capabilities and activities. Threat actions, adjacent friendly forces, and civilian populations can contribute to the cyberspace and EW risk.

4-98. Units can manage risk by applying protection actions such as electromagnetic protection, cybersecurity, operations security, and force protection. They may also implement operational controls such as contingencies, redundancies, and assessments. Frequency deconfliction between the CEMA spectrum manager and the G-6 or S-6 spectrum manager is an example of a protection measure to reduce the risk of frequency fratricide. CEWOs recommend protective measures to mitigate hazards of electromagnetic radiation to personnel, fuels, and ordnance. Units must also consider the operational risk posed by pervasive civilian use of cyberspace- and electromagnetic spectrum-dependent devices throughout their operational environment.

KNOWLEDGE MANAGEMENT

4-99. The CEWO collaborates with the knowledge manager to ensure knowledge management and information dissemination management processes get the right information to the right staff personnel to support targeting and decision making. Units must be prepared to conduct knowledge management in a denied and degraded environment. In some instances, this may require units being prepared to transition to analog planning methods and minimizing or ceasing electromagnetic emissions.

4-100. In collaboration with the G-6 or S-6 and the rest of the staff, the CEWO advises on risk decisions relating to the use of cyberspace- and spectrum-dependent knowledge management systems. They help balance the operational benefits of knowledge management against the limitations and risks within their operational environment and the capabilities of the enemy to maximize resilience and survivability. Refer to ATP 6-01.1 for more information about knowledge management. Refer to ATP 6-02.71 for more information about information dissemination management.

INTEGRATION WITH THE JOINT FORCE

4-101. An *ARFOR* is the Army component and senior Army headquarters of all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command (FM 3-94). The ARFOR headquarters CEMA section integrates with the joint force through the combatant command joint cyber center for cyberspace operations, the joint task force's joint electromagnetic spectrum operations cell for EW, and the joint frequency management office (if not part of the joint electromagnetic spectrum operations cell) for spectrum management operations.

JOINT CYBERSPACE OPERATIONS

4-102. Army units may work as subordinate elements of a joint or combined joint task force, or they may form the core headquarters of a joint or multinational task force. The Army uses its CEMA staff to integrate cyberspace and EW capabilities into the joint and multinational operations processes. If not acting as a joint task force headquarters, the ARFOR headquarters CEMA section coordinates cyberspace operations through the joint task force or the combatant command joint cyber center.

JOINT ELECTROMAGNETIC SPECTRUM OPERATIONS

4-103. Joint electromagnetic spectrum operations include all joint force actions to exploit, attack, protect, and manage the electromagnetic operational environment. Joint electromagnetic spectrum operations rely on personnel and systems from EW, electromagnetic spectrum management, intelligence, space, and cyberspace mission areas. Joint electromagnetic spectrum operations integrate and synchronize EW, spectrum management, intelligence (including SIGINT), space, and other mission areas to achieve electromagnetic spectrum superiority. Instead of these mission areas being planned and executed in a minimally coordinated and stovepiped fashion, joint electromagnetic spectrum operations guidance and processes prioritize, integrate, synchronize, and deconflict all joint force operations in the electromagnetic operational environment, enhancing unity of effort. The result is a fully integrated scheme of maneuver in the electromagnetic operational environment to achieve electromagnetic spectrum superiority and joint force commander objectives (JP 3-85). Figure 4-2 on page 68 shows the joint electromagnetic spectrum operations actions.

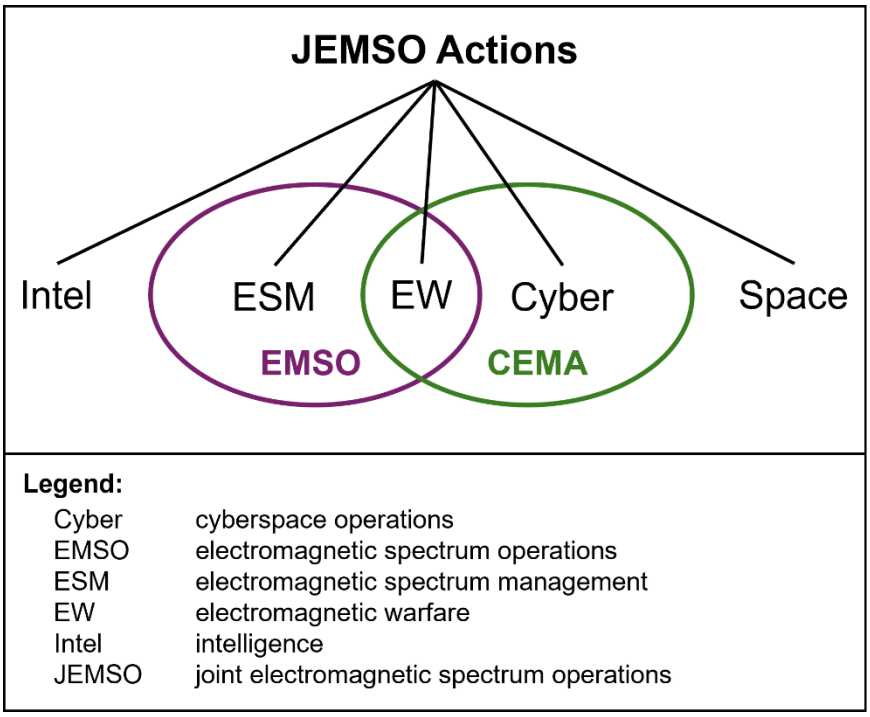


Figure 4-2. Joint electromagnetic spectrum operations actions

Army Approach to Electromagnetic Spectrum Operations

4-104. Each Service has a unique approach to electromagnetic spectrum operations; the Army's Service approach is CEMA. Army commanders and their staffs conduct CEMA to plan, integrate, and synchronize cyberspace and EW operations as a unified effort to project power in and through cyberspace and the electromagnetic spectrum (JP 3-85).

4-105. Component commanders should establish electromagnetic spectrum operations cells (or equivalent) to enable command and control of their respective electromagnetic spectrum operations and to coordinate their electromagnetic spectrum operations with the joint force through the joint electromagnetic spectrum operations cell (CJSCM 3320.01D). For the Army, the theater army CEMA section performs the functions of an electromagnetic spectrum operations cell for all Army forces in the combatant command through the CEMA working group. The ARFOR CEMA section and CEMA working group are the equivalent for a joint task force.

4-106. The CEWO hosts the CEMA working group with representation from maneuver, intelligence, fires, space, information advantage, and spectrum management operations personnel (see paragraph 4-42) to integrate cyberspace operations and EW in operation plans and orders. The G-6 or S-6 spectrum manager participates in the CEMA working group to deconflict friendly spectrum use with EW and SIGINT elements and update the joint restricted frequency list (including TABOO, protected, and guarded frequencies). The ARFOR coordinates EW and spectrum management operations with the joint task force joint electromagnetic spectrum operations cell and joint frequency management office. Refer to ATP 6-02.70 for more information about the roles and responsibilities of the G-6 or S-6 spectrum manager.

Joint Integration

4-107. The joint task force's joint electromagnetic spectrum operations cell coordinates electromagnetic spectrum management with the joint frequency management office, and integrates cyberspace and EW operations with SIGINT, collection management, and space operations to support electromagnetic spectrum superiority. Refer to AR 525-24 for more information about the relationship of CEMA to joint and multinational electromagnetic spectrum operations.

JOINT ELECTROMAGNETIC SPECTRUM OPERATIONS PLANNING

4-108. Joint force commanders centralize joint electromagnetic spectrum operations planning under the designated electromagnetic spectrum coordinating authority and decentralize execution to ensure unity of effort while maintaining tactical flexibility. The joint force prioritizes, integrates, and synchronizes operations in the electromagnetic spectrum to—

- Achieve electromagnetic spectrum superiority.
- Achieve the commander's objectives.
- Mitigate electromagnetic interference.
- Avoid friendly fire electromagnetic attack incidents (frequency fratricide).

Commander's Guidance

4-109. The joint force commander conveys guidance for achieving electromagnetic spectrum superiority within the joint operations area through their concept of operations. Subordinate commanders plan operations within the joint force commander's guidance and intent. The joint force commander's guidance includes—

- Operational approach.
- Mission statement.
- Commander's planning guidance.
- Commander's intent.
- Commander's critical information requirements.

Staff Estimate

4-110. The joint electromagnetic spectrum operations staff estimate forms the basis for the commander's approach to achieve electromagnetic spectrum superiority. The staff estimate is used during course of action development and analysis to determine—

- The spectrum activities and capabilities needed to accomplish the mission.
- The joint electromagnetic spectrum capabilities required to support operations.
- The risk to the operation if electromagnetic spectrum superiority is not achieved.

Joint Electromagnetic Spectrum Operations Appendix

4-111. The joint electromagnetic spectrum operations appendix to Annex C (Operations) of joint plans and orders establishes procedures for command and control of forces conducting joint electromagnetic spectrum operations in the joint operations area and includes spectrum coordination measures, specifying procedures and rules of engagement for joint force use of the electromagnetic spectrum.

4-112. The joint electromagnetic spectrum operations appendix should form the basis of Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) to the ARFOR's operation plan or order to ensure the Army component operates within the higher commander's mission and intent. The ARFOR CEMA appendix becomes the basis of subordinate Army units' CEMA appendixes.

JOINT TARGETING

4-113. While the Army plans effects through the Army targeting methodology—decide, detect, deliver, and assess—as the primary integrating echelon for converged effects, the corps must also integrate into the joint targeting cycle:

- Commander's objectives, targeting guidance, and intent.
- Target development and prioritization.
- Capabilities analysis.
- Commander's decision and force assignment.
- Mission planning and force execution.
- Combat assessment.

4-114. CEMA sections must integrate with the joint targeting cycle to allow time to develop tailored cyberspace and EW capabilities. While the delivery of effects in cyberspace and the electromagnetic spectrum can occur quickly, generating capabilities requires significant planning, preparation, software

development, and iterations of intelligence and reconnaissance operations. Generally, these types of effects are only feasible for deliberate targets that are preplanned during concept plan or operation plan development. Depending on the nature of a capability, it may be able to engage unscheduled targets if the target is exposed for long enough or meets certain conditions. In these instances, using a tailored capability may or may not preclude its future use.

4-115. In the event a division or corps is tasked as the ARFOR or tactical headquarters, the targeting team must be prepared to participate in the joint targeting cycle of the higher headquarters to submit target nominations for joint capabilities. All effects that cannot be created by organic capability must be requested through predetermined channels. Higher headquarters typically prescribe the methods for support requests and target nominations. In addition to participating in the higher headquarters processes, divisions and corps conduct joint targeting working groups and joint targeting coordination boards at their level for echelon-specific synchronization and integration. Working group and board facilitators must be conscious of roles, targeting tasks, and command and support relationships and include all necessary participants. Refer to JP 3-60 for more information about joint targeting.

4-116. Targeting in cyberspace requires close integration with the joint targeting cycle through the joint force commander and combatant command. This integration is necessary for three main reasons:

- Targets engaged through cyberspace must be on an approved joint target list or restricted target list.
- Cyberspace attacks may generate adverse second- and third-order effects that extend far beyond the requesting commander's assigned area.
- National-level intelligence assets may be conducting ongoing exploitation of a requested target. Approval to engage these targets requires a high-level intelligence gain-loss decision, balancing continued intelligence value versus the military utility of engaging the target.

4-117. Other Services employ EW capabilities the corps and joint task force may leverage to engage targets nominated by Army units. Navy and Air Force airborne EW platforms can conduct electromagnetic support sensing and electromagnetic attack in the deep area, which greatly enhances the corps and division's ability to set conditions for lower echelons.

4-118. The CEMA section nominates targets in cyberspace through the Army targeting methodology. Identified targets should support the commander's desired end state and objectives. Units forward CERFs prepared through the Army targeting methodology through their chain of command to the joint task force headquarters, where the CERF is entered into the joint targeting cycle as a request for service. Developing a cyberspace capability to engage targets requires extended lead time and high-level approval. Figure 4-3 on page 71 shows the integration of Army targeting in cyberspace at echelons corps and below with the joint targeting cycle.

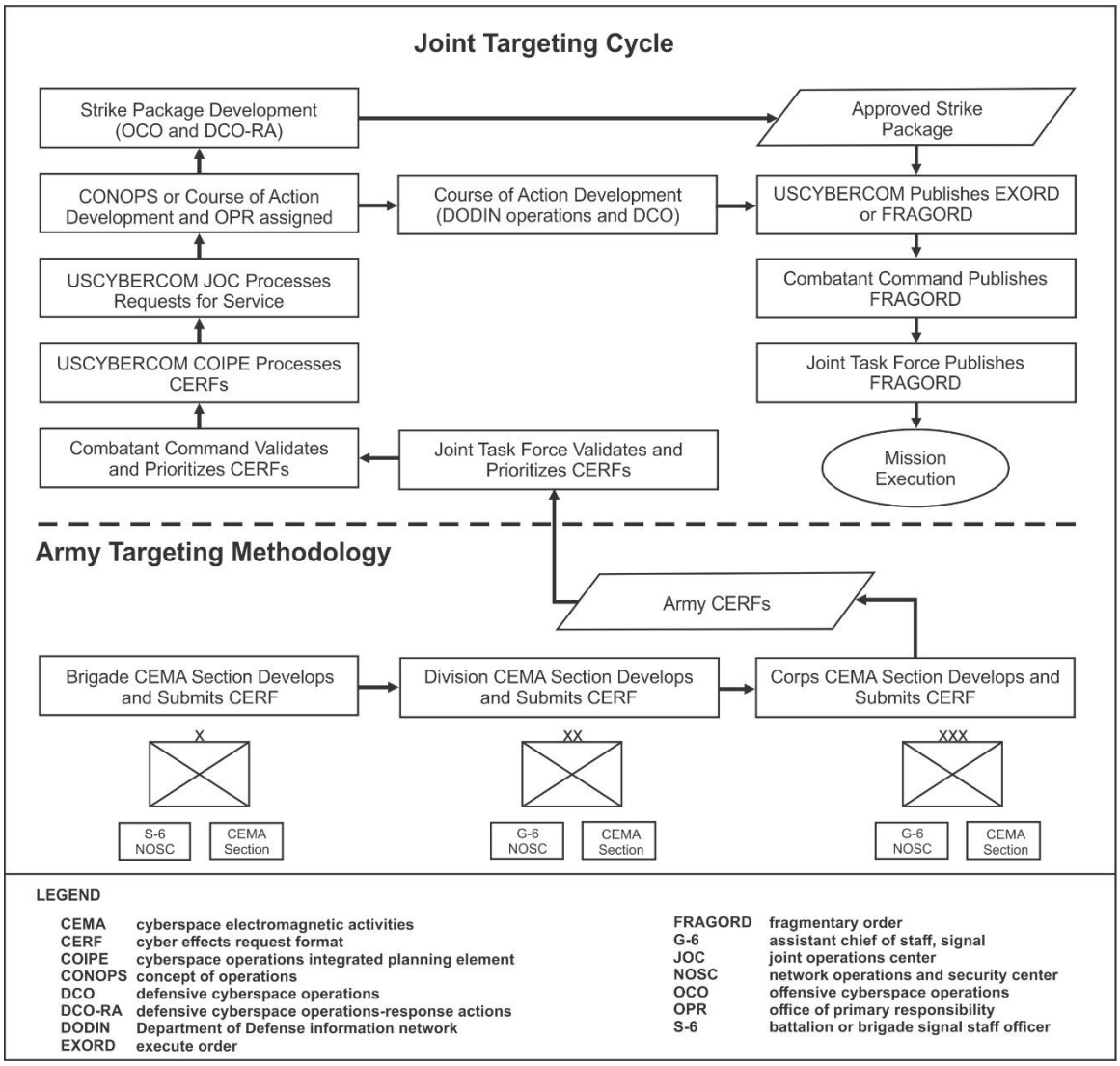


Figure 4-3. Integration of Army targeting with the joint targeting cycle

This page intentionally left blank.

Chapter 5

Cyberspace and Electromagnetic Warfare Operations in Combined Arms

This chapter addresses the contributions of cyberspace and electromagnetic warfare operations in a combined arms approach. The chapter begins with a discussion of convergence, and integration with the joint force. It then discusses cyberspace and electromagnetic warfare operations across the competition continuum.

SECTION I – CONVERGENCE AND INTEGRATION WITH THE JOINT FORCE

5-1. During large-scale combat operations, a corps headquarters normally functions as a tactical headquarters under a joint or multinational land component or as the joint force land component command. The corps is the echelon best positioned and resourced to converge Army and joint capabilities. *Convergence* is an outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area (FM 3-0).

CONVERGING EFFECTS ACROSS DOMAINS

5-2. The corps converges effects in the air, land, maritime, space, and cyberspace domains using organic fires capabilities, subordinate division and brigade combat team fires and maneuver, and support from the joint force, other Services, or multinational partners to apply combat power from and in multiple domains to multiple decisive points. The fires capabilities include both lethal and nonlethal attack or delivery systems. Electromagnetic attack capabilities supporting convergence may come from the division or brigade combat teams' organic EW forces; be provided by supporting Navy or Air Force aerial EW platforms; or be provided by multinational partners. Offensive cyberspace capabilities supporting convergence are provided by national-level cyber forces or multinational partners and require extended planning time and coordination through the combatant command.

5-3. Cyberspace and EW capabilities are key contributors to convergence. Cyberspace and EW effects can affect the function of enemy command and control communications, sensors, radars, electromagnetic countermeasures, and navigation systems. Tactical advantages from denied, degraded, disrupted, destroyed, or manipulated enemy capabilities often come from second- and third-order effects in the air, land, maritime, and space domains as technical equipment temporarily ceases to function as the enemy requires. This creates windows of opportunity to apply combat power to decisive points in other domains to present enemy forces multiple dilemmas they cannot overcome. Refer to FM 3-0 for more information about convergence.

ELECTROMAGNETIC ATTACK

5-4. The cascading effects of an electromagnetic attack on enemy command and control communications may eventually include the enemy adapting their electromagnetic protection tactics, techniques, and procedures. This could include—

- Changing hop sets.
- Using an alternate frequency.
- Using highly directional antennas.
- Changing to alternate communications devices.
- Moving electromagnetic sensors closer to the forward line of enemy troops to geolocate friendly jammers.

5-5. An enemy adapting their tactics, techniques, and procedures requires commanders and their staffs to forecast and plan accordingly and may require friendly maneuver to counter.

ENGAGING CYBERSPACE TARGETS WITH OTHER MILITARY CAPABILITIES

5-6. The CEMA section and targeting working group must do their due diligence in identifying and nominating targets in cyberspace. While units at echelons corps and below do not have organic offensive cyberspace operations capabilities, they can still create effects in cyberspace using available military capabilities. Units may be able to create desired effects in cyberspace by engaging an approved target with lethal fires, electromagnetic attack, maneuver forces, or air attack at critical points in an operation.

COUNTERING AIR AND MISSILE THREATS

5-7. Army EW forces counter the air and missile threat by integrating electromagnetic jamming, electromagnetic deception (decoys), and electromagnetic masking to deny, degrade, or disrupt enemy sensors from producing accurate and timely targeting information regarding friendly units.

SUPPORTING JOINT COMMAND AND CONTROL

5-8. CEMA supports joint command and control through support for joint spectrum interference resolution, situational awareness of friendly electromagnetic signatures, and integration of defensive cyberspace operations with cybersecurity to protect friendly networks.

ENABLING OPERATIONS

5-9. CEMA sections at corps and below and EW elements at division and below support the following enabling operations:

- Reconnaissance operations.
  - Hunt operations.
  - Electromagnetic support.
- Security operations.
  - Cyberspace security (in conjunction with the G-6 or S-6).
  - Electromagnetic protection.
  - Counterreconnaissance.

RECONNAISSANCE OPERATIONS

5-10. Brigade combat team, division, and corps commanders use organic or attached ground or air assets and intelligence elements to accomplish reconnaissance. The purpose of reconnaissance is to gain information about enemy forces or terrain, and to gain and maintain contact with the enemy.

5-11. Electromagnetic support at echelons division and brigade combat team, integrated with organic SIGINT capabilities, contributes to reconnaissance through electromagnetic contact. Additionally, EW teams in the close area may contribute to reconnaissance through direct visual observation and reporting of enemy movements and activities.

Hunt Operations

5-12. Hunt is a tactical mission task undertaken in friendly controlled or contested cyberspace to identify and characterize threat presence and activity on the network. A hunt operation is analogous to reconnaissance and security tasks in the land domain.

5-13. Hunt operations enable offensive and defensive cyberspace operations, DODIN operations, and influence operations. Defensive cyber forces conduct hunt operations to develop the situation and to identify, create, and preserve options to seize, retain, and exploit the initiative. Hunt operations allow commanders to visualize cyberspace in their operational environment, understand the situation, and make decisions. Hunt operations answer commanders' critical information requirements, identify threat activities, and help mitigate cyberspace risk.

5-14. The CEMA section submits information requests through the collection manager to support the commander's understanding of the cyberspace environment in their areas of operations. Tactical information requests are prioritized by supporting defensive cyber forces and theater intelligence units. As information

requirements are answered, the CEMA section updates its running estimate to ensure the commander and staff are aware of friendly, threat, and neutral activities in cyberspace.

Electromagnetic Support

5-15. Electromagnetic contact is one of the nine forms of contact (refer to FM 3-0). Electromagnetic support is a shared mission space between EW and SIGINT forces. EW and SIGINT teams can detect and identify threat emissions, direction find, and geolocate threat emission points of origin. Army SIGINT personnel have the additional mission of in-depth signals analysis, processing, and decryption to generate intelligence about threat activities, plans, and capabilities. Common functions between electromagnetic support and SIGINT include—

- Advising for placement of friendly systems.
- Monitoring the electromagnetic spectrum for friendly awareness (see ourselves).
- Advising for EMCON plans.
- Monitoring for evidence of enemy activity (see the enemy).
- Demodulating unencrypted signals for the purpose of threat identification.
- Supporting the commander's situational understanding (understand the operational environment).
- Enabling tip and cue of assets from the collection plan to support engagement of high-priority targets.

Note. Certain signal analysis tasks are strictly limited to SIGINT teams by National Security Agency policies. Refer to ATP 2-22.6 for more information about SIGINT authorities. Refer to AR 525-24 for more information about signals externals parameters authorities for EW personnel.

SECURITY OPERATIONS

5-16. Cyber forces support security operations through cyberspace security. EW forces support security operations through electromagnetic protection and support to counterreconnaissance.

Cyberspace Security

5-17. Protection in cyberspace consists of coordinated cybersecurity and defensive cyberspace operations. The CEMA section supports the G-6 or S-6 implementing the cybersecurity program to secure the network against known vulnerabilities and identified threat tactics, techniques, and procedures. The CEMA section also collaborates with the joint cyberspace operations integrated planning element and the G-2 or S-2 for current threat information to inform defensive cyberspace operations-internal defensive measures.

Cybersecurity

5-18. Signal personnel in the G-6 or S-6 establish the baseline security of their portion of the Army network by applying the risk management framework and cybersecurity measures, including antivirus updates, software patching, event logging, and analysis to secure the network against known vulnerabilities and exploits and identify unusual network activity. Refer to ATP 6-02.71 for more information about cybersecurity measures.

Defensive Cyberspace Operations

5-19. Local network defenders perform defensive cyberspace operations-internal defensive measures tasks in their respective portions of the Army network. If defensive cyberspace operations capabilities are required beyond the capabilities of local network defenders, the CEMA section submits a request for cyber protection team or expeditionary CEMA team support through the joint force headquarters.

Electromagnetic Protection

5-20. The CEMA section and organic or supporting EW forces support electromagnetic protection by—

- Assisting with terrain analysis as it affects electromagnetic propagation.
- Synchronizing plans for spectrum-dependent capabilities with operations.

  - Fire finding radar.
  - Air defense radar.
  - EMCON plans.
- Supporting joint spectrum interference resolution investigation and reporting activities.

Counterreconnaissance

5-21. Threat forces use a wide range of space-, air-, maritime-, and land-based surveillance, and reconnaissance capabilities to detect and collect information about U.S. forces. Cyberspace and EW capabilities contribute to counterreconnaissance to prevent the threat from collecting critical information through cyberspace and the electromagnetic spectrum.

Cyberspace

5-22. Army forces and individuals are in constant electromagnetic contact with threats who persistently probe and disrupt individual, group, and Army network capabilities. Local network defenders perform defensive cyberspace operations-internal defensive measures to defend the DODIN against enemy cyberspace surveillance and reconnaissance.

Electromagnetic Warfare

5-23. EW and SIGINT elements support counterreconnaissance through the conduct of electromagnetic support to detect, identify and geolocate emitters used by threat reconnaissance elements. EW teams may conduct electromagnetic attack to disrupt threat reconnaissance elements' reporting. Combat information provided by the EW team further informs targeting decisions regarding the employment of lethal or nonlethal capabilities against threat reconnaissance elements.

SECTION II – CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS ACROSS THE COMPETITION CONTINUUM

5-24. The current strategic environment is typified by continuous competition among great powers which challenges the security environment and operational deterrence. Subsequently, today's reality is that commanders face a complex environment that requires employment of available combat power across all domains to accomplish missions across the competition continuum.

RELATIVE WEIGHTING OF EFFORT

5-25. The weighting of effort between cyberspace and EW capabilities varies across the competition continuum. Army units and joint forces must perform defensive cyberspace operations tasks across the competition continuum to defend friendly network capabilities from threat cyberspace activities.

5-26. In competition and crisis, most friendly offensive cyberspace operations take place at the national and theater strategic levels to set conditions in the theater. These activities primarily consist of cyberspace surveillance and reconnaissance and cyberspace exploitation.

5-27. As a crisis transitions to armed conflict, national cyberspace forces will expend most of their available offensive cyberspace capabilities to overcome enemy antiaccess, area denial, and integrated air defense capabilities, enabling U.S. forces to gain physical access to the joint operational area through joint forcible entry operations. After the earliest phases of operations in armed conflict, the available capabilities at echelons corps and below are heavily weighted toward organic and supporting EW assets. Figure 5-1 on page 77 illustrates the relative weighting of cyberspace and EW capabilities across the competition continuum.

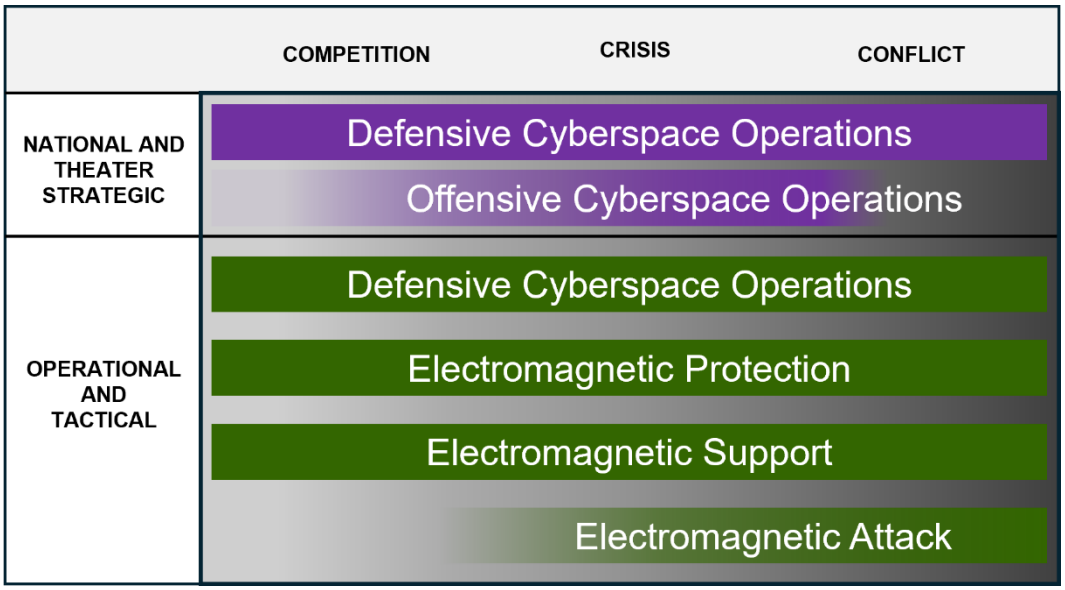


Figure 5-1. Cyberspace and electromagnetic warfare across the competition continuum

COMPETITION

5-28. Competition activities include obtaining access for U.S. forces, maintaining sufficient forward-based presence within a theater to influence conditions in the strategic environment, and mitigating conditions that could lead to a crisis or armed conflict. At any time during competition, but especially during times of heightened tension, leaders must take great care to ensure Army forces avoid activities that may provoke crisis or armed conflict. U.S. forces attempt to create favorable conditions in theater to support military operations without crossing the threshold that might provoke an armed response. Army forces play an integral role in this effort, actively engaging across domains (including space and cyberspace) and in the electromagnetic spectrum. The goal is to enable the defeat of adversary information warfare and hybrid threat, conduct intelligence operations, counter threat reconnaissance, and demonstrate credible deterrence.

SETTING THE THEATER

5-29. The ability to effectively compete below the level of armed conflict and to respond to escalation toward armed conflict is necessary to establish a position of strength and set favorable conditions if conflict ensues. This position of strength provides a favorable environment for the Army and mission partners' efforts to counter adversary coercion. The combined and persistent effects of defeating adversary information warfare capabilities and hybrid threat during competition generate additional friendly options and demonstrate credible deterrence. The combatant command, theater army, multi-domain task force, and units at echelons corps and below have important roles in setting the theater for future operations.

Combatant Command

5-30. An essential step in setting conditions for armed conflict in a theater involves organizing assigned and allocated forces for employment. Clear command relationships between current and projected units are essential. Combatant commanders expect the command relationship between the supporting and supported commands may change based on evolving situations.

5-31. During competition, the combatant command, affected country teams, Service components, and special operations forces execute the theater campaign plan to create conditions in the theater favorable to U.S. interests and prepare for anticipated military operations. The theater campaign plan—

- Integrates target development during competition and crisis.
- Ensures the combatant commander's strategic communications initiatives are fully integrated and convey clear messages to multinational partners, friendly populations, and adversaries.

- Connects posture changes to the DOD's global cyberspace and EW campaign plans and provides a vehicle for continuously reassessing posture needs, refining those needs, and updating the DOD and regional posture plans accordingly.
- Enables the DOD to synchronize theater strategic cyberspace and EW plans with current priorities to allocate resources addressed through contingency plans.

5-32. Combatant command activities to set the theater may include—

- Electromagnetic support to develop situational understanding of the electromagnetic spectrum in theater—
  - Understand friendly electromagnetic signatures and take steps to reduce or mitigate the signatures.
  - Understand neutral use of the electromagnetic spectrum in theater.
  - Understand adversary use of the electromagnetic spectrum and characterize adversary emitters.
  - Develop targets in case the situation transitions to armed conflict.

Note. The Defense Information Systems Agency and the Joint Electromagnetic Warfare Center collaborate with the intelligence community to include threat and neutral electromagnetic order of battle data sources.

- Intelligence and counterintelligence activities, including cyberspace surveillance and reconnaissance and SIGINT to—
  - Understand friendly cyberspace signatures and vulnerabilities.
  - Understand adversary use of cyberspace and identify adversary weaknesses to exploit.
  - Identify the adversary's antiaccess and area denial capabilities.
  - Develop targets in cyberspace to support joint forcible entry operations.
  - Develop the electromagnetic order of battle and threat template to generate flexible options for effects delivery against critical adversary links and nodes.
- Offensive and defensive cyberspace operations.
- Operations in the information environment (refer to JP 3-04).
- Determine how to 'live off the land,' using existing host-nation communications infrastructure to reduce electromagnetic signatures and the risk of detection.
  - Understand network design and architecture in potential host nations.
  - Inventory hardware to determine what systems friendly nations use.

Theater Army

5-33. The theater army contributes to an integrated cyberspace and EW plan to support joint operations. The theater army supports the combatant commander's campaign plan by planning Army use of cyberspace and EW capabilities. During competition, the theater army supports the combatant command in conducting missions, tasks, and actions that shape the environment to assure friends, deter adversaries, and establish conditions for future contingencies. The theater army develops contingency plans to support the combatant command plan. Well in advance of crisis or armed conflict, the theater army ensures the Army's targeting requirements are represented during the development of the joint target list, restricted target list, and no-strike list.

5-34. During competition, the theater army staff generates thorough understanding of friendly, adversary, and neutral use of cyberspace and the electromagnetic spectrum in theater to identify—

- Friendly vulnerabilities.
- Possible targets in cyberspace.
- Adversaries' critical spectrum-dependent capabilities.

5-35. Early targeting during competition is critical to get cyberspace targets supporting joint forcible entry operations into the joint targeting cycle, approved, and forwarded to USCYBERCOM to develop offensive cyberspace capabilities to engage the targets in conflict.

Multi-Domain Task Force

5-36. During competition, the multi-domain task force may be forward stationed in a combatant commander's area of responsibility to employ joint and Army capabilities in support of target development. The multi-domain task force headquarters coordinates and synchronizes space, cyberspace, EW, and intelligence operations of its assigned formations with other theater (including theater army and combatant command) and national assets. The multi-domain task force is designed to operate in a distributed fashion while retaining the ability to deliver effects that create opportunities for joint force exploitation. Based on the mission variables of METT-TC (I), the multi-domain task force may be augmented with capabilities from across the warfighting functions.

Corps and Division

5-37. During competition, corps commanders base their planning and decisions on a continually evolving understanding of their operational environment. Integrated EW, SIGINT, and cyberspace capabilities collect against and analyze adversary systems and other factors of the operational environment and civil networks. This effort builds situational understanding and helps bridge between operational-level plans and tactical planning and execution. The division EW company conducts surveys of the electromagnetic spectrum in conjunction with SIGINT and space support elements to support situational understanding in the electromagnetic spectrum and space.

5-38. The division EW companies assist in countering adversary electromagnetic deception while supporting counterreconnaissance by detecting, identifying and geolocating emitters used by adversary reconnaissance elements. Collectively, these actions enable the joint force to rapidly transition to armed conflict and create uncertainty for the adversary as to whether it can achieve its objectives through a surprise attack.

5-39. The division EW companies integrate EW activities with SIGINT and cyberspace operations to complicate the adversary's efforts to determine the capability and capacity of friendly forces in theater. While exercises, training, and alerts demonstrate capabilities, they also provide opportunities to mislead adversaries regarding friendly use of the electromagnetic spectrum, cyberspace signatures and patterns, and methods of employment. These actions create unpredictability and complicate the adversary's reconnaissance efforts, which increases the likelihood of compromising adversary assets.

5-40. The corps and division CEMA chiefs assist the brigade combat team CEWOs with integrating and synchronizing cyberspace targeting into the targeting process and provide insight into cyberspace capabilities. The CEMA chiefs collaborate with CEWOs in vetting and processing target nominations from subordinate units for effects in cyberspace. The CEMA chiefs—

- Assist CEWOs in the integration, coordination, and synchronization of cyberspace and EW targeting.
- Provide CEWOs information about the effects of cyberspace operations, including associated rules of engagement, impacts, and constraints used to advise the commander.
- Assist CEWOs with developing and maintaining a consolidated targeting synchronization matrix.
- Assist in nominating cyberspace targets through the combatant command.
- Assist CEWOs in monitoring and assessing measures of performance and effectiveness while maintaining updates on cyberspace operations' effects on the operational environment.
- Assist CEWOs in requesting and coordinating offensive cyberspace operations support as needed.
- Integrate supporting cyber mission forces into operations.
- Coordinate with multinational partners for cyberspace capabilities that complement or enhance joint and Army cyberspace capabilities.
- Coordinate and deconflict cyberspace and EW operations with the G-2 or S-2 and the G-6 or S-6.
- Assist in performing target systems analysis and target nomination for development of electromagnetic attack techniques to meet higher headquarters objectives.

Note. Division EW companies and their equipment sets are in the process of fielding across the force. Not all divisions will have these formations in place until fielding is complete.

Brigade Combat Team

5-41. The brigade CEMA section—

- Plans operations for organic EW forces.
- Prepares requests for external cyberspace and EW support.
- Nominates targets in cyberspace.
- Integrates effects.
- Assesses cyberspace and EW effects in the brigade's assigned area.

5-42. Forward-deployed brigade combat teams assess and improve protection actions (including defensive cyberspace operations and electromagnetic protection) against adversary capabilities and promote interoperability with multinational partners' tactical units. While most rotational brigades' training occurs in the continental United States and does not involve partner nation forces, brigade combat teams should anticipate the need for multinational integration and plan and train using the multinational secret-releasable mission partner network to integrate with mission partners.

5-43. During competition, forward-stationed brigade combat team EW platoons conduct electromagnetic support to identify and locate threat emitters and spectrum-dependent devices within the brigade's assigned area. Information gathered through electromagnetic support provides the commander with critical decision-making and targeting support. This data and information also support electromagnetic battle management by providing continuous situational understanding to the CEMA spectrum manager to develop and update the common operational picture.

COMPETITION ACTIVITIES

5-44. During periods of competition, Army units conduct operations to shape the operational environment in theater to support the combatant commander's campaign plan. Competition activities include—

- Force protection.
- Security cooperation.
- Security assistance.
  - Security force assistance.
  - Foreign internal defense.
  - Security sector reform.
- Nuclear deterrence and countering weapons of mass destruction.
- Humanitarian assistance.

Force Protection

5-45. Cyber and EW forces at echelon, supported by SIGINT elements, support force protection through—

- Electromagnetic support to—
  - Understand friendly electromagnetic signatures and take steps to mitigate.
  - Detect and geolocate adversary emissions.
- Support to planning and validation of EMCON procedures.
- Multi-spectral camouflage—camouflage that attempts to hide objects in the visible, infrared, and radar portions of the electromagnetic spectrum.
- Defensive cyberspace operations.
- Support to influence operations dissemination.

Security Cooperation

5-46. Cyber and EW forces participate in security cooperation activities to deter aggression against partner nations, reassure allies and partners of U.S. resolve, and maintain the period of competition. The combatant command coordinates security cooperation activities with the Department of State country team.

5-47. Security cooperation includes—

- Cyber and EW exchanges with allies.
- Assistance in securing and defending allies' military or civilian cyberspace.
- Cyberspace- and EW-specific multinational exercise objectives.

- Collaboration to enable friendly nations to defend their own cyberspace and electromagnetic spectrum.

Security Assistance

5-48. Security assistance is a group of programs by which the U.S. Government provides defense articles, military education and training, and other defense-related services to eligible foreign governments by grant, loan, credit, cash sales, or lease. The Department of State supervises and directs the U.S. Government's security assistance programs, in consultation and coordination with the DOD and other government entities. Security assistance programs include—

- Security force assistance.
- Foreign internal defense.
- Security sector reform.

Security Force Assistance

5-49. DOD security force assistance activities help strengthen multinational partners' security forces. The DOD works with other U.S. government agencies to train and equip foreign security forces and help partners develop better organizations and systems. Security force assistance programs support either individual partner nations or regional security organizations (such as North Atlantic Treaty Organization) in addressing security issues. The goal is to help these countries become more secure and capable, which ultimately helps the United States achieve its own goals.

5-50. Army forces conduct security force assistance as part of the combatant commander's campaign plan. Units conducting security force assistance may conduct electromagnetic spectrum surveys to gain situational understanding of the electromagnetic spectrum in the host nation or conduct combined EW training with host-nation forces. Cyberspace forces' participation in security force assistance might include steps to secure and defend friendly, host-nation, or allies' military or civilian cyberspace.

Foreign Internal Defense

5-51. Foreign internal defense activities attempt to establish, consolidate, and transfer control of security, political and economic stability where threats exist. The goal of foreign internal defense is to ensure effective and legitimate global, regional, and local information is distributed and protected. Cyber and EW forces' foreign internal defense activities may include cyberspace defense and electromagnetic protection approaches to protect allies' communications infrastructure, gain support of a population, disrupt adversary control over the population, and disrupt the adversary's relations with the international community. U.S. forces can contribute to defense of multinational partners' military and civilian critical infrastructure through cyberspace defense and electromagnetic protection. Refer to JP 3-22 and ATP 3-05.2 for more information about foreign internal defense missions.

Security Sector Reform

5-52. The objective of security sector reform is to help host-nation governments provide effective, legitimate, and accountable security for their citizens, consistent with the rule of law. Conducting electromagnetic spectrum surveys, verifying friendly emitters, and conducting host-nation frequency coordination help host-nation governments respond appropriately to adversary actions within and outside their borders.

Nuclear Deterrence and Countering Weapons of Mass Destruction

5-53. Due to their operational and strategic importance, weapons of mass destruction targets are different from other tactical targets. These targets present increased risk to friendly forces and civilians, more destructive effects on strategic or key operational terrain, and unique mitigation requirements. The identification and prioritization of targets drive the development and allocation of reconnaissance, targeting guidance, and fires assets.

5-54. EW and SIGINT may provide critical reconnaissance capabilities to support targeting for countering weapons of mass destruction. The possibility of catastrophic second- or third-order effects when engaging a weapons of mass destruction site might make cyberspace attack or electromagnetic attack the most

appropriate capability to engage it. Offensive cyberspace targets will likely need to be engaged by national-level assets, while electromagnetic attack would probably be delivered by forces closer to the target site.

Humanitarian Assistance

5-55. Planning with nongovernmental organizations may be necessary for foreign humanitarian assistance, peace operations, and civil-military operations. Incorporating these organizations into an operation requires the commander to balance the need of the nongovernmental organization for information with operations security concerns. Planning for the inclusion of nongovernmental organizations into civil-military operations will likely involve cybersecurity coordination with nongovernmental partners. Army network defenders may need to assist nongovernmental partners securing shared network resources.

CONSOLIDATION OF GAINS

5-56. Consolidation of gains is an integral and continuous part of competition, and it is necessary for achieving success across the competition continuum. Successful consolidation of gains in competition requires a realistic and pragmatic assessment of—

- Strategic conditions.
- Allies and partners' legitimacy.
- Friendly and adversary relative advantages.
- The viability of a sustainable political outcome.

5-57. Local network defenders consolidate gains by maintaining defense of their respective portions of the network. If required and authorized, cyber defenders may assist partner nations and host-nation civil authorities securing and defending networks and critical infrastructure against malicious cyberspace activity.

TRANSITION TO CRISIS

5-58. Army forces and leaders anticipate the potential for armed conflict in their assigned areas. This is informed by input from the intelligence community and direction from strategic-level leaders. Security force assistance brigades and other regionally-aligned forces maintain access to sensitive areas and allied and partner nation leaders. Their access and robust communications enable them to gain insight into actual conditions on the ground and provide near real-time updates to decision makers in fluid situations. Decisions made before and during the initial stages of a crisis have significant impact on adversary decisions and the ultimate outcome of a particular situation.

CRISIS

5-59. A *crisis* is an emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives (JP 3-0). The joint force competes to seek advantages relative to adversaries during crisis. Army forces play an integral role in this effort, actively engaging across domains (including space and cyberspace) and in the electromagnetic spectrum. The goal is to—

- Consolidate gains in cyberspace into relative advantages.
- Enable the defeat of adversary information warfare and hybrid threat.
- Enable information collection.
- Counter adversary reconnaissance activities.
- Demonstrate credible deterrence.

5-60. Adversary forces conduct a detailed analysis of their available capabilities, capacity, and operational reach within a theater relative to friendly forces; their overall desired end state; and their willingness to achieve that end state before deciding to escalate. A regional peer may have an inherent numerical and proximity advantage over U.S. forces operating in an overseas theater. The adversary will attempt to prevent U.S. forces from overcoming their relative advantages.

BEGINNING OF CRISIS

5-61. Once a crisis starts, adversaries use all capabilities at their disposal to disrupt the deployment of Army forces. They will attempt to prevent the Army and the joint force from obtaining the time needed to deploy and build combat power. This chaos, with its resultant frictions, is the environment into which Army forces will respond. Army cyber and EW forces at echelon support early identification of transition to crisis through the reporting of relevant indicators and warnings of adversary activity in cyberspace and the electromagnetic spectrum.

INITIAL EMPLOYMENT OF FORWARD-STATIONED FORCES

5-62. Army ground-based EW capabilities must be placed forward on terrain advantageous for the detection of electromagnetic emissions or the conduct of electromagnetic attack. Airborne EW capabilities require sufficient altitude and proximity to produce accurate lines of bearing which can produce or refine targeting information. Due to the possibility of extreme distances, electromagnetic support information may require confirmation by other intelligence, surveillance, and reconnaissance capabilities to produce actionable targets.

COUNTERING ADVERSARY ACTIVITIES IN CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

5-63. Two key information activities are protecting friendly information and attacking the adversary's ability to communicate, sense, make effective decisions, and maintain influence with relevant actors and populations. Cyberspace and EW capabilities are key to both functions. The goal is to make better decisions faster than the adversary.

Cyberspace

5-64. Adversaries are likely to calculate that they can conduct malicious cyberspace activities against U.S. networks to deny friendly forces this critical enabler without crossing the threshold which would elicit an armed response. In crisis, the adversary will attempt to penetrate U.S. networks, either to collect intelligence about U.S. capabilities, disposition, and intentions, or to plant malicious code to disrupt the friendly network. Local network defenders conduct defensive cyberspace operations-internal defensive measures to defeat adversary attempts to collect information from or otherwise disrupt the Army network.

5-65. In crisis, authorities to attack adversary systems will be limited and likely retained at the national level. CEMA sections identify, nominate, and continuously refine possible targets in cyberspace for engagement by higher echelons. If available, cyberspace effects delivered by higher echelons can enable operations at echelons corps and below. Units develop and refine their high-priority target lists in case the crisis escalates to the point U.S. forces need to engage approved targets with available military capabilities.

Electromagnetic Spectrum

5-66. Electromagnetic protection helps protect friendly spectrum-dependent devices from adversary direction finding, geolocation, and intelligence collection. Denying the adversary's ability to collect information through the study of U.S. emissions helps complicate the adversary's decision cycle. CEMA sections nominate targets in the electromagnetic spectrum. EW forces prepare to conduct electromagnetic attacks to disrupt the adversary's communications, fire control systems, information warfare capabilities, and other spectrum-dependent capabilities. EW and SIGINT elements conduct electromagnetic support sensing and direction finding to develop situational understanding of adversary emitters in their assigned area. The direction-finding data contributes to the threat template and common operational picture.

SUPPORT TO OPERATIONS SECURITY

5-67. Operations security to deny the adversary information about friendly forces is vital to the success of operations during crisis. Effective operations security makes it harder for adversaries to identify units and their locations and plan operations against them if the crisis escalates to armed conflict.

5-68. Units and individuals contribute to operations security through disciplined use of cyberspace. Protective measures include—

- Cybersecurity program compliance.
- Individuals following cybersecurity best practices.
- Secure access controls.
- Defensive cyberspace operations.
- Adhering to social media policies for both official and personal social media accounts.
- Limiting or eliminating use of personal electronic devices.

5-69. Units employ electromagnetic protection—including EMCON—to support operations security. Electromagnetic protection measures to support operations security include—

- Minimizing electromagnetic emissions.
- Limiting the duration of radio transmissions to the maximum possible extent.
- Limiting use of personal cell phones, particularly those with U.S. provider subscriber identification modules.

Note. Refer to ATP 6-02.53 for techniques to minimize emissions and limit the duration of radio transmissions.

CREATING AND EXPLOITING RELATIVE ADVANTAGES

5-70. Commanders seek to achieve relative advantages over adversaries in the physical, information, and human dimensions of their operational environment. Army forces build upon the physical, information, and human advantages gained during competition to mitigate friction, deter adversaries, and when necessary, transition into armed conflict.

Physical Advantages

5-71. If there is key or decisive terrain, Army forces and host-nation partners may seek to deter adversaries by setting a defense of that ground early in a crisis. Army forces combine capabilities in multiple domains to control key terrain and deny it to adversaries. Electromagnetic support and electromagnetic attack capabilities may contribute to the converged approach to controlling key terrain.

Information Advantages

5-72. During crisis, commanders lead their staffs to refine information activities based upon plans and processes developed during competition. One of the challenges as a multinational force responds to a crisis is building, securing, and defending the secret-releasable mission partner network to enable secure information sharing during operations. Cybersecurity personnel and local network defenders secure the U.S. portion of the mission partner network and may need to assist mission partners' network security and defense. Army forces implement EMCON and electromagnetic masking to deny adversaries the ability to collect information about friendly forces' position, strength, and disposition through the electromagnetic spectrum.

Human Advantages

5-73. While forward-stationed units commonly train with host-nation and other allied forces, those deploying into an operational area from home stations will likely have limited experience collaborating with host-nation and other multinational partner forces. This requires leaders to focus their staffs on the most critical interoperability tasks necessary for effective multinational operations. A critical element in interoperability is information exchange. Units consider the releasability of classified information to multinational partners and establish the classified mission partner network to enable interoperability. CEMA sections and EW forces share situational awareness of the electromagnetic spectrum with mission partners to enable interoperability.

SUPPORT TO THE JOINT FORCE

5-74. Army forces plan, prepare, execute, and assess cyberspace and EW operations in collaboration with joint forces and multinational partners as required. Army commanders and staffs will likely coordinate or interact with joint forces to enable cyberspace and EW operations. For this reason, commanders and staff

should be aware of joint planning systems and processes that enable cyberspace and EW operations. Some of these systems and processes include—

- The joint planning process (refer to JP 5-0).
- Adaptive planning and execution (refer to JP 5-0).
- Joint electromagnetic spectrum operations (refer to JP 3-85).
- Review and approval process for cyberspace operations (refer to JP 3-12).

FORCE PROJECTION AND CONTESTED DEPLOYMENT

5-75. *Force projection* is the ability to project the military instrument of national power from the United States or another theater in response to requirements for military operations (JP 3-0). The demonstrated ability to project Army forces into an operational area is an essential element of conventional deterrence. Army forces depend almost entirely upon joint lift capabilities for deployment.

Opening the Theater

5-76. In the transition to crisis, USCYBERCOM sends forces forward to theater to provide subject matter expertise in cyberspace operations. USCYBERCOM collaborates with other specialized units to assist with planning other information activities into their operations.

Mobilization

5-77. During mobilization, adversaries will conduct malicious cyberspace activities to collect intelligence or disrupt network capabilities. They may also attempt to sabotage critical infrastructure—for example, aerial ports and seaports of embarkation, fuel distribution, or utilities—through malicious cyberspace activities. Local network defenders conduct defensive cyberspace operations-internal defensive measures to protect the DODIN from adversary malicious cyberspace activities. See paragraph 5-84 for responsibilities for protecting federal civilian, state, and private sector networks.

Deployment from Home Station

5-78. Peer threats will attempt to interfere with the Army formations deploying from home station, in transit to the theater of operations, and at aerial ports and seaports of debarkation. Theater army, corps, and division staffs coordinate closely to identify information and assets that need protection, and they request and apply appropriate protection and security measures consistent with their collective threat analysis. Cybersecurity, defensive cyberspace operations-internal defensive measures, and electromagnetic protection actions support protection by securing and defending the DODIN-A.

5-79. Adversary information warfare can be conducted at a very low cost compared to conventional warfare methods, and these operations may have global reach. Adversaries will conduct strategic information warfare to slow or otherwise degrade force projection. Adversary information warfare activities to disrupt deployment from home station may include—

- Targeted content sent through social media, e-mail, or other means designed to frighten and distract deploying Soldiers and their families.
- Malicious cyberspace activities against—
  - Soldiers and family members' banks and credit agencies, cutting off or disrupting access to personal funds.
  - Civilian infrastructure—including transportation, supply, fuel, and navigation—used to support military operations.
  - The DODIN to disrupt communications between units, installations, and civilian partners that assist in deployment.
- Disinformation designed to—
  - Undermine the legitimacy of, or otherwise reduce support for, U.S. Government action.
  - Incite civil unrest in local communities and along rail and road lines of communications that deploying forces need or plan to use to reach ports of embarkation.
  - Reduce trust in future official communications from government, law enforcement, or military officials by releasing disinformation that appears genuine but contains incorrect or confusing information.

5-80. As U.S. forces transition from crisis to armed conflict, adversaries will likely increase the intensity and lethality of their attacks within the homeland. This could include sabotaging critical military and civilian infrastructure by pre-positioned agents or malicious cyberspace activity.

5-81. Defensive cyberspace operations and electromagnetic protection are key capabilities in the integrated approach to countering threat information warfare. Refer to ADP 3-13 for more information about protecting friendly information, data, and networks.

Fort to Port

5-82. Army forces at all echelons must comprehensively assess threat capabilities that may impede deployment in a contested environment. Units should account for being under constant observation in all domains and take steps to mitigate adversaries' ability to collect critical information through the protect information activity, including safeguarding information about deployment timelines and locations, maintaining dispersion of critical assets, and securing friendly networks and data.

5-83. Successful fort-to-port deployment involves coordination and collaboration with numerous civilian partners. Besides attacks on the DOD network, adversaries may conduct malicious cyberspace activity on critical civilian infrastructure to disrupt movement of forces from home station to an aerial or seaport of embarkation. Units must balance the value of the use of computers and data to plan and support operations with the risk of adversary malicious cyberspace activity. The effects of adversary malicious cyberspace activity on critical military, national, or private infrastructure could halt or delay unit deployment operations before units have departed the continental United States.

5-84. Planning to mitigate deployment disruptions requires collaboration between the deploying unit, the installation, appropriate federal, state, and local government and law enforcement agencies, and U.S. Army Reserve and Army National Guard elements. Installations build these relationships during competition. Installations and mission partners develop understanding of how threats will likely affect their local areas by modifying their threat working groups to incorporate relevant military, government, and other local and regional stakeholders. The working group shares information about threat efforts to promote civil unrest, cyberspace vulnerabilities that may adversely affect critical transportation infrastructure, and other adversary activities that may impact deployment operations. Mitigation planning includes establishing cyberspace defenses for systems and associated data used to support movement. Responsibility for defending some of these systems may fall under the Department of Homeland Security; state, local, or tribal governments; or private industry. Shared information about threat capabilities, tactics, techniques, and procedures contributes to a holistic defense of critical networks and infrastructure. Prior understanding of the operational environment, dependencies on cyberspace and spectrum-related capabilities, dependencies on data, and the roles of mission partners is critical to mitigation planning.

Reception, Staging, Onward Movement, and Integration

5-85. During reception, staging, onward movement, and integration, U.S. forces and host-nation civilian infrastructure are vulnerable to malware, denial-of-service attacks, and phishing as ways to conduct brute force attacks. Local network defenders perform defensive cyberspace operations-internal defensive measures within their capabilities. The G-3 or S-3 requests support through higher headquarters if they determine adversary malicious cyberspace activity is beyond the scope of local network defenders.

Initial Employment of Forces

5-86. Army forces have limited ability to conduct large-scale defense on initial arrival in theater until sufficient forces arrive. On early entry, signal elements of the deploying forces establish the initial network connectivity for reachback to the sustaining base and to support the flow of follow-on forces into theater.

5-87. Adversaries will attempt to disrupt communications and network capabilities at aerial ports and seaports of debarkation. Electromagnetic protection, cybersecurity, and defensive cyberspace operations-internal defensive measures are critical to secure and defend the network as units arrive in theater.

CYBERSPACE AND ELECTROMAGNETIC WARFARE ROLES DURING CRISIS

5-88. As competition transitions to crisis, Army forces will deploy into theater to deter adversaries from conflict. Adversaries will use cyberspace and EW capabilities to interfere with force projection and gain intelligence on friendly positions, disposition, and capabilities.

Joint Force Commander

5-89. At the onset of a crisis that may escalate into armed conflict, the combatant commander generally designates a joint task force to provide operational control of all Service components supporting the operation. If the Army is designated the lead Service in the joint task force, the role of commander, joint task force usually falls to the corps commander. If another Service is the designated joint task force lead, the corps will provide augmentation to the joint task force headquarters. The lead Service in the joint task force will stand up a joint electromagnetic spectrum operations cell and a joint cyber center, with augmentation from the other Service components. Refer to JP 3-85 for more information about the role of the joint electromagnetic spectrum operations cell and JP 3-12 for more information about the role of the joint cyber center.

Theater Army

5-90. As forces deploy into theater, the theater army exercises administrative control of all Army forces allocated to the combatant command to support the operation. The theater army CEMA section disseminates situational awareness of cyberspace and the electromagnetic spectrum to corps, divisions, and brigade combat teams in theater. The theater army CEMA section continues to develop cyberspace and EW targets for engagement in case the crisis escalates to armed conflict.

Corps

5-91. As the primary integrating echelon for multidomain convergence, the corps' CEMA section integrates subordinate divisions and brigade combat teams' EW activities and CEMA reporting. The corps CEMA section reports to the joint task force joint cyber center (for cyberspace operations) and joint electromagnetic spectrum operations cell for EW. The G-6 spectrum manager reports to the joint electromagnetic spectrum operations cell for spectrum management operations. During crisis, the corps CEMA section participates in the targeting process to nominate cyberspace and EW targets in the corps deep area and validate target nominations from subordinate divisions and brigade combat teams.

Note. Per AR 525-24, the Army uses its CEMA staff to integrate cyberspace and EW capabilities into the joint and multinational operations process. The theater army or ARFOR CEMA section coordinates cyberspace operations with the joint cyber center and EW with the joint task force joint electromagnetic spectrum operations cell. The corps G-6 coordinates spectrum use with the joint electromagnetic spectrum operations cell. The joint task force integrates EW and spectrum management into joint electromagnetic spectrum operations.

Division

5-92. The division CEMA section nominates cyberspace and EW targets in the division deep and close areas and validates targets nominated by subordinate brigade combat teams. The division EW company and SIGINT elements conduct electromagnetic support in the division's assigned area to develop thorough situational understanding of friendly, adversary, and neutral use of the electromagnetic spectrum. This baseline understanding helps the division EW elements better characterize adversary activities in the electromagnetic spectrum in case the crisis transitions to armed conflict. The division EW company also augments subordinate brigade combat teams' EW platoons in the close area.

Brigade Combat Teams

5-93. During crisis, the brigade EW platoons conduct electromagnetic support to understand friendly, adversary, and neutral use of the electromagnetic spectrum in the brigade's assigned area. Understanding

friendly spectrum use informs electromagnetic protection efforts, including EMCON plans. The brigade CEMA section participates in the targeting process to nominate cyberspace and EW targets in case the crisis escalates to armed conflict.

CONSOLIDATION OF GAINS

5-94. During and after crisis response, Army forces consolidate gains to deny adversary forces the means to extend the crisis or create a similar crisis in the future. This will often entail maintaining an enhanced force posture in a joint operations area to demonstrate the United States' continued willingness to defend allies and partners. Army cyber and EW forces may be called on to support improvements to host-nation cyberspace defense and EW capabilities through a security cooperation plan to make them less vulnerable to future crises. If an adversary directly targets partner nations' military or civil networks, joint or Army cyber forces may need to help the partner nation reconstitute, secure, and defend their networks.

TRANSITION TO COMPETITION OR ARMED CONFLICT

5-95. There are two outcomes of a crisis—a de-escalation to competition or an escalation to armed conflict. Transitions are typically points of friction. Commanders emphasize information collection before and during transitions to maintain a detailed understanding of the adversary and continuously assess the situation so they can position their forces to retain the initiative.

5-96. Cyberspace surveillance and reconnaissance and electromagnetic support contribute to situational understanding of cyberspace and the electromagnetic spectrum in the unit's assigned area. EW and SIGINT forces conduct direction finding and geolocation of adversary emitters to help assess adversary positions, capabilities, and disposition.

Transition Back to Competition

5-97. During a crisis, partner nation security forces and government institutions may suffer losses that reduce their capability and capacity due to the actions of adversary or proxy forces. Army forces may be tasked to execute security cooperation programs to help restore or maintain partner nation capabilities and capacity to consolidate gains. Army forces seek to restore partner nation security forces and government institutions as quickly as possible to maintain popular support. Army cyber forces may be called on to help secure partner nation military or civilian network infrastructure in the transition back to competition.

Transition to Armed Conflict

5-98. Army forces responding to a crisis are prepared to and expect to fight. This saves time during the transition and requires an understanding of the operation plan or likely concept of operations as early as possible. Units continue to defend the DODIN against adversary malicious cyberspace activity. EW forces locate adversary emitters for situational awareness and targeting. CEMA sections at echelons corps and below continue to nominate cyberspace and EW targets for lethal or nonlethal attack in case the force transitions to armed conflict.

ARMED CONFLICT

5-99. Armed conflict causes significant changes to regional security environments. The corps and division EW companies provide a persistent presence to ensure the new security environment is advantageous for U.S. forces and mission partners. The corps and division CEMA sections coordinate with the combatant command and joint task force headquarters to best adapt force posture to the changing operational environment. This ensures Army EW forces retain the ability to immediately counter aggression and enables maneuver forces to rapidly commence offensive operations.

5-100. During armed conflict, forward-deployed and expeditionary Army forces enable the rapid defeat of aggression through a combination of calibrated force posture, multidomain formations, and convergence to immediately contest an enemy attack in-depth.

5-101. Corps and divisions are the formations central to the conduct of large-scale combat. These echelons synchronize available capabilities across all domains to converge effects to destroy enemy systems and formations and break the enemy's capability and will to continue a conventional conflict. As the primary

integrating echelon for converged effects, the corps integrates joint, other Services, and multinational partner support, including—

- Joint fires.
- Other Services or allies' air support.
- Airborne electromagnetic attack capabilities.
- Theater- and national-level intelligence and cyberspace operations support.
- Multinational partners' cyberspace and EW capabilities.
- Multinational partners' maneuver and fires elements.
- Special operations forces.

5-102. Refer to FM 3-0 for more information about large-scale combat operations and multidomain integration. Refer to FM 3-16 for more information about the Army in multinational operations.

RELATIVE ADVANTAGES

5-103. In conflict, Army commanders seek to create and exploit relative advantages in all domains. Relative advantages in this context include physical, human, and information advantages. Cyberspace and EW operations provide key contributions to information advantage, both by protecting friendly information and information systems and by attacking enemy command and control and information warfare capabilities.

5-104. Cyberspace and EW operations can also contribute to relative advantages in the other domains. For instance, a cyberspace or electromagnetic attack that neutralizes or degrades an enemy air defense or fire control system can create a window of advantage in the air or land domain a commander can exploit to enable maneuver.

Physical

5-105. Throughout armed conflict, leaders seek physical advantages that include—

- Position.
- Range.
- Speed of movement.
- Technologically superior capabilities.
- Terrain and weather.

5-106. The G-2 or S-2 staff identifies enemy key terrain as part of intelligence preparation of the operational environment. Identified key terrain in cyberspace is subject to actions the controlling combatant—friendly or enemy—deems advantageous such as defending, exploiting, or attacking. Key terrain in cyberspace corresponds to nodes, links, processes, or assets in cyberspace, whether part of the physical, logical, or cyber-persona layer. Key terrain in cyberspace may include—

- Locations in cyberspace in which friendly forces can gather intelligence.
- Locations in cyberspace that support network connectivity.
- Entry points to friendly networks.
- Locations in cyberspace that friendly forces rely on to provide essential functions or capabilities.

5-107. EW forces contribute to positional advantages by geolocating enemy forces to allow commanders to maneuver to a position of advantage that negates some of the benefits of the enemy's prepared defenses. Long-range EW sensors—including those provided by the joint force or other Services—can contribute to a range advantage. Counter radio-controlled improvised explosive device electromagnetic warfare systems can help protect maneuver elements while maintaining their speed of movement. Cyber and EW forces, in conjunction with intelligence forces, develop a thorough understanding of the effects of terrain on friendly and enemy forces. Thorough situational understanding may allow commanders to exploit a terrain advantage.

Information

5-108. Creating and exploiting relative advantages to achieve objectives is central to multidomain operations. Like physical and human advantages, information advantages are often temporary and change over time relative to an operational environment and how the enemy responds to friendly activities. While friendly forces seek information advantages, enemy forces are doing the same. As such, an information advantage is

something to gain, protect, and exploit across all domains. Examples of information advantages during armed conflict to which Army cyberspace and EW capabilities contribute include—

- The ability to access enemy command and control systems to disrupt, degrade, or exploit enemy information through cyberspace or electromagnetic attack.
- Opportunities created through tactical deception, including electromagnetic deception, to achieve surprise and thwart enemy targeting.
- The ability to mask electromagnetic signatures through EMCON.
- The ability to rapidly share and analyze information among commanders and staffs to enable decision making and orders dissemination.

Human

5-109. A human advantage occurs when a force holds the initiative in terms of training, morale, perception, and will. Human advantages enable friendly morale and will, degrade enemy morale and will, and influence popular support. Examples of human advantages include leader and Soldier competence, morale of troops, and the health and physical fitness of the force. The exploitation of physical and information advantages may reduce an enemy force's capacity to fight, creating human advantages. Physical and information advantages gained through cyberspace and EW operations can implicitly or explicitly communicate a message that can influence enemy forces' will to fight, sway popular support, and influence enemy risk calculus.

5-110. Examples of cyberspace and EW activities that help achieve human advantages include—

- Routine interaction with allies and other mission partners to build and maintain human, technical, and procedural interoperability through agreed-upon standards.
- Exchange of liaison officers with multinational partners.
- Sustained presence by theater-aligned advisor teams to build relationships and promote interoperability over time.

COUNTERING ENEMY ACTIVITIES IN CYBERSPACE

5-111. Enemies will undertake malicious cyberspace activities to disrupt U.S. and allies' command and control and to collect intelligence. Countering enemy malicious cyberspace activities requires coordinated cyberspace defense. G-6 or S-6 DODIN operations personnel, local network defenders, and CEMA staff across echelons will synchronize their efforts to implement the cybersecurity program, defensive cyberspace operations-internal defensive measures, and cyber incident reporting to prevent, identify, quarantine, and mitigate threat malicious cyberspace activity on the DODIN-A.

Defensive Cyberspace Operations-Internal Defensive Measures

5-112. Cyber forces act on cues from cybersecurity or intelligence alerts of enemy activity within friendly networks. Cyberspace tasks during defensive cyberspace operations-internal defensive measures include hunting for enemy activities on friendly networks and responding to mitigate their effects.

Defensive Cyberspace Operations-Response Actions

5-113. Defensive cyberspace operations-response actions are carried out outside the protected network without permission of the owner of the affected system. Some defensive cyberspace operations-response actions may include actions that rise to the level of use of force and may cause physical damage or destruction of enemy systems. These actions consist of cyberspace attacks and cyberspace exploitation as with offensive cyberspace operations. However, defensive cyberspace operations-response actions use those actions to prevent or stop enemy action.

5-114. Decisions to conduct defensive cyberspace operations-response actions depend heavily on broader strategic and operational contexts such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat, the damage the enemy has or is expected to cause, and national policy considerations. These missions are conducted by a cyber national mission team and require a properly coordinated military order; coordination with interagency partners; and unified scope, rules of engagement, and operational objectives.

DEFEATING ENEMY ANTIACCESS AND AREA DENIAL

5-115. Defeating layered antiaccess and area denial relies on targeting efforts undertaken as part of setting the theater during competition and crisis. Developing targets in cyberspace well in advance of conflict allows the necessary lead time to develop tailored capabilities to engage the targets at the beginning of conflict. The theater army and multi-domain effects battalion's targeting conducted during competition and crisis supports delivery of converged effects to overcome enemy antiaccess and area denial and supports joint forcible entry at the onset of armed conflict. The multi-domain task force can coordinate and integrate cyberspace, EW, and space capabilities with long-range surface fires to deceive, neutralize, or disrupt enemy formations, command and control nodes, layered air defenses, and cyberspace and EW activities. This allows Army and joint forces to penetrate and disintegrate enemy antiaccess and area denial capabilities, enable command and control, and exploit the resulting freedom of maneuver. *Disintegrate* means to disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations (ADP 3-0).

JOINT FORCIBLE ENTRY

5-116. Neutralizing enemy long-range systems enables theater strategic- and operational-level operations by reducing the vulnerability of friendly lines of communications. Simultaneously, forward-deployed forces begin to defeat enemy stand-off from the inside by operating within the range of enemy long- and mid-range systems in conjunction with the joint force and other Services. Cyberspace attacks conducted by national-level assets can partially neutralize some enemy standoff capabilities, including long-range precision fires and integrated air defenses, long enough for joint and Army forces to destroy the systems. Electromagnetic attack against enemy air defense radars also contributes to suppression of enemy air defenses to defeat enemy antiaccess and area denial. Electromagnetic jamming or spoofing of enemy positioning, navigation, and timing satellite signals can render guidance systems of enemy long-range precision fires ineffective.

5-117. National- and theater strategic-level cyberspace attacks are critical to support joint forcible entry operations. National-level assets will engage cyberspace targets developed during competition and crisis to defeat enemy long-range precision fires and integrated air defenses to allow combat forces to enter and establish a foothold in the theater and commence offensive operations. Joint forcible entry operations can extend from the close area into the deep area, based on the enemy's antiaccess and area denial capabilities.

5-118. Success in joint forcible entry entails neutralizing enemy air defenses in the close area and long-range precision fires and strategic command and control in the deep area. Cyberspace and electromagnetic attack capabilities from the national and theater strategic levels are key contributors to joint forcible entry operations. Electromagnetic attack capabilities employed at echelons corps and below may support suppression of enemy air defenses in the close area. The corps may need to integrate airborne deep sensing capabilities provided by other Services. Refer to ATP 3-04.1 for more information about suppression of enemy air defenses.

CYBERSPACE AND ELECTROMAGNETIC WARFARE OPERATIONS IN THE DEFENSE

5-119. In the defense, commanders typically retain the deep and rear areas, but they divide the close area into two distinct portions: the security area and main battle area. Commanders use this approach to synchronize operations, including those in air, space, and cyberspace to defeat an enemy force throughout its depth.

5-120. During large-scale combat operations, the enemy will employ extensive malicious cyberspace activity and electromagnetic attacks to disrupt U.S. communications; automated information systems; fire control; and positioning, navigation, and timing. Local network defenders continue to protect their respective portions of the network against malicious cyberspace activity. Units implement electromagnetic protection plans—including EMCON—to protect spectrum-dependent devices from detection, geolocation, jamming, and lethal fires.

Deep Operations in the Defense

5-121. The corps staff conducts planning to counter enemy long-range fires and shape conditions in the deep area for future division and brigade combat team operations. The corps' planning horizon for deep operations in large-scale combat operations is 48 hours–5 days. This gives the corps ample time to integrate required capabilities from the joint force, other Services, or multinational partners to support shaping activities.

Extended Deep Operations

5-122. The combatant command plans and conducts operations to shape conditions in the extended deep area, including lines of communication from the enemy's strategic base to the joint operational area. Shaping in the extended deep area may use support from national-level assets (including offensive cyberspace operations capabilities) to create desired effects. Planning for extended deep operations requires a longer planning horizon than deep or close operations due to the need to coordinate for joint or national capabilities.

Deep Operations

5-123. The division conducts operations in its deep area to neutralize enemy long range fires, disrupt enemy command and control and sustainment, and shape conditions for future operations as close operations move forward in the assigned area. The division's planning horizon for deep operations is at least 24–48 hours to allow coordination and integration of supporting capabilities from the joint force and other Services. Other Service EW capabilities in the air tasking order extend the planning horizon for deliberate targeting. Planners must consider the longer lead time when planning shaping operations in the deep area. Immediate EW targets in the deep area that arise outside the planning horizon of the joint air tasking cycle can be engaged by re-tasking air assets.

Close Operations

5-124. Divisions employ maneuver brigades in close operations against enemy maneuver forces. Divisions employ attack aviation and close air support to enable close operations and conduct rear operations to sustain tempo and operational reach.

Main Battle Area

5-125. Brigade combat team EW platoons conduct electromagnetic support in the close area for combat information to support targeting and electromagnetic attack to jam enemy communications and fire direction control. The division EW company augments brigade EW capabilities in the close area. The brigade planning horizon for close operations is much shorter term than the division and corps planning horizons; brigade combat teams generally plan operations 12–24 hours out.

Security Area

5-126. A *security area* is that area occupied by a unit's security elements and includes the areas of influence of those security elements (ADP 3-90). The security area is inside, or close to, an operational area where forces and sustainment from two or more Services are positioned to conduct or support operations. Enemies are invested in diminishing friendly security areas. Electromagnetic protection measures minimize the effects of natural phenomena and mitigate the enemy's ability to conduct electromagnetic sensing and attack against friendly forces in the security area.

Rear Operations

5-127. The objective of rear operations is to ensure freedom of maneuver and continuity of operations through sustainment. Enemies often target the rear area because it is vulnerable and critical to sustained operations. Electromagnetic protection helps defend against lethal attacks by denying enemy use of the electromagnetic spectrum to target, guide, and trigger weapons. Electromagnetic support supports situational understanding and enables force protection, self-protection, and operations security efforts by countering an enemy's surveillance and reconnaissance capabilities.

Cyberspace and Electromagnetic Warfare Operations in the Offense

5-128. Maneuver commanders may engage approved cyberspace targets with available military capabilities to support movement and maneuver by opening avenues necessary to disperse and displace enemy forces. Converging effects in cyberspace with effects in other domains establishes conditions that enable maneuver forces to gain or exploit positions of relative advantage. Electromagnetic attack—including electromagnetic jamming, electromagnetic intrusion, and electromagnetic probing—supports movement and maneuver by

projecting power within the time and tempo of the scheme of maneuver. Electromagnetic support provides combat information to support situational understanding, targeting, and assessment.

5-129. Cyberspace and EW in the offense might involve the following actions, some of which span different domains and functional areas (for example intelligence or operations security):

- Countering enemy unmanned aircraft systems.
- Protecting friendly unmanned aircraft systems.
- Gaining access to enemy closed networks in or near a unit's assigned area, including extracting and injecting data.
- Using EW systems as delivery platforms for precision cyberspace effects.
- Exploiting new devices and applications developed and deployed by the enemy that are being tested for battle.
- Delivering messages to relevant audiences.
- Preventing the spread of misinformation and disinformation.

OPERATIONAL FRAMEWORK CONSIDERATIONS IN THE OFFENSE

5-130. Within the context of the higher echelon commander's operational framework and the general phasing scheme, commanders must design attacks that defeat enemy forces across all echelons, while enabling disciplined initiative of subordinate leaders. When designing attacks, commanders divide the task of defeating an enemy force and maintain an integrated approach through deep, close, and rear operations. Commanders account for air, space, cyberspace, and when relevant, maritime capabilities across the operational framework. They also consider friendly, enemy, and neutral use of the electromagnetic spectrum in their assigned areas.

Deep Operations

5-131. Echelons division and above conduct deep operations to establish conditions for subordinates' success in close operations. In general, the combatant command conducts extended deep operations to set conditions for the corps and below; the corps and division conduct deep operations to set conditions for brigade combat teams conducting close operations.

Extended Deep Operations

5-132. Signal recognition, detection, identification, and geolocation are critical requirements in the extended deep area to enable commanders to discover, exploit, and attack. The combatant command plans and conducts offensive operations in the extended deep area to set conditions for future events in time and space. Higher echelon headquarters—the theater army, combatant command, and national assets—are responsible for the extended deep area. Operational missions seek to disrupt the movement of the enemy's operational reserves, prevent enemy forces from employing long-range fires and integrated air defense systems, and interfere with enemy space and cyberspace capabilities to improve the protection of tactical formations. Special operations forces can conduct electromagnetic attacks to deny the enemy electromagnetic spectrum access, attack targets, and ensure maneuverability. Army forces request joint effects in the extended deep area by submitting CERFs and electromagnetic attack request formats through the chain of command to the combatant command. See appendix C for more information about the CERF and electromagnetic attack request format.

Deep Operations

5-133. In tactical-level deep operations, the corps headquarters might direct fires into its deep area to defeat enemy long-range fires, disrupt enemy sustainment and command and control, separate maneuver formations, and enable effective offensive maneuver. Deep operations are inherently joint, since many of the capabilities employed in support of Army formations are provided by a joint force headquarters or another Service, including the long-range airborne EW and air-to-surface fires platforms operated by the Navy and Air Force.

Close Operations

5-134. EW teams at the brigade and division geolocate enemy emitters in the main battle area and security area for targeting with lethal or nonlethal capabilities or maneuver. They can also jam enemy command and control communications to open temporary windows of advantage for maneuver forces. Counter radio-controlled improvised explosive device electromagnetic warfare systems help protect combat and sustainment forces from improvised explosive devices when maneuvering in the main battle area. Because they typically perform a scout role well forward of the main body, EW teams may be positioned to directly observe enemy activities and report combat information to address the commander's critical information requirements in the main battle area.

Rear Operations

5-135. Enemy deep operations often target friendly rear operations because they are often both vulnerable and essential to friendly mission success. Units conducting rear operations must protect themselves using both passive and active measures. Cyberspace defense and electromagnetic protection help protect friendly communications to support sustainment operations and command and control in the rear area.

5-136. Maneuver forces will need to defeat bypassed forces in the rear area to consolidate gains. EW teams in the rear area, synchronized with SIGINT forces, can conduct direction finding to geolocate enemy forces in the rear area for engagement by lethal or nonlethal attack or maneuver forces.

Transition to Stability Operations

5-137. As a transition to stability operations occurs, leaders focus on stability tasks and information activities to inform and influence populations and conduct security force assistance. Effective collaboration with diplomatic and humanitarian organizations enhances the ability to achieve stability mechanisms. Army forces play a key role in enabling the joint force to establish and conduct military governance until a civilian authority or government is given control of their assigned areas.

5-138. During transition from defensive to stability operations, Army cyber forces may assist host nations and multinational partners in reconstituting and hardening critical networks and infrastructure. Commanders anticipate and incorporate mission partner planning factors, such as their domestic laws, regulations, and operational limitations on the use of various cyberspace defense and cyberspace security actions such as password management, software patching, encryption and storage device management, mandatory cyberspace training for all users, and restricting access to suspicious websites. Army EW forces may help the host nation reestablish spectrum-dependent capabilities and generally provide electromagnetic protection during transition.

Return to Post-Conflict Competition

5-139. Through a successful transition from armed conflict to the return to competition, integrated EW, SIGINT, and cyberspace operations planning and assessment translate operational success to the achievement of strategic objectives. During consolidation of gains, friendly EW forces reconstitute and help build or reinforce the spectrum capacity of host-nation partners to enable long-term deterrence and prevent return to armed conflict. Cyber forces may help partner nations improve the security and defense of their military and civilian network infrastructure until they are adequately prepared to conduct their own network defenses.

Theater Army Role

5-140. Theater armies play a significant role in the return to post-conflict competition. The theater army's continuous, long-term focus on theater strategy, relevant national interests, and established relationship with host-nation civil and military authorities enables them to holistically plan and conduct the transition. The theater army CEMA section anticipates requirements and requests additional cyber and EW forces and capabilities needed to support the transition to post-conflict competition.

5-141. Theater requirements will change as combat operations reduce and the focus on stability tasks increases. As the transition progresses, the theater army helps ensure the host nation is prepared to defend itself and continue civil governance post-conflict. This may require assistance securing and defending civilian network and communications infrastructure.

Corps Role

5-142. As large-scale combat operations conclude in a corps' assigned area, the corps continues to adjust its operational framework to meet the increasing demand on stability tasks while maintaining a posture that prevents enemies from reconstituting their forces and operations. Operations primarily focus on area security in high threat areas, followed by the performance of stability tasks in lower threat areas. During transition, the corps will likely conduct simultaneous offense, defense, and stability operations.

5-143. During the transition, enemy information warfare elements or their proxies may continue to conduct malicious cyberspace activity against U.S., allied, and host-nation networks and civil infrastructure. Local network defenders continue to defend the corps' portion of the network and assist multinational partners in securing and defending their networks, if required and authorized.

Division Role

5-144. Divisions perform the stability tasks necessary to create conditions within their assigned areas that allow transition to a legitimate civilian authority or a transitional authority. Divisions also control brigades as they conduct security force assistance to build the capability and capacity of foreign security forces.

5-145. Local network defenders continue to defend the division's portion of the network against enemy malicious cyberspace activity. The division CEMA section and EW forces work to understand enemy activities in the electromagnetic spectrum, since increased activity in the electromagnetic spectrum may be an early indication of the enemy's intent to re-commence combat operations.

Brigade Combat Team Role

5-146. Task-organized brigade combat teams perform most area security tasks, and they enable the accomplishment of most stability tasks in concert with multinational partners. Army forces' actions upon culmination of large-scale combat operations include—

- Consolidation.
- Establishing area security.
- Conducting stability tasks.

5-147. Local network defenders continue to defend the brigade's portion of the network. The brigade CEMA section and EW platoon maintain situational awareness of enemy activities in the electromagnetic spectrum to provide early warning of enemy attempts to re-commence combat operations.

This page intentionally left blank.

Appendix A

Cyber Incident Response

Cyber incident response refers to the processes and technologies for detecting and responding to malicious cyberspace activity or security breaches. The goal of incident response is to minimize the cost and mission disruption resulting from threat malicious cyberspace activity. This appendix explains how different types of malicious cyberspace activity should be identified, analyzed, reported, contained, and resolved.

SECTION I – DEPARTMENT OF DEFENSE CYBER INCIDENT HANDLING PROGRAM

A-1. Effective cybersecurity requires the ability to respond to malicious cyberspace activity. The DOD maintains a comprehensive cyber incident handling program to rapidly identify and respond to cyber incidents. The DOD cyber incident handling program is a component of the overall DOD approach to cyberspace defense.

OVERVIEW

A-2. In a dynamic threat environment, it is critical that those responsible for building, operating, defending, maintaining, and ensuring the continuity of information networks maintain unified and resilient network capabilities. These capabilities must be able to adapt over time to changes in the threat environment. Refer to DODI 8530.03 for more information about DOD cyber incident response. The cyber incident handling program aligns with the defensive cyberspace operations services of—

- Protect.
- Monitor.
- Respond.

A-3. The DOD cyber incident handling program is comprised of activities across many federal agencies which include—

- Reporting and notification.
- Incident analysis.
- Containment.
- Eradication and recovery through coordinated incident response actions.

A-4. Coordinated cyber incident response ensures the acquisition and preservation of data required for tactical analysis, strategic analysis, or further investigation.

ACTIVITIES

A-5. The cyber incident handling program establishes the requirements for detecting, analyzing, and responding to cyberspace events and incidents. It establishes standardized processes that ensure timely and effective response. It enables timely and accurate reporting on the causes, impacts, and current state of incidents.

A-6. How organizations implement the cyber incident handling program may vary depending on resources, technical capabilities, and local policies and procedures. The objectives of the cyber incident handling program are to—

- Minimize the scope and duration of impacts from incidents.
- Understand malicious actions taken on the network and the associated risks.
- Improve the overall defensive posture of the network based on lessons learned.

CYBER INCIDENT REPORTING

A-7. Cyber incident reporting provides an accurate, meaningful, and comprehensive understanding of the cyber incident from initial detection to analysis and remediation. This information feeds into the user-defined operational picture, which provides tactical, operational, and strategic situational understanding of cyberspace defense actions and their impact. See section IV for ARCYBER reporting models.

A-8. Army cyber incident reporting and handling is subject to the requirements of CJCSM 6510.01B, CJCSI 6510.01F, and DODI 8530.01. Prompt, accurate reporting provides awareness and insight into past and ongoing cyber incidents.

CYBER INCIDENT ANALYSIS

A-9. Cyber incident analysis identifies critical elements of an incident to determine and characterize its possible effects on DOD networks, information, operational missions, and other defense programs. This activity follows the cycle of—

- Preparation.
- Detection and analysis.
- Containment, eradication, and recovery.
- Post-incident recovery.

A-10. Figure A-1 illustrates the cyber incident analysis process. Refer to DODI 8530.03 for more information about cyber incident analysis.

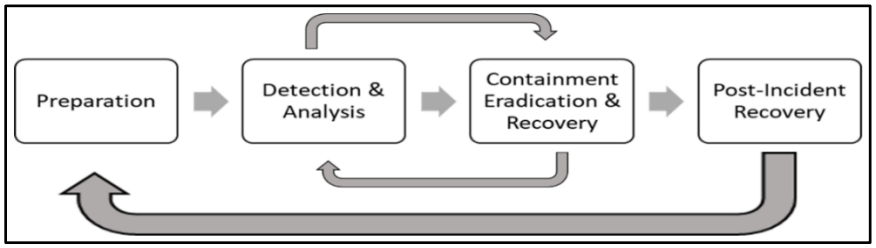


Figure A-1. Cyber incident analysis

SECTION II – RESPONSE

GENERAL

A-11. The cyber incident response life cycle (figure A-2) provides an organized and coordinated series of response actions to resolve or mitigate a reported incident. It also includes the steps taken to recover affected systems and return them to a fully operational and secure state. Coordination, communication, and documentation actions are also taken during incident response to ensure the right organizations are involved, notified of the outcomes, and provided follow-up reports. Once the incident is resolved, a final report is submitted, and the unit completes any remaining post-incident actions. The primary objectives for an incident response are to—

- Halt or minimize attack effects or damage while maintaining the operational mission.
- Ensure effective and timely recovery of system in a way that prevents similar incidents.
- Strengthen the defensive posture and operational readiness of network systems.
- Protect data throughout the incident response according to its sensitivity.
- Rapidly and completely characterize the attack.

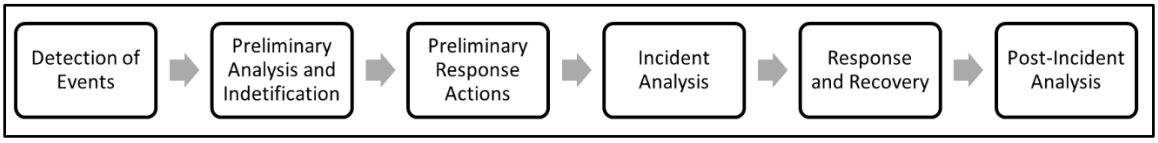


Figure A-2. Cyber incident response life cycle

DETECTION OF EVENTS

A-12. Detection of cyber events is a continuous process of identifying any unusual network or information system activity that can adversely affect DOD networks, systems, or operational missions. The primary objectives of detecting cyber events include—

- Detection and reporting of suspicious activity so that further analysis can take place to determine whether it is a reportable cyber event or incident.
- Reporting of suspicious activity within required reporting timelines.
- Coordination with higher echelons and other DOD organizations.

A-13. As part of this process, local defenders gather and report information about possible malicious cyberspace activities, identified vulnerabilities, or other security or incident information to the appropriate authorities for analysis and response. This is important because it is the point where an anomalous or unusual cyber event is first noticed and identified as something that must be reviewed. It may also be the first point at which a cyber event is reported.

A-14. Detection starts the reporting process. Gathering report information in a database helps analysts identify emerging trends and patterns. This knowledge can help service desks learn from ongoing activity and incidents so they can properly secure and defend their portions of the network.

A-15. For proper detection to take place, guidelines must be established defining what to consider abnormal or suspicious. This information should be passed to appropriate network and information system administrators or incorporated into the configuration of automated detection systems. Without the detection process, the Army Enterprise Service Desk would not be alerted that something must be checked or resolved. If this does not happen in a timely, standard, consistent manner, a serious incident may not be properly reported and significant damage and loss to the component infrastructure can occur. Detection of a cyber event may occur in various ways, including—

- An automated detection system or sensor.
- A report from an individual or user.
- An incident report or situational awareness update from other internal or external organizational components, such as USCYBERCOM, or other external computer security incident response team entities.

A-16. Cyber incident detection can be from any stakeholder, and initial event details can vary. Alerts from automated detection systems might include more details than a report from a non-technical user. Additional information may need to be collected as part of the incident analysis phase. Examples of cyber events and the various ways they are detected include—

- The network intrusion detection system sends alerts for suspicious network traffic.
- The antivirus software alerts that a device is infected with a worm, virus, or other malicious code.
- A web server crashes.
- Users complain of slow access to hosts on the Internet or mail servers.
- The system administrator sees a filename with unusual characters.
- A user calls the service desk to report a suspicious e-mail message (possible phishing attempt).
- An information system records a suspicious configuration change in its log.
- An information system logs multiple failed login attempts from an unfamiliar remote system.
- An e-mail administrator sees many e-mails with suspicious content.
- A network administrator notices deviation from typical network traffic flows.
- A firewall administrator sees unauthorized outbound connections not seen by other means.

A-17. An event is not determined to be an incident until after preliminary analysis to assess and validate the event against the criteria for determining whether it is an incident. Network defenders should categorize reportable cyber events and incidents and follow the established cyber incident handling process in accordance with CJCSM 6510.01B.

PRELIMINARY ANALYSIS AND IDENTIFICATION

A-18. Initial assessments should be conducted quickly, even with limited details and analysis. As the investigation continues and analysts more accurately characterize the true impact, the report is reassessed and modified.

A-19. To make an accurate impact assessment, the analyst performing the preliminary assessment must have access to personnel with a good understanding of the function and criticality of the information system, network, or data in question and its role in fulfilling the mission.

A-20. Local network defenders begin to document the incident if documentation has not already begun. If analysis determines that computer forensics are required (for instance, a Criminal Investigation Division investigation), defenders begin to document the chain of custody. Documentation should include—

- All known information about the event or incident.
- All actions taken during the preliminary analysis and the results of that analysis.
- A chain of custody record initiation if forensic evidence is collected and further prosecutorial investigation may be required.

INITIAL REPORT SUBMISSION

A-21. Local network defenders prepare and submit the initial report to the appropriate organizations and commands and through the established reporting mechanisms. Whenever possible, cyber incident reporting should take place outside the affected network. Local network defenders should not report through a potentially compromised network because an attacker may be monitoring the compromised network and could be warned of detection. There are two different types of reporting—technical and operational.

Technical Reporting

A-22. Technical reporting assists with the handling of incidents and enables mitigation of the operational and technical impact of an incident. Technical reporting may include submitting an incident report to the regional cyber center or Army Enterprise Service Desk.

Operational Reporting

A-23. Operational reporting provides notification to commanders at all levels about the status of their networks and information systems and the operational impact of the incident on their missions. Operational reporting is a vital conduit for commanders to identify operational impacts and direct the incident handling process to mitigate negative impact on their missions. Responding to an incident may require immediate action by all affected units.

PRELIMINARY RESPONSE ACTIONS

A-24. Organizations use a combination of cyber incident actions. The types of cyber incident actions are—

- Technical actions.
- Command actions.
- Legal and policy actions.

TECHNICAL ACTIONS

A-25. Technical actions contain or eradicate risks or vulnerabilities associated with the incident and rebuild or restore affected systems to their normal operational state. These actions focus on minimizing incident effects, facilitating incident analysis, and restoring operational capabilities. The personnel required to execute technical actions depend on the organization responsible for the affected system and mission components.

COMMAND ACTIONS

A-26. Command actions direct other incident response actions and direct changes to current operations. They ensure appropriate resources are dedicated to cyber response and ensure changes to operations are coordinated, nested, and effective. They require some type of command or leader intervention, notification,

interaction, escalation, or approval as part of any response. Often, directed response actions are based on technical analysis with short reaction, compliance, and reporting timelines.

LEGAL AND POLICY ACTIONS

A-27. Legal and policy actions are associated with—

- Legal liability.
- Privacy issues.
- Creating or reviewing nondisclosure and service level agreements.
- Other legal and policy actions taken in response to an incident.

A-28. Units prepare to facilitate legal and policy actions through the testing of networks, information systems, and mission systems. Units archive boot disks and distribution media for all applications, security patches, and operating systems. This is especially important for deployed units who may lose network capabilities due to malicious cyberspace activity. Depending on the type of data compromised, commands may have additional responsibilities (for example, conducting a personnel asset inventory).

RESPONSE AND RECOVERY

A-29. USCYBERCOM has the authority to direct and assist commands with mitigation actions for incidents that fall into a DOD enterprise incident set or when actions otherwise affect multiple theater or Service information networks. For further information about developing incident response courses of action and approaches, refer to NIST SP 800-61. Incident response courses of action include the actions necessary to—

- Respond to the reportable cyber event or incident.
- Restore the information or mission system.
- Return the system to operation.
- Assess residual risk for the system or network.

DEVELOPMENT

A-30. Analysis, comparison, and selection of courses of action should take place at the lowest echelon practicable. Proposed courses of action should include the development and issuance of notifications to promote awareness, direct response actions, and ensure compliance. Those with key roles in responding to an intrusion must be notified and kept informed to fulfill their responsibilities.

IMPLEMENTATION

A-31. Implementation of the selected course of action and information dissemination procedures may include contacting users, security personnel, vendors, Internet service providers, other commands, and other internal or external security organizations. Coordination may be required with DOD agencies or with external law enforcement organizations when DOD support is not available due to time or distance factors. International coordination may be needed if attacking hosts reside in a foreign nation.

CONTAINMENT

A-32. Containment consists of short-term actions to stop an attacker's access to a compromised information system, limit the extent of an intrusion, and prevent an intruder from causing further damage. While an intruder has access to the system, the information system cannot be properly analyzed or restored. Containment prevents an intruder from accessing or exfiltrating data or other information, destroying evidence, or tampering with the system during analysis. Containment provides a reasonable security solution until enough information has been collected to address the vulnerabilities exploited and the damage sustained. Containment actions are performed by the unit responsible for operating and maintaining the affected network or system.

ERADICATION

A-33. During eradication, incident response focuses on eliminating the attacker's presence and access. All exploits and vulnerabilities should be removed from networks and systems before returning the system to service. If the exploit is not removed, the system can be easily compromised or breached again. Eradication measures remove the cause of the malicious activity and any associated files. Eradication ensures the

elimination of any access methods used by the intruder, including vulnerabilities, weaknesses in physical security, or human error.

A-34. Eradication is system-specific. In some cases, full eradication requires long-term policy or configuration changes. In that case, the exploit should be mitigated to the extent possible before rebuilding and reconnecting affected systems. Due to the nature of an incident, some systems may not need any eradication steps, or the eradication may occur as part of recovery when the infected system is wiped and reimaged.

A-35. The unit responsible for operating and maintaining the affected information network or system performs eradication. Who performs the measures depends on the type of incident, affected component, and local policy and procedures. Eradication techniques depend on the nature of the incident. Eradication techniques include—

- Removal of malware.
- Remediation or mitigation of vulnerabilities.
- Modification of access controls.

Removal of Malware

A-36. To remove malware, network or system administrators should quarantine, delete, replace, or restore the integrity of infected files. This may require reimaging the system from trusted media. It may also involve updating antivirus signatures.

Remediation or Mitigation of Vulnerabilities

A-37. Units can mitigate vulnerabilities through technical and non-technical means. Network or system administrators can remove vulnerabilities by installing up-to-date patches to vulnerable operating systems or applications to prevent exploitation. If the system cannot be patched for technical or operational reasons, the vulnerability may be mitigated by updating the system configuration and defenses to protect or segment the affected host. If a patch is not available, system or network administrators apply workarounds or temporary mitigation measures. Units may also use policies, physical security measures, and other mechanisms to augment technical controls.

Modification of Access Controls

A-38. Network administrators may need to update user and network access controls. Examples include—

- Removing compromised user or administrator accounts.
- Updating intrusion detection systems or intrusion protection systems.
- Modifying firewall settings.
- Filtering content.
- Updating baseline configurations.
- Removing other access mechanisms used by the threat.

RECOVERY

A-39. Recovery restores the integrity of the affected system and implements protective measures to prevent similar incidents from occurring in the future. The goal of recovery is to return to normal, steady-state operations. During recovery, administrators restore the integrity of affected systems, return the affected data, systems, and information networks to an operational state, and implement follow-up measures to prevent reoccurrence of the incident. As part of recovery, network and system administrators confirm that the systems operate normally and that the follow-up measures are effective.

A-40. Data and systems are fully restored when the necessary patches and fixes have been installed. The integrity of all data and software on an affected information system is suspect. The intruder could have changed the kernel, binaries, data files, running processes, or memory. The only way to be sure a system is free of malicious code and back doors is to reinstall software from trusted media and install up to date security patches and upgrades. This includes both operating system and application patches.

A-41. As part of the recovery process, containment activities completed may need to be removed. This can include removing blocks that are no longer necessary, re-enabling services, and reconnecting information systems and networks.

A-42. Recovery measures are implemented by a variety of defensive cyberspace operations. cybersecurity personnel, or network and system administrators based on their cyberspace workforce roles. Multiple measures may need to be implemented across affected components. Who implements the measures depends on the type of incident, affected component, and local policy. Depending on the nature of the incident, recovery actions may include—

- Reimaging the system from trusted media—reinstalling the operating system and application software from a trusted backup or from the original distribution media.
- Verifying system data—reviewing data on the affected system to ensure its integrity. Someone who knows what user or other data was on the information system should review the data to ensure it has not been changed. Alternatively, system administrators can restore data from a trusted backup.
- Changing system passwords—changing all passwords (including administrator passwords) on the information system and possibly on all information systems that have trust relationships with the affected system.
- Improving network and host security.

Recovering Without Performing Technical Analysis

A-43. Data from all incidents must be preserved to enable technical analysis. However, under certain circumstances, and with approval, technical analysis may not be required prior to information and mission system recovery. For example, it may not be possible to conclusively identify the root cause of an incident through additional analysis. The intruder may have deleted or tampered with logs and files, making them untrustworthy. The existence of multiple unpatched vulnerabilities may make it impossible—or not worth the effort—to try to identify which vulnerability was exploited. In such cases, it may be more expedient to begin system recovery and hardening.

A-44. Administrators should carefully assess technical and operational implications before recovering an information system without technical analysis. Technical analysis provides valuable information to prevent the same or similar attacks in the future. Such an assessment will indicate how this may impact mission success. For example, the primary benefit of determining root cause and eradicating it before redeploying an information or mission system is to prevent similar system compromises and to share that information with other network defenders, thereby strengthening the overall security of the network. If a root cause is not identified and eradicated, the system may be compromised again, or the same exploit may be used on other systems.

POST INCIDENT ANALYSIS

A-45. An after action review of the incident, including detection, analysis, and action, will improve operations, processes, and network defense. The primary objectives of an after action review include identifying infrastructure problems to be addressed, system and configuration weaknesses, and organizational policy and procedural problems to be reviewed and modified. After action reviews are an opportunity to determine unclear or undefined roles, responsibilities, interfaces, and authorities while identifying technical or operational needs.

A-46. Upon completion of the after action review, administrators provide feedback to suggest improvements to policies, procedures, and infrastructure defenses to NETCOM through the regional cyber center. These improvements may include updating security policies or implementation guides (for example, SOPs or security technical implementation guides), and incident handling processes and procedures. During this time, modifications are made to configurations and filters on network perimeter devices, such as firewalls, routers, and gateways.

A-47. After action reviews produce information and incident data that can be collected and used in various ways. This information can be used to establish baselines for benchmarking performance, timeliness, and types of incidents seen. It can also be used to generate trending and correlation information for historical purposes to determine whether response actions are resolving problems over time.

SECTION III – EVENT AND INCIDENT SCHEMA AND CLASSIFICATION

EVENTS AND INCIDENTS

A-48. An *event* is any observable occurrence in a network or system (NIST SP 800-61). Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with negative consequences, such as—

- System crashes.
- Denial-of-service attacks.
- Unauthorized use of system privileges.
- Unauthorized access to sensitive data.
- Execution of malware that destroys data.

A-49. An *incident* is an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (Title 44, United States Code). Examples of cyber incidents include—

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash (distributed denial-of-service).
- Users are tricked into opening a malicious file sent via e-mail (phishing). Running the malicious software may infect their computers and establish connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money (cyber extortion).
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

CYBER INCIDENT AND REPORTABLE CYBER EVENT CATEGORIES

A-50. A cyber incident or reportable cyber event category is a collection of events or incidents sharing a common underlying cause of which an incident or event is reported. Each cyber incident or event is associated with one or more categories as part of the incident handling process. Table A-1 on page 105 outlines the categories of cyber incidents. Refer to CJCSM 6510.01B for more information about categorizing incidents and reportable events.

Table A-1. Cyber incident categories

Category	*Description*
0	**Training and exercises**. Operations performed for training purposes or support to a combatant command, Service, agency, or field activity.
1	**Root level intrusion (incident)**. Unauthorized privileged access to an information system. Privileged access, often referred to as administrator or root access, provides unrestricted access to the system. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions. If the information or mission system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
2	**User level intrusion (incident)**. Unauthorized non-privileged access to a system. Non-privileged access, often referred to as user-level access, provides restricted access to the system based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to perform user functions such as accessing web applications, web portals, or other similar information resources. If the system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
3	**Unsuccessful activity attempt (event)**. Deliberate attempts to gain unauthorized access to an information system that are defeated by normal defensive mechanisms. An attacker fails to gain access to the system (attacker attempts valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical to gather useful effects-based metrics. ***Note.*** This does not apply to a virus that is defeated and deleted by antivirus software. Viruses that are defeated and deleted by antivirus software are not reportable events or incidents and should not be annotated.
4	**Denial-of-service (incident)**. Activity that denies, degrades, or disrupts normal functionality of an information system or network.
5	**Non-compliance activity (event)**. Activity that may expose systems or security domains, install vulnerable applications, or breach cybersecurity policy. Reporting of these events is critical for the gathering of useful effects-based metrics.
6	**Reconnaissance (event)**. Activity that seeks to gather information used to characterize system applications, networks, or users that may be useful in formulating an attack. This includes activity such as mapping networks, system devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
7	**Malicious logic (incident)**. Installation of software designed or deployed by adversaries with malicious intent for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised system. Malicious code that allows interactive access should be categorized as category 1 or category 2 incidents, not category 7. Interactive access may include automated tools that establish an open channel of communications to a system.
8	**Investigating (event)**. Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as category 8. Category 8 events are re-categorized to category 1–7 or 9 prior to closure.
9	**Explained anomaly (event)**. Suspicious events that, after further investigation, are determined to be non-malicious activity and do not fit the criteria for any other categories. The reason the anomaly cannot be otherwise categorized must be clearly specified.

INITIAL IMPACT ASSESSMENT

A-51. The initial impact assessment table (table A-2 on page 106) describes the severity of a cyber event or incident and establishes a common framework for evaluating and assessing events or incidents. This ensures all units share a common view of the severity of a given event or incident. It should only be used during initial reporting. A more complete impact assessment is conducted later in the cyber incident handling process as more details are available and analysis conducted.

Table A-2. Initial impact assessment table

Type of Impact	*Impact Level Description*		
Operational	High: Loss of ability to perform mission.	Moderate: Significant degradation of mission.	Low: Fully mission capable with reduced efficiency.
Information	High: Compromise of classified information.	Moderate: Compromise of protected information (personally identifiable information or protected health information).	Low: Compromise of non-publicly releasable information.
Recoverability	Extended: Time unpredictable and may require external assistance.	Supplemented: Predictable time with additional resources.	Normal: Predictable time with existing resources.

A-52. The initial assessment must be performed quickly, even with limited details and analysis. As the investigation continues and the true impact is understood, the report is reassessed and modified.

MAJOR CYBER INCIDENTS

A-53. A major cyber incident may be interchangeably termed a 'significant cyber incident.' A major incident is either—

- An incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
- A breach that involves personally identifiable information that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

A-54. Cybersecurity personnel and local network defenders assess each breach on a case-by-case basis to determine whether it meets the definition of a major cyber incident. Refer to Office of Management and Budget Memorandum M-23-03, Fiscal Year 2023, for more information about categorization of major cyber incidents.

CYBER INCIDENT RESPONSE SEVERITY SCHEMA AND NATIONAL RESPONSE COORDINATION CENTER ACTIVATION CROSSWALK

A-55. In case of cyber incidents, certain decisions and activities require coordination to respond in the most appropriate manner. Table A-3 on page 107 compares the cyber incident severity schema with the Department of Homeland Security National Response Coordination Center activation scale when comparing response levels for cyberspace and physical incidents.

Table A-3. Cyber incident severity schema crosswalk

Description	*Disaster Level*	*Cyber Incident Response*	*Description*	*Observed Actions*
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of U.S. citizens.	Effect
Requires elevated coordination among federal, state, local, tribal, and territorial governments due to moderate levels and breadth of damage. Significant involvement of the Federal Emergency Management Agency or other federal agencies.	Level 2	Level 4 Severe	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 High	Likely to result in a demonstrable impact on public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal, state, local, tribal, and territorial governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 Medium	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 Low	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

SECTION IV – CYBER INCIDENT RESPONSE REPORTING

A-56. When a cyber incident is suspected, users must stop all activities on the affected system and notify local network defenders (information systems security officers or information systems security managers) immediately. Local defenders contact the supporting regional cyber center and NETCOM strategic signal brigade. Supporting strategic signal brigades notify the signal command (theater). The initial notification must be conducted through secure, preferably out-of-band, communication channels. For example, via encrypted e-mail for initial communication on unclassified networks. Response reporting should take place when the unit is not in direct or indirect fire contact with the enemy. Units should not delay offensive or defensive actions in the physical domains for the sake of reporting compliance. In this case, the unit submits cyber incident reports as soon as practicable after breaking enemy contact.

Note. In theaters without a signal command (theater), the strategic signal brigade is the highest level NETCOM unit.

A-57. Local network defenders in the G-6 or S-6 who observe, suspect, or are notified of a possible cyber incident should prohibit unnecessary activity on the affected system and immediately notify the servicing regional cyber center. The regional cyber center notifies the Department of the Army Criminal Investigation Division and counterintelligence elements as necessary. Local network defenders do not further investigate the incident or isolate the system until directed by the regional cyber center. Additional actions may be necessary following coordination with ARCYBER, Criminal Investigation Division, or counterintelligence elements, as any action could compromise the investigation and integrity of forensic data.

A-58. Users who cannot make immediate contact with local network defenders in their G-6 or S-6 for incident handling contact their servicing network enterprise center service desk to initiate incident reporting until local network defenders are engaged. If the service desk is not available, users should report to either the Army Enterprise Service Desk or the regional cyber center.

BRIGADE COMBAT TEAM

A-59. The brigade S-6 and the brigade signal company perform incident and problem management for the brigade and subordinate battalions and companies. When DODIN operations personnel identify an incident at the brigade combat team, they analyze the incident to determine whether it can be resolved locally. At echelons brigade and below, the local ability to analyze incidents is very limited. If personnel cannot identify a local solution, they escalate the incident to the next higher headquarters.

CORPS AND DIVISION

A-60. The corps or division G-6 and the signal, intelligence, and sustainment company (or the headquarters and headquarters company, division signal battalion) conduct incident reporting for the corps and division headquarters. When DODIN operations personnel identify an incident at corps or division (or a subordinate organization), they analyze the incident to determine whether it can be resolved locally. If the corps or division G-6 cannot identify a local solution, they escalate the incident to the next higher headquarters. If DODIN operations personnel cannot find a local solution, and a higher headquarters is not part of the incident handling protocol, corps and division DODIN operations personnel escalate the incident to the regional cyber center or joint network operations control center.

SECTION V – ROLES OF DEPARTMENT OF DEFENSE AND FEDERAL CYBERSECURITY CENTERS

A-61. The DOD and other federal entities have established cybersecurity centers to synchronize DODIN operations, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public and private sector stakeholders.

UNITED STATES CYBER COMMAND

A-62. USCYBERCOM directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. USCYBERCOM manages both the threat and asset responses for the DODIN and receives support from the other centers, as needed.

DEPARTMENT OF DEFENSE CYBER DEFENSE COMMAND

A-63. DOD Cyber Defense Command is a subordinate unified command under USCYBERCOM. In this role, DOD Cyber Defense Command leads the unified force approach to operations, security, and defense of the DODIN. This mission covers a broad range of activities on behalf of USCYBERCOM, including threat-informed steps to reduce cybersecurity risk and lead attack response across the DODIN.

UNITED STATES CYBER COMMAND INTEGRATED CYBER CENTER/JOINT OPERATIONS CENTER

A-64. The Integrated Cyber Center/Joint Operations Center directs cyberspace operations and defense of the DODIN. The USCYBERCOM director of operations, J-3 oversees all U.S. cyber forces across the globe from the Integrated Cyber Center/Joint Operations Center to coordinate and deconflict cyberspace operations worldwide. The Integrated Cyber Center/Joint Operations Center integrates the military, intelligence community, other federal agencies, and selected multinational partners. The center includes dedicated space for USCYBERCOM and National Security Agency personnel, who operate under different authorities. The center serves to link together the other federal cyber centers, the DOD components, and the intelligence community.

UNITED STATES ARMY CYBER COMMAND

A-65. Upon determining the category and impact of an incident, the regional cyber center reports details of the incident to ARCYBER. ARCYBER determines whether the incident is widespread within the DODIN or localized. ARCYBER provides recommendations, guidance, and orders to regional cyber centers, network enterprise centers, and units to respond and prevent repeat incidents.

DEPARTMENT OF DEFENSE CYBER CRIME CENTER

A-66. The DOD Cyber Crime Center supports the law enforcement, counterintelligence, cybersecurity, defensive cyberspace operations, and critical infrastructure protection communities through digital forensics, focused threat analysis, and training. The DOD Cyber Crime Center provides analytical and technical capabilities to interagency partners conducting national cyber incident response.

NATIONAL SECURITY AGENCY CYBERSECURITY THREAT OPERATIONS CENTER

A-67. The National Security Agency's Cybersecurity Threat Operations Center characterizes and assesses foreign cybersecurity threats. The center informs partners of current and likely malicious cyberspace activity through its analysis of foreign intelligence, with a focus on threat computer network attacks, capabilities, and exploits. Upon request, the National Security Agency Cybersecurity Threat Operations Center also provides technical assistance to other U.S. Government departments and agencies.

CYBER THREAT INTELLIGENCE INTEGRATION CENTER

A-68. Operated by the Office of the Director of National Intelligence, the Cyber Threat Intelligence Integration Center is the primary platform for intelligence integration, analysis, and supporting activities for the U.S. Government. The center provides integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE

A-69. The National Cyber Investigative Joint Task Force is a multi-agency center hosted by the Federal Bureau of Investigation. It is the primary platform to coordinate U.S. Government threat response.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

A-70. The Cybersecurity and Infrastructure Security Agency is the component of the Department of Homeland Security responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with the states, and improving U.S. government cybersecurity protection against private and nation-state hackers.

Appendix B

Cyberspace Electromagnetic Activities Planning and Integration

SECTION I – THE MILITARY DECISION-MAKING PROCESS

B-1. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). During the military decision-making process, CEWO maintains the cyberspace and EW running estimate and plans cyberspace and EW integration into unit's operation plans and orders.

RUNNING ESTIMATE

B-2. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Commanders and staffs use running estimates throughout the operations process. In their running estimates, the commander and each staff member continuously consider the effect of new information and update—

- Facts.
- Assumptions.
- Friendly force status.
- Enemy activities and capabilities.
- Civil considerations.
- Conclusions and recommendations.

B-3. The staff derives the running estimate from facts, assumptions, and situational analysis (terrain, friendly situation, enemy situation, and support requirements). CEWOs use the cyberspace and EW running estimate through each step of the military decision-making process. Planners update the running estimate when—

- The commander and staff recognize new facts.
- The staff can replace assumptions with facts or find previous assumptions invalid.
- The mission changes.
- Planners receive updated information from other staff sections (for example, the G-2 or S-2 updates the enemy situation template or the electromagnetic order of battle).

B-4. The cyberspace and EW running estimate outlines the CEMA section and the assigned or supporting cyberspace and EW elements' ability to support various friendly courses of action. CEWOs evaluate the cyberspace and EW requirements for each proposed course of action and match them with the available support. Evaluating the available support includes considering the capabilities and limitations of organic and supporting EW systems. CEMA sections must also account for threat and civilian use of cyberspace and the electromagnetic spectrum. An accurate running estimate is invaluable throughout the military decision-making process. If cyberspace and EW elements cannot support a proposed course of action, the running estimate helps the CEWO identify and articulate the shortfall. The cyberspace and EW running estimate includes all relevant information, including a mission analysis chart. Figure B-1 starting on page 112 shows an example of a cyberspace and EW running estimate.

1. SITUATION AND CONSIDERATIONS.

a. Area of Interest. *Identify and describe those factors of the area of interest that affect cyberspace and EW considerations*.

b. Characteristics of the Assigned Area.

(1) Terrain. *State how terrain affects cyberspace and EW capabilities*.

(2) Weather. *State how weather affects cyberspace and EW capabilities*.

(3) Enemy Forces. *Describe enemy disposition, composition, strength, and systems as they relate to cyberspace and electromagnetic warfare (EW) operations. Describe enemy capabilities and possible courses of action (COAs) and their effects on cyberspace and EW operations. List threat spectrum-dependent devices, including—*

- System nomenclature and disposition by echelon.
- System characteristics (frequency, bandwidth, power, and modulation).
- Threat tactics, techniques, and procedures, including threat means of communication.
- What the enemy employment of a system or capability is an indication or warning of.
- Frequency allocations and cueing cycles for radar systems.
- Modeling and simulations of systems, based on varying parameters and location.
- Critical capabilities and vulnerabilities by system.

(4) Friendly Forces. *List current cyberspace and EW resources in terms of equipment, personnel, and systems.*

- Friendly EW systems available, including—
  - System nomenclature and disposition by echelon.
  - System capabilities.
  - System information (configuration and location).
  - Constraints and limitations of each system.
  - Tactics, techniques, and procedures for each system.
  - Critical capabilities and vulnerabilities of each system.
  - Combinations of systems that can be used together or will cause conflict or require additional support.
- Friendly EW team capabilities and limitations, including—
  - Characteristics of EW systems.
  - Team line of sight and beyond line of sight characteristics.
  - Team mobility platform characteristics.
  - Team sustainment requirements.
- Friendly non-EW systems that depend on or emit in the electromagnetic spectrum, including—
  - System nomenclature by disposition and echelon (for example, terrestrial radios, satellite communications, radar, and unmanned aircraft systems).
  - System characteristics (frequency ranges, bandwidth requirements, power, and modulation).
  - Modeling and simulation of each system for configuration and location.
  - Constraints and limitations of each system.
  - Which friendly systems are vulnerable to threat EW capabilities.
- Friendly electromagnetic signatures, including—
  - System nomenclature by disposition and echelon (for example, vehicles and generators).
  - System characteristics (frequency ranges, power, and detection range).
- Identify additional cyberspace and EW resources located at higher echelon, adjacent, or other units. List those capabilities from other military and civilian partners that may be available to provide cyberspace and EW support. Compare requirements to current capabilities and suggest solutions for satisfying discrepancies.

(5) Civil Considerations. *Describe civil considerations that may affect cyberspace and the electromagnetic spectrum. Include possible cyber and EW support needed by civil authorities and possible interference from civil aspects, including—*

- Civilian networks in the unit's assigned area (for example, supervisory control and data acquisition, Internet service providers, and fiber optic infrastructure).
- Spectrum resources, allocation, and use (for example, Wi-Fi, television, radio, and satellite ground stations).
- Physical access to civilian infrastructure and equipment.
- Civilian use of computer systems and applications in the unit's assigned area (for example smartphones, social media, and navigation services).

Figure B-1. Example cyberspace and electromagnetic warfare running estimate

c. Facts and Assumptions. *List all facts and assumptions that affect cyberspace and EW operations*.

2. MISSION. *Show the restated mission resulting from mission analysis*.

3. COURSES OF ACTION.

a. *List friendly courses of action that were war-gamed*.

b. *List enemy actions or courses of action that were templated that impact cyberspace and EW operations*.

c. *List the evaluation criteria identified during* course of action *analysis. All staffs use the same criteria*.

4. ANALYSIS. *Analyze each course of action using the evaluation criteria from COA analysis. Review enemy actions that impact cyberspace and EW operations as they relate to courses of action. Identify issues, risks, and deficiencies these enemy actions may create with respect to cyberspace and EW operations*.

5. COMPARISON. *Compare courses of action. Rank order courses of action for each key consideration. Use a decision matrix to aid the comparison*.

6. RECOMMENDATIONS AND CONCLUSIONS.

a. *Recommend the most supportable course of action from the perspective of cyberspace and EW operations.*

b. Prioritize and list issues, deficiencies, and risks and provide recommendations on how to mitigate them.

Figure B-1. Example cyberspace and electromagnetic warfare running estimate (continued)

B-5. Commanders and staffs continually collect, process, and evaluate information throughout the military decision-making process. Staff members update their running estimates as they receive and assess new information. After course of action approval, the cyberspace and EW running estimate forms the basis for Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) to the operation plan or order.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

B-6. Information obtained as part of intelligence preparation of the operational environment is key to many planning activities. The CEMA section collaborates with the rest of the staff during intelligence preparation of the operational environment to analyze the mission variables in the assigned area. See chapter 4 for details about the G-2 or S-2 and CEMA section's roles in intelligence preparation of the operational environment.

STEPS OF THE MILITARY DECISION-MAKING PROCESS

B-7. The commander, CEMA section, and other staff integrate cyberspace and EW operations throughout the military decision-making process. The CEMA section relies heavily on collaboration with other members of the CEMA working group to plan, integrate, and synchronize cyberspace and EW operations and the G-6 or S-6 spectrum manager to deconflict spectrum use throughout the operations process. The military decision-making process consists of seven steps:

- Step 1—Receipt of mission.
- Step 2—Mission analysis.
- Step 3—Course of action development.
- Step 4—Course of action analysis.
- Step 5—Course of action comparison.
- Step 6—Course of action approval.
- Step 7—Orders production, dissemination, and transition.

STEP 1—RECEIPT OF MISSION

B-8. Commanders initiate the military decision-making process upon receipt or in anticipation of a mission. Members of the CEMA section participate throughout the military decision-making process to ensure integration and synchronization of cyberspace and EW operations into the overall operation. On receipt of mission, the CEMA section gathers the necessary tools to participate in step 2—mission analysis. These tools include—

- The cyberspace and EW running estimate, which includes—
  - Facts regarding cyberspace and the electromagnetic spectrum in the assigned area.
  - Assumptions regarding cyberspace and the electromagnetic spectrum in the assigned area.

  - Friendly forces' cyberspace and EW capabilities in the assigned area, including available technical data.
  - Outgoing unit's high-payoff target list recommendations, if applicable.
  - Outgoing unit's detailed frequencies of interest, if applicable.
  - Enemy activities and cyberspace and EW capabilities, including available technical data.
  - Electromagnetic order of battle from the G-2 or S-2.
- Relevant publications, including Army and joint regulations and doctrine on cyberspace and EW operations.
- All documents related to the mission and assigned area, including—
  - The higher headquarters' order, including operational graphics.
  - Maps and terrain products.
  - Known friendly, neutral, and threat cyberspace and EW capabilities and use of the electromagnetic spectrum in the unit's assigned area.
- Higher headquarters and other organizations' intelligence and assessment products on—
  - Friendly, neutral, and threat cyberspace and EW activities, use, and characteristics.
  - Cyberspace- and EW-related terrain aspects in the unit's assigned area.

B-9. The CEMA section begins updating the cyberspace and EW running estimate, especially the status of friendly forces, cyberspace and EW capabilities, use of the electromagnetic spectrum, and key civil considerations when employing cyberspace attack and electromagnetic attack. Considerations for the running estimate specific to the assigned area include—

- Civilian systems.
  - Airports (air traffic control radar and air-to-ground communications frequencies).
  - Cellular infrastructure (cell towers and cell service provider facilities).
  - Internet service providers and their connections to the public Internet.
  - Emergency services (police, fire, and ambulance).
  - Hospitals.
- Allied systems.
  - Communications.
  - Radar.
  - Intelligence, surveillance, and reconnaissance.
  - Satellite based positioning, navigation, and timing.
  - Offensive and defensive cyberspace capabilities.
  - Electromagnetic sensing and attack capabilities.
- Airspace deconfliction.
- Joint and other Service systems used in the assigned area.
  - Communications.
  - Radar.
  - Intelligence, surveillance, and reconnaissance.
  - Offensive cyberspace operations.
  - Ground-based and airborne EW capabilities.

B-10. The CEMA section conducts an initial assessment of time and resources available to plan, prepare, and execute cyberspace and EW operations that may support the commander's concept of operations. Table B-1 on page 115 illustrates the key inputs, substeps, and key outputs of the CEMA section during step 1 of the military decision-making process.

Table B-1. Military decision-making process step 1—receipt of mission.

Key Inputs	Substeps	Key Outputs
Commander's alert and initial guidance. Higher headquarters plan or order. Higher headquarters provides cyberspace and EW tools, including current running estimates.	Gather relevant cyberspace and EW tools. Prepare cyberspace and EW running estimate.	Updated cyberspace and EW running estimate. Consolidation of other relevant cyberspace and EW tools. Warning order to subordinate units.
Legend: EW electromagnetic warfare		

STEP 2—MISSION ANALYSIS

B-11. The military decision-making process continues with mission analysis to assess the situation. The commander and staff, informed by subordinate and adjacent commanders and joint and multinational partners, gather, analyze, and synthesize information to understand current conditions in the operational environment. Through mission analysis, the commander and staff generate situational understanding. They can then identify what the command must accomplish, when and where operations must take place, and why the operation is required.

B-12. The CEMA section analyzes and synthesizes the cyberspace and EW tools gathered during step 1 to develop understanding of cyberspace and the electromagnetic spectrum within the unit's assigned area. The CEMA section analyzes the higher headquarters order, focusing on the base order and Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations).

B-13. By analyzing the higher headquarters' order, the CEMA section develops understanding of the unit's cyberspace and EW tasks, purpose, and how they contribute to the mission, and the commander's intent and concept of operations. During mission analysis, the CEMA section uses the higher headquarters' order to develop understanding of available cyberspace and EW assets, the timeline of the operation, and other Services and multinational partners' cyberspace and EW missions in the assigned area.

B-14. During mission analysis, the G-2 or S-2 leads intelligence preparation of the operational environment to analyze the mission variables of enemy, terrain and weather, and civil considerations in an area of interest. The Air Force staff weather officer can assist the G-2 or S-2 in analysis of weather and terrain considerations as a subject matter expert in terrestrial and space weather analysis. The CEMA section collaborates with the G-2 or S-2 throughout intelligence preparation of the operational environment to help analyze the effects of those variables on cyberspace and EW operations. The G-2 or S-2 continually updates the electromagnetic order of battle. This collaboration includes using tools and products received from higher headquarters to conduct the initial terrain analysis.

B-15. Intelligence preparation of the operational environment identifies critical gaps in the commander's knowledge of the operational environment, including gaps in one or more of cyberspace and spectrum-related aspects of the terrain, threat, and overall operational environment. The commander and staff use these gaps as a guide to establish their information requirements.

B-16. The CEMA section identifies and nominates information requirements to address information gaps identified during mission analysis to develop situational understanding of cyberspace and the electromagnetic spectrum. The CEMA section and other staff sections' input to intelligence preparation of the operational environment during mission analysis results in—

- Initial priority intelligence requirements.
- A complete modified combined obstacle overlay with cyberspace and EW considerations within the assigned area.
- Threat overlays, including—

  - Cyberspace and electromagnetic spectrum considerations within the assigned area.
  - How threat units communicate.
  - Likely threat command and control links.
- A list of cyberspace- and spectrum-related high-value targets.
- Identified cyberspace- and spectrum-related military aspects of the terrain.
- Unrefined event templates and matrixes that include cyberspace and EW considerations.

B-17. The CEMA section analyzes the higher headquarters' order and the higher commander's guidance to determine their specified, implied, and essential cyberspace and EW tasks. The 'what' of a mission statement in the higher headquarters' plan or order is always a task. The CEMA section determines essential tasks from the specified and implied cyberspace and EW tasks in the unit's recommended mission statement.

B-18. The CEMA section analyzes the current task organization of the unit's cyberspace and EW assets, command and support relationships for augmentation, and status of current cyberspace and EW capabilities and their limitations. The CEMA section also analyzes the cyberspace and EW capabilities of adjacent Army units and joint and multinational partners. This analysis results in the CEMA section determining whether the unit has the assets needed to complete all specified, implied, and essential tasks and to identify other cyberspace and EW resources required or available to fulfill those tasks for mission success. The CEWO informs the commander of all identified cyberspace and EW resource gaps that need forwarding to higher headquarters. The CEMA section advises the commander of any deviations necessary from the standard task organization to consider when developing planning guidance.

B-19. The CEMA section identifies constraints placed on the unit regarding cyberspace and EW operations. Constraints should appear in paragraph 3 of the higher headquarters' order. They may also appear in Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of the higher headquarters' order. The CEMA section should be aware of cyberspace and EW limitations, including—

- Spectrum usage.
- The types of cyberspace and EW capabilities allowed or disallowed.
- Cyberspace and EW authorities, either delegated or not delegated to the unit commander.
- Higher headquarters' EMCON criteria.

B-20. The CEMA section gathers critical facts based on analyzing the operational and mission variables provided through intelligence preparation of the operational environment and from adjacent, higher, and joint organizations and other mission partners. This information helps with developing assumptions for cyberspace and the electromagnetic spectrum throughout the assigned area. In the absence of facts, the CEMA section makes informed, relevant assumptions about the use of cyberspace and the electromagnetic spectrum within their assigned area. These assumptions include known threat cyberspace and EW capabilities, use of the electromagnetic spectrum, and projected locations. Staffs should limit their assumptions to only those needed to support decision making.

B-21. The CEMA section uses the risk management process to mitigate cybersecurity vulnerabilities. The CEMA section collaborates with the G-6 or S-6 spectrum manager to review the joint restricted frequency list and mitigate possible frequency and network conflicts. The CEMA section plans electromagnetic protection to—

- Mitigate electromagnetic environmental effects.
- Mitigate electromagnetic compatibility issues.
- Implement electromagnetic hardening.
- Implement electromagnetic masking.
- Implement EMCON.

B-22. During mission analysis, the CEMA section identifies cyberspace- and spectrum-related gaps in the information received from higher headquarters, adjacent and joint units, and multinational partners. These gaps are relayed to the commander for consideration as commander's critical information requirements, which fall into two categories—priority intelligence requirements and friendly force information requirements.

B-23. The CEMA section works closely with the G-3 or S-3 and the G-2 or S-2 in developing the initial information collection plan. The CEMA section also works with these sections to adjust the information

collection effort to answer information requirements necessary to develop an effective plan. The CEMA section nominates cyberspace- and EW-related information requirements as part of their contribution to the information collection plan.

B-24. The initial information collection plan sets intelligence, surveillance, reconnaissance, and security, operations in motion. The G-2 or S-2 manages information collection and works closely with the G-3 or S-3 to collect information supporting intelligence preparation of the operational environment by synchronizing all available combat information, intelligence products, and electromagnetic support capabilities to satisfy the commander's information requirements and develop situational understanding.

B-25. As more information becomes available, the CEMA section updates the cyberspace and EW running estimate. This may result in recommended adjustments to the operation plan or order. The CEMA section considers the time available by comparing the time needed to accomplish cyberspace and EW tasks to the higher headquarters' timeline and determines whether mission accomplishment is possible within the allotted time. The CEMA section makes the necessary adjustments to the operation plan or order to stay within the higher headquarters' timeline and informs the commander of any task that cannot be accomplished within the allotted time, especially critical and essential tasks. The commander uses this information to make informed risk decisions and to inform the higher headquarters of gaps identified due to timeline constraints.

B-26. The CEMA section contributes cyberspace and EW subject matter expertise to development of course of action evaluation criteria. Developing these criteria during mission analysis helps eliminate bias before analyzing and comparing courses of action. Table B-2 on page 118 illustrates the key inputs, substeps, and key outputs during step 2—mission analysis.

Table B-2. Military decision-making process step 2—mission analysis

Key Inputs	Substeps	Key Outputs
Commander's initial guidance. Higher headquarters' tools, including operation order, intelligence products, and knowledge products. Knowledge products from other organizations.	Analyze cyberspace and EW information from higher headquarters tools. Participate in intelligence preparation of the operational environment. Analyze higher headquarters order for specified, implied, and essential tasks. Examine current task organization of cyberspace and EW assets. Examine cyberspace and EW capabilities of adjacent units and joint, other Service, and multinational partners. Gather critical facts to develop assumptions. Begin risk management process for cyberspace and EW assets. Continue analysis of the higher headquarters' cyberspace and EW information. Participate in mission analysis briefing.	Understanding of unit's cyberspace and EW tasks, purpose, and contribution. Understanding of available cyberspace and EW assets and timeline. Understanding of the missions of adjacent, supported, and supporting units. Awareness of the operational environment in the assigned area, including mission partners. Understanding of critical gaps in cyberspace and the electromagnetic spectrum. Initial cyberspace and EW intelligence requirements. Specified, implied, and essential tasks. List of assets needed to complete specified, implied, and essential tasks. Additional cyberspace and EW resources needed (request from higher headquarters). Awareness of deviation from normal task organization to assist in course of action development. Cyberspace and EW constraints. Cyberspace and EW assumptions (friendly and threat). Cyberspace and EW information requirements. Updated cyberspace and EW running estimate. Recommended evaluation criteria for course of action evaluation. Warning order to subordinate units.

Legend:
EW electromagnetic warfare

STEP 3—COURSE OF ACTION DEVELOPMENT

B-27. Courses of action are broad potential solutions to a specific military problem. Course of action development generates options for subsequent analysis and comparison to satisfy the commander's intent and planning guidance. During course of action development, the staff uses the planning products received and analyzed from higher headquarters, adjacent and joint units, and multinational partners in conjunction

with the commander's intent and planning guidance. The CEMA section contributes to course of action development by integrating and synchronizing cyberspace and EW operations into proposed courses of action using operational art. During course of action development, the CEMA section develops varying methods to integrate, synchronize, and conduct cyberspace and EW operations that are within the commander's intent and planning guidance.

B-28. The CEMA section assists the other staff with examining each proposed course of action for validity using the evaluation criteria established during mission analysis. When considering the validity of each proposed course of action, screening criteria should include—

- **Feasibility.** Cyberspace and EW operations integrated and synchronized into the proposed courses of action to accomplish the mission within the established time, space, and cyberspace and EW resource limitations.
- **Acceptability.** Cyberspace and EW operations integrated and synchronized into the proposed courses of action to balance cost and risk with the advantage gained.
- **Suitability.** Cyberspace and EW operations support the courses of action to accomplish the mission within the commander's intent and planning guidance.
- **Distinguishability.** Cyberspace and EW operations integration, synchronization, and conduct of operations should be different for each course of action developed. Differences should include task organization, cyberspace and EW capabilities, and the use of cyberspace and EW resources from adjacent units and joint and multinational partners.
- **Completeness.** Cyberspace and EW operations integrated and synchronized into the proposed courses of action should incorporate—
  - How cyberspace and EW operations support each course of action, accounting for offensive, defensive, and stability or defense support of civil authorities' tasks.
  - How cyberspace and EW operations enable the main and supporting efforts.
  - How to perform cyberspace and EW operations specified, implied, and essential tasks to create desired conditions in cyberspace and the electromagnetic spectrum.
  - How cyberspace and EW operations will help achieve the commander's objectives.
  - How to use cyberspace and EW capabilities to mitigate obstacles, gain access to various avenues of approach (including observation and fields of fire), and protect key terrain in cyberspace and the electromagnetic spectrum.

B-29. During course of action development, the commander and staff need to understand and appreciate the unpredictable and uncertain nature of their operational environment. The CEMA section should show this same understanding and appreciation for unpredictability and uncertainty when supporting the development of schemes of cyberspace and EW operations for each course of action.

B-30. The CEMA section makes recommendations for cyberspace and EW operations as enablers for combat power (assess the dynamics of combat power).

B-31. The CEMA section identifies and assesses organic and non-organic cyberspace and EW capabilities available for the operation, along with the dependency of the unit and its systems on cyberspace and the electromagnetic spectrum. This assessment assists the CEMA section in making a rough estimate of the ratio of friendly cyberspace and EW capabilities to known or anticipated enemy cyberspace and EW capabilities.

B-32. The CEMA section compares the combined (organic and non-organic) friendly cyberspace and EW capabilities against enemy cyberspace and EW vulnerabilities, and vice versa. The CEMA section uses this comparison to identify vulnerabilities in friendly cyberspace and the electromagnetic spectrum and gain insight into enemy vulnerabilities to exploit throughout the assigned area.

B-33. Based on the commander's guidance and the initial results of relative combat power assessment, the CEMA section generates different schemes of cyberspace and EW operations to support the staff's proposed courses of action. The scheme for each course of action should indicate opposition toward each likely enemy course of action while accounting for essential stability tasks (providing a level of civil security, civil control, and certain essential services). The staff incorporates brainstorming to generate options to produce the broadest range of choices in establishing schemes of cyberspace and EW operations for the courses of action. All staff members should remain unbiased and open-minded when brainstorming proposed options.

B-34. The CEMA section determines the necessary Army and joint requirements for cyberspace operations, EW, and supported and supporting operations. The CEMA section further considers cyberspace and EW capabilities of non-organic units and other non-military organizations and agencies.

B-35. The commander and staff develop an operational framework to visualize and describe the application of combat power in time, space, purpose, and resources while developing the concept of operations. The three models commonly used to build an operational framework are—

- Assigned areas.
- Deep, close, and rear operations.
- Main effort, supporting effort, and reserve.

B-36. The staff brainstorms to generate options on how to provide the necessary cyberspace and EW capabilities to support the three components of the operational framework. Once the CEMA section has explored approaches to provide cyberspace and EW operations support for each course of action, the staff examines each course of action to determine whether it satisfies the evaluation criteria (see paragraph B-26), changing, adding, and eliminating courses of action as appropriate. The CEMA section places extensive focus on cyberspace and EW operations to support each proposed course of action during the screening. The staff should avoid creating one good course of action among several inadequate courses of action when generating options.

B-37. The CEMA section determines the necessary cyberspace and EW capabilities to employ as enablers for combat power required to support deep, close, and rear operations. The CEMA section also considers the relative cyberspace and EW capabilities necessary to shape the operational environment, resulting in an initial array that identifies the cyberspace and EW assets needed to accomplish the mission. The CEMA section adds this information to the unit's total array of forces used in the commander's broad concept of operations. In the concept of operations, the commander describes how arrayed forces accomplish the mission within the commander's intent.

B-38. The CEMA section participates in the course of action briefing in which the staff briefs each proposed course of action to the commander. The CEWO briefs the commander on the cyberspace and EW activities and capabilities included in each course of action, including anticipating effects on the operational and mission variables. The CEWO also describes how cyberspace and EW effects may result in or support the desired outcome in each proposed course of action. After the course of action briefing, the commander selects or modifies courses of action for continued analysis and issues planning guidance.

B-39. Throughout course of action development, the CEMA section continues to update the cyberspace and EW running estimate and intelligence preparation of the operational environment products (such as modified combined obstacle overlays, electromagnetic order of battle, high-value target list, threat courses of action, and key aspects of terrain). Table B-3 on page 121 illustrates the CEMA section's key inputs, substeps, and key outputs of the during course of action development.

Table B-3. Military decision-making process step 3—course of action development

Key Inputs	Substeps	Key Outputs
Mission statement, planning guidance, and commander's intent. Commander's critical information requirements. Updated intelligence preparation of the operational environment products. Higher headquarters' cyberspace and EW tools, included updated running estimates.	Generate cyberspace and EW options for each proposed course of action. Assist staff in examining each course of action for validity. Assess cyberspace and EW as functions of combat power. Assess available organic and non-organic cyberspace and EW capabilities. Compare friendly cyberspace and EW capabilities against threat forces and vice versa. Determine joint and Army doctrine requirements. Develop cyberspace and EW statements and sketches. Participate in operational framework development. Participate in course of action briefing.	Validated cyberspace and EW support for each propose course of action. Approximate ration of friendly-to-threat cyberspace and EW capabilities. Identified vulnerabilities in cyberspace and the electromagnetic spectrum. List of cyberspace and EW capabilities needed to support specified, implied, and essential tasks. Updated cyberspace and EW running estimate. Updated intelligence preparation of the operational environment products. Cyberspace and EW sketches for proposed courses of action. • Task organization of supporting cyberspace and EW assets. • How cyberspace and EW operations support the larger operation.

Legend:
EW electromagnetic warfare

B-40. Using the information obtained through the collaborative efforts of all staff sections, the CEMA section develops cyberspace and EW statements and sketches for the G-3 or S-3 to incorporate with the statement and supporting sketches for each course of action. The statement expresses how cyberspace and EW operations contribute to a combined arms approach for the course of action. The sketch provides visuals of how cyberspace and EW operations will support maneuver forces, including the positioning of forces.

B-41. The commander may reject all courses of action, accept one or more courses of action, or incorporate elements of two or more presented courses of action into a new course of action. If the commander rejects all proposed courses of action, the staff starts over at developing new courses of action. Accepted or modified courses of action move forward to step 4—analysis and war-gaming.

STEP 4—COURSE OF ACTION ANALYSIS AND WAR-GAMING

B-42. Course of action analysis helps the commander and staff to identify difficulties, coordination problems, or probable consequences of planned actions for each course of action accepted or modified during course of action development. During this step, the CEMA section identifies cyberspace and electromagnetic spectrum vulnerabilities in each proposed course of action. These vulnerabilities may include—

- Likely undesirable cyberspace and EW effects to the operational and mission variables and undesired impacts on cyberspace and EW capabilities due to the operational and mission variables.
- Possible coordination issues with non-organic organizations for cyberspace and EW support.
- Lack of available cyberspace and EW capabilities to achieve the desired outcome.

- Reduced survivability due to enemy observation of cyberspace activity or electromagnetic emissions.

B-43. The CEMA section uses this information to revisit and refine cyberspace and EW portions of the course of action as discrepancies arise. Analysis may also reveal potential execution problems, decisions, and contingencies and may require restarting the planning process.

B-44. One process used to analyze courses of action is called war-gaming. War-gaming consists of rules and steps to visualize the flow of an operation, given the force's strengths and disposition, the enemy's capabilities, and each proposed course of action. War-gaming incorporates the mission variables into the scenario to include the impact and requirements of civilians in the assigned area.

B-45. Through war-gaming, the CEMA section can visualize and articulate the required capabilities to affect cyberspace and EW targets in the assigned area. The CEMA section can also identify vulnerabilities that may require cyberspace defense and electromagnetic protection. During war-gaming, the CEMA section assists the G-3 or S-3 in the war-gaming process by employing and assessing cyberspace and EW operations as part of the friendly scheme of maneuver. The CEMA section also assists the G-3 or S-3 by providing cyberspace and EW input into the course of action statement and supporting sketch for each course of action. War-gaming results in refined courses of action with updated schemes of cyberspace and EW operations, a completed synchronization matrix, and decision support templates and matrixes for each course of action.

Note. The G-6 or S-6 assesses DODIN operations, spectrum management operations, and their feasibility for each war-gamed course of action with input from the CEMA section regarding threat cyberspace and EW capabilities and courses of action.

B-46. A synchronization matrix records the results of a war game and depicts how friendly forces synchronize in time, space, and purpose relating to an enemy course of action for each proposed friendly course of action. The depiction includes the synchronization and integration of cyberspace and EW operations in support of the warfighting functions for each course of action. The decision support template and matrix illustrate key decisions and potential actions that are likely to arise during the execution of each course of action.

B-47. The CEMA section participates in the war game briefing, delivering a brief to subordinate cyber and EW elements to ensure everyone understands the results of the war game. The CEMA section captures all cyberspace and EW-related points of the war game before presenting the briefing to the commander. The CEMA section drafts and submits a CERF or electromagnetic attack request format for additional cyberspace and EW assets to mitigate capability gaps and vulnerabilities identified during war-gaming. Table B-4 on page 123 illustrates the key inputs, substeps, and key outputs of the CEMA section during course of action analysis and war-gaming.

Table B-4. Military decision-making process step 4—course of action analysis and war-gaming

Key Inputs	Substeps	Key Outputs
Revised commander's planning guidance. Proposed courses of action, including cyberspace and EW solutions. Updated intelligence preparation of the operational environment products. Higher headquarters' cyberspace and EW tools, including cyberspace and EW running estimate. Assumptions from previous steps.	Participation in war-gaming courses of action. Identify cyberspace and EW vulnerabilities for each war-gamed course of action. Draft request for support documents for additional cyberspace and EW support. Provide cyberspace and EW input for the synchronization matrix.	Refine cyberspace and EW support for each course of action. Refined intelligence preparation of the operational environment products for targeting and overlays. Additional input to commander's critical information requirements. Submitted request for cyberspace and EW support. Updated cyberspace and EW running estimate. Updated assumptions.

Legend:
EW electromagnetic warfare

STEP 5—COURSE OF ACTION COMPARISON

B-48. The commander and staff evaluate war-gamed courses of action objectively and independently against the evaluation criteria established during mission analysis and refined during course of action development. The goal is to identify the strengths and weaknesses of each proposed course of action, select the course of action with the highest probability of success, and further develop the operation plan or order.

B-49. The CEMA section analyzes advantages and disadvantages of each proposed course of action against the evaluation criteria (see paragraph B-26) using a decision matrix. The CEMA section highlights the cyberspace and EW advantages and disadvantages for each proposed course of action. The CEMA section presents those findings to the commander and other staff members. Feedback received in response to the CEMA section's CERFs and electromagnetic attack request formats contributes to the determining factors during the advantage and disadvantage analysis.

B-50. The staff implements findings from the analysis of advantages and disadvantages into a decision matrix for the commander to compare and evaluate courses of action thoroughly and logically. A decision matrix assists the commander in making a sound decision.

B-51. After analysis and comparison, the staff identifies the preferred course of action and makes a recommendation. If the staff cannot reach a decision, the chief of staff (executive officer) decides which course of action to recommend. Table B-5 on page 124 illustrates the actions and key outputs of the CEMA section during course of action comparison.

Table B-5. military decision-making process step 5—course of action comparison

Key Inputs	Substeps	Key Outputs
Updated intelligence preparation of the operational environment products. Refined courses of action with updated schemes of cyberspace and EW operations. Higher headquarters cyberspace and EW tools, including current running estimate. Feedback from submitted cyberspace and EW requests for support from higher headquarters.	Conduct advantage and disadvantage analysis for each course of action. Compare courses of action with the CEMA section focusing on the cyberspace and EW aspects of each criterion.	Recommended course of action. Updated cyberspace and EW running estimate.

Legend:
CEMA cyberspace electromagnetic activities
EW electromagnetic warfare

STEP 6—COURSE OF ACTION APPROVAL

B-52. The staff delivers a decision briefing to the commander with the chief of staff highlighting changes to each course of action resulting from the war game. After the decision briefing, the commander selects the course of action that best accomplishes the mission. If the commander rejects all courses of action, the staff restarts the course of action development process. If the commander modifies a proposed course of action or gives the staff an entirely different course of action, the staff war-games the new course of action and presents the results to the commander with a recommendation.

B-53. Upon approval of a course of action, the commander issues the final planning guidance that includes a refined commander's intent and new commander's critical information requirements to support execution. The final planning guidance also contains any additional guidance on priorities for the warfighting functions, orders preparation, rehearsals, and preparation activities. It also includes priorities to preserve freedom of action and ensure continuous sustainment.

B-54. The commander identifies the acceptable risk level in the final planning guidance to gain approval from the higher commander before accepting risks that could affect the higher commander's mission. Based on the commander's decision and final planning guidance, the staff converts the approved course of action into the concept of operations and issues a warning order to subordinate commanders. The CEMA section provides input to the warning order, as required. The CEMA section continues refining Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of the plan or order and assists the G-6 or S-6 with Appendixes 1 and 6 of Annex H as appropriate. Table B-6 on page 125 illustrates the key inputs, substeps, and key outputs of the CEMA section during course of action approval.

Table B-6. Military decision-making process step 6—course of action approval

Key Inputs	Substeps	Key Outputs
Updated cyberspace and EW running estimate. Evaluated courses of action. Recommended course of action. Higher headquarters' cyberspace and EW tools, including current running estimate. Feedback from submitted cyberspace and EW requests for support from higher headquarters.	Participate in course of action decision briefing to select the staff's recommended course of action. Review commander's final planning guidance. Review the commander's acceptable risk tolerance. Provide cyberspace and EW input for the warning order.	Commander's final planning guidance. Approved course of action. Commander's risk decisions. Draft Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Assistance to G-6 or S-6 with Draft Annex H (Signal) appendixes 1 and 6. Refined commander's intent. Refined commander's critical information requirements. Refined essential elements of friendly information. Updated assumptions. Warning order to subordinate headquarters.
Legend: EW electromagnetic warfare		

STEP 7—ORDERS PRODUCTION, DISSEMINATION, AND TRANSITION

B-55. The staff turns the approved course of action into an operation plan or order with a clear, concise concept of operations and supporting information. The course of action statement becomes the concept of operations for the plan or order. The CEMA section drafts the final Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations). The CEMA section assists the G-6 or S-6 with appendixes 1 and 6 of Annex H (Signal) as appropriate.

B-56. Before the commander approves the plan or order, the staff ensures its consistency and that it is nested with the higher commander's intent through plans and orders reconciliation and crosswalk. The staff reconciles the plan or order by conducting a detailed review of the entire plan or order and all attachments, ensuring all staff members are in complete agreement. During reconciliation, the staff explicitly compares the commander's intent, mission, and commander's critical information requirements against the concept of operations and the different schemes of support, including those for cyberspace and EW operations. Any discrepancies or gaps in planning receive corrective actions.

B-57. The staff conducts the plans and orders crosswalk by comparing the plan or order with those of the higher and adjacent commanders to achieve unity of effort and ensure the plan meets the higher commander's intent. As with reconciliation, the crosswalk also identifies discrepancies or gaps in planning that require corrective actions. Step 7 bridges the transition between the planning and preparation activities of the operations process. The final function of step 7 is the commander's approval. The commander signs the plan or order, the G-3 or S-3 disseminates the approved plan or order to subordinate headquarters, and the commander and staff begin the transition to the preparation activities of the operations process. Table B-7 on page 126 illustrates the key inputs, substeps, and key outputs of the CEMA section during orders production, dissemination, and transition.

Table B-7. Military decision-making process step 7—orders production, dissemination, and transition

Key Inputs	Substeps	Key Outputs
Approved course of action. Higher headquarters' cyberspace and EW tools, including updated cyberspace and EW running estimate and electromagnetic order of battle. Feedback from submitted cyberspace and EW requests for support. Draft Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations).	Participate in plans and orders reconciliation. Participate in plans and orders crosswalk. Commander's review of the draft plan or order.	Approved plan or order with finalized attachments, including Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) with tabs and CEMA input to Annex H (Signal). Dissemination of approved plan or order to subordinate headquarters. Transition to preparation activities.

Legend:
CEMA cyberspace electromagnetic activities
EW electromagnetic warfare

OPERATION PLAN OR ORDER

B-58. Cyberspace and EW information appears in various paragraphs to Annex C (Operations) and Annex H (Signal) of an operation plan or order. The scheme of cyberspace and EW operations appears in paragraph 3.g. (Cyberspace Electromagnetic Activities) and 5.g. (Signal) of operation plans, operation orders, and fragmentary orders. In warning orders, cyberspace and EW operations information appears in paragraph 5.g. (Signal).

PARAGRAPH 3.E. (SCHEME OF INFORMATION COLLECTION)

B-59. The CEWO coordinates with the collection manager and the technical control and analysis cell to coordinate who and when in time and space the CEMA section can answer information requirements based on organic assets. This coordination includes priority intelligence requirements and friendly force information requirements. Refer to ATP 3-12.4 for examples.

PARAGRAPH 3.F. (SCHEME OF FIRES)

B-60. The CEWO fulfills three main objectives in supporting the scheme of fires—

- Establishing synchronization between electromagnetic support assets and gun target lines or mortar firing points and optimizing the lethal to nonlethal turnover time to reduce the time commanders (at echelon) spend making decisions.
- Applying appropriate electromagnetic attack when applicable to accomplish the commander's objectives.
- Nominating targets for lethal or nonlethal attack, based on cyberspace or electromagnetic spectrum considerations of either their exposure or value.

PARAGRAPH 3.G. (SCHEME OF PROTECTION)

B-61. Paragraph 3.g. (Cyberspace Electromagnetic Activities) describes how cyberspace and EW operations support the concept of operations and refers readers to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations), Annex E (Protection), and Annex H (Signal) as required.

PARAGRAPH 3.K. (COORDINATING INSTRUCTIONS)

B-62. The CEMA section's input to paragraph 3.k. (Coordinating Instructions) should include any cyberspace operations or EW tasks that apply to two or more units, such as task organization of EW teams with scout elements or SIGINT elements.

PARAGRAPH 5.G. (SIGNAL)

B-63. Paragraph 5.g. (Signal) contains information regarding DODIN operations and spectrum management operations. The CEMA spectrum manager collaborates with the G-6 or S-6 spectrum manager to deconflict frequency use between friendly EW and communications requirements.

ANNEX B (INTELLIGENCE)

B-64. The CEMA section draws relevant cyberspace and EW threat information from paragraph 1.c (Situation) of Annex B (Intelligence). Paragraph 3.d summarizes SIGINT and electromagnetic support tasks. Appendix 3 summarizes key tasks and requirements for SIGINT support.

ANNEX D (FIRES)

B-65. The CEMA section provides cyberspace and EW targeting information, including desired effects to contribute to the scheme of fires.

ANNEX E (PROTECTION)

B-66. The CEMA section describes how electromagnetic protection, defensive cyberspace operations, and cybersecurity tasks support the scheme of protection in paragraph 3.a. Scheme of Protection, of the operation plan or order.

APPENDIX 5 (SPECTRUM MANAGEMENT OPERATIONS) TO ANNEX H (SIGNAL)

B-67. The CEMA spectrum manager assists the G-6 or S-6 spectrum manager in preparing Appendix 5—Spectrum Management Operations, to Annex H (Signal).

ANNEX L (INFORMATION COLLECTION)

B-68. Paragraph 3.a. (5) (d). (Cyberspace Electromagnetic Activities Support). Summarize limitations or any special considerations regarding intelligence, surveillance, and reconnaissance platform or sensor tasking. Refer to Annex D (Fires) regarding procedures for submitting reconnaissance objectives and determining collection priorities. This is only applicable to tactical and operational units providing cyberspace and EW support or conducting cyberspace and EW operations. This is accomplished through participation in the development of the information collection plan (see paragraph 4-71).

ANNEX N (SPACE OPERATIONS)

B-69. The CEMA section assists the space officer as necessary in preparing paragraph 3.b. (11) of the operation plan or order.

APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS)

B-70. The CEWO has primary staff responsibility for preparing Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of the operation plan or operation order. Attachments to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) include—

- Tab A—Offensive Cyberspace Operations.
- Tab B—Defensive Cyberspace Operations.
- Tab C—Electromagnetic Attack.
- Tab D—Electromagnetic Protection.
- Tab E—Electromagnetic Support.

B-71. Figure B-2 starting on page 128 shows the instructions for preparation of Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations). Refer to FM 5-0 for more information about plans, orders, and planning processes.

[CLASSIFICATION]

Place the classification at the top and bottom of every page of the OPLAN or OPORD. Place the classification marking at the front of each paragraph and subparagraph in parentheses. See AR 380-5 for classification and release marking instructions.

Copy ## of ## copies
Issuing headquarters
Place of issue
Date-time group of signature
Message reference number

Include the full heading if attachment is distributed separately from the base order or higher-level attachment.

APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

(U) **References:** *Add any specific references to cyberspace electromagnetic activities (CEMA), if needed.*

1. (U) Situation. *Include information affecting cyberspace operations and electromagnetic warfare (EW) that paragraph 1 of Annex C (Operations) does not cover or that needs expansion.*

a. (U) Area of Interest. *Include information affecting cyberspace and the electromagnetic spectrum; cyberspace may expand the area of local interest to a worldwide interest.*

b. (U) Assigned Area. *Include information affecting cyberspace and the electromagnetic spectrum; cyberspace may expand the assigned area outside the physical maneuver space.*

c. (U) Enemy Forces. *List known and templated locations and cyberspace and EW unit activities for one echelon above and two echelons below the order. Identify the vulnerabilities of enemy information systems and cyberspace and EW systems. List enemy cyberspace and EW operations that will impact friendly operations. State probable enemy courses of action and employment of enemy cyberspace and EW assets. See Annex B (Intelligence) as required.*

d. (U) Friendly Forces. *Outline the higher headquarters' CEMA plan. List plan designation, location and outline of higher, adjacent, and other cyberspace and EW operations assets that support or impact the issuing headquarters or require coordination and additional support. Identify friendly cyberspace and EW operations assets and resources that affect the subordinate commander. Identify friendly forces cyberspace and electromagnetic spectrum vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the electromagnetic spectrum, especially for joint or multinational operations. Deconflict and prioritize spectrum distribution.*

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. *Identify and describe other organizations in the assigned area that may impact cyberspace and EW operations or implementation of cyberspace and EW operations specific equipment and tactics. See Annex V (Interagency) as required.*

f. (U) Third Party. *Identify and describe other organizations, both local and external to the assigned area that can influence cyberspace and EW operations or the implementation of cyberspace and EW operations specific equipment and tactics. This category includes criminal and non-state sponsored rogue elements.*

g. (U) Civil Considerations. *Describe the aspects of the civil situation that impact cyberspace and EW operations. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to Annex B (Intelligence) and Annex K (Civil Affairs Operations) as required.*

[page number]
[CLASSIFICATION]

Figure B-2. Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of an operation plan or order

[CLASSIFICATION]

h. (U) Attachments and Detachments. *List units attached or detached only as necessary to clarify task organization. List any cyberspace and EW operations assets attached or detached, and resources available from higher headquarters. See Annex A (Task Organization) as required.*

i. (U) Assumptions. *List any CEMA specific assumptions.*

2. (U) **Mission**. *State the commander's mission and describe cyberspace and EW operations to support the base plan or order.*

3. (U) Execution.

a. Scheme of Cyberspace Electromagnetic Activities. *Describe how cyberspace and EW operations support the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how cyberspace and EW effects will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive cyberspace and EW measures. Identify target sets and effects, by priority. Describe the general concept for the integration of cyberspace and EW operations. List the staff sections, elements, and working groups responsible for aspects of CEMA. Include the cyberspace and EW collection methods for information developed in staff sections, elements, and working groups outside the CEMA section and working group. Describe the plan for the integration of governmental and nongovernmental partners and organizations. See Annex C (Operations) as required. This section is designed to provide insight and understanding of the components of cyberspace and EW and how these activities are integrated across the operation plan. It is recommended that this appendix include an understanding of technical requirements. This appendix concentrates on the integration requirements for cyberspace and EW operations and references appropriate annexes and appendixes as needed to reduce duplication.*

(1) (U) Organization for Combat. Provide direction for the proper organization for combat, including the unit designation, nomenclature, and tactical task.

(2) (U) Miscellaneous. Provide any other information necessary for planning not already mentioned.

b. (U) Scheme of Cyberspace Operations. *Describe how cyberspace operations support the commander's intent and concept of operations. Describe the general concept for the implementation of planned cyberspace operations measures. Describe the process to integrate joint and multinational partners and nongovernmental organizations into operations, including cyberspace requirements and constraints. Identify risks associated with cyberspace operations. Include collateral damage, discovery, attribution, fratricide (to U.S., allied, or multinational networks or information), and possible conflicts. Describe actions that will prevent enemy and adversary action(s) to critically degrade the combatant command's ability to effectively conduct military operations in its assigned area. Identify countermeasures and the responsible agency. List the warnings, and how they will be monitored. State how the cyberspace operations tasks will destroy, degrade, disrupt, and deny enemy computer networks. Identify and prioritize target sets and effect(s) in cyberspace. If appropriate, state how cyberspace operations support the accomplishment of the operation. Identify plans to detect or assign attribution of enemy and adversary actions in the physical domains and cyberspace. Ensure subordinate units are conducting defensive cyberspace operations. Synchronize the CEMA section with the G-39. Pass requests for offensive cyberspace operations to higher headquarters for approval and implementation. Describe how DODIN operations support the commander's intent and concept of operations. Synchronize DODIN operations with the G-6 or S-6. Prioritize the allocation of applications utilizing cyberspace. Ensure the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Considerations should be made for degraded networks. (Reference appropriate annexes and appendixes as needed to reduce duplication).*

[page number]

[CLASSIFICATION]

Figure B-2. Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of an operation plan or order (continued)

[CLASSIFICATION]

(1) (U) DODIN Operations. *Describe how Department of Defense information network operations are coordinated, synchronized, and support operations integrated with the G-6 or S-6 to design, build, configure, secure, operate, maintain, and sustain networks. See Annex H (Signal) as required.*

(2) (U) Defensive Cyberspace Operations. *Describe how defensive cyberspace operations are conducted, coordinated, integrated, synchronized, and support operations to defend the DODIN-A and preserve the ability to utilize friendly cyberspace capabilities.*

(3) (U) Offensive Cyberspace Operations. *Describe how offensive cyberspace operations are coordinated, integrated, synchronized, and support operations to achieve real-time awareness and direct dynamic actions and response actions. Include target identification and operational pattern information, exploit and attack functions, and maintain intelligence information. Describe the authorities required to conduct offensive cyberspace operations.*

c. (U) Scheme of Electromagnetic Warfare. *Describe how EW supports the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how the EW tasks will degrade, disrupt, deny, and deceive the enemy. Describe the process to integrate and coordinate mission partner EW capabilities which support the commander's intent and concept of operations. State the electromagnetic attack, electromagnetic protection, and electromagnetic support measures and plan for integration. Identify target sets and effects, by priority, for EW operations. Synchronize with information operations officer. See the following attachments as required: Tab C, D, E (Electromagnetic Warfare) to Appendix 12 (Cyberspace Electromagnetic Activities); Appendix 15 (Information Operations) to Annex C.*

(1) (U) Electromagnetic Attack. *Describe how electromagnetic attack activities are coordinated, integrated, synchronized, and support operations. See Tab C (Electromagnetic Attack) to Appendix 12 (Cyberspace Electromagnetic Activities).*

(2) (U) Electromagnetic Protection. *Describe how electromagnetic protection activities are coordinated, synchronized, and support operations. See Tab D (Electromagnetic Protection) to Appendix 12 (Cyberspace Electromagnetic Activities).*

(3) (U) Electromagnetic Support. *Describe how electromagnetic support activities are coordinated, synchronized, and support operations. See Tab E (Electromagnetic Support) to Appendix 12 (Cyberspace Electromagnetic Activities).*

d. (U) Scheme of Spectrum Management Operations. *Describe how spectrum management operations support the commander's intent and concept of operations. Outline the effects the commander wants to create while prioritizing spectrum management operations tasks. List the objectives and primary tasks to achieve those objectives. State the spectrum management, frequency assignment, host nation coordination, and policy implementation plan. See Annex H (Signal) as required.*

e. (U) Tasks to Subordinate Units. *List cyberspace and EW operations tasks assigned to each subordinate unit not contained in the base order.*

f. (U) Coordinating Instructions. *List cyberspace and EW operations instructions applicable to two or more subordinate units not covered in the base order. Identify and highlight any cyberspace and EW operations specific rules of engagement, risk reduction control measures, environmental considerations, coordination requirements between units, and commander's critical information requirements and critical information that pertain to CEMA.*

[page number]
[CLASSIFICATION]

Figure B-2. Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of an operation plan or order (continued)

[CLASSIFICATION]

4. (U) Sustainment. *Identify priorities of sustainment for cyberspace and EW operations key tasks and specify additional instructions as required. See Annex F (Sustainment) as required.*

a. (U) Logistics. *Use subparagraphs to identify priorities and specific instruction for logistics pertaining to cyberspace and EW operations. See Appendix 1 (Logistics) to Annex F (Sustainment) and Annex P (Host Nation Support) as required.*

b. (U) Personnel. *Use subparagraphs to identify priorities and specific instruction for human resources support pertaining to cyberspace and EW operations. See Appendix 2 (Personnel Services Support) to Annex F (Sustainment) as required.*

c. (U) Health System Support. *See Appendix 3 (Army Health System Support) to Annex F (Sustainment) as required.*

5. (U) Command and Signal.

a. (U) Command.

(1) (U) Location of Commander. *State the location of key cyberspace and EW operations leaders.*

(2) (U) Liaison Requirements. *State the cyberspace and EW operations liaison requirements not covered in the unit's SOPs.*

b. (U) Control.

(1) (U) Command Posts. *Describe the employment of cyberspace and EW operations specific command posts, including the location of each command post and its time of opening and closing.*

(2) (U) Reports. *List cyberspace and EW specific reports not covered in SOPs. See Annex R (Reports) as required.*

c. (U) Signal. *Address any cyberspace and EW specific communications requirements. See Annex H (Signal) as required.*

ACKNOWLEDGE: *Include only if attachment is distributed separately from the base order.*

[Commander's last name]

[Commander's rank]

The commander or authorized representative signs the original copy of the attachment. If the representative signs the original, add the phrase 'For the Commander.' The signed copy is the historical copy and remains in the headquarters' files.

OFFICIAL:

[Authenticator's name]

[Authenticator's position]

[page number]
[CLASSIFICATION]

Figure B-2. Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) of an operation plan or order (continued)

SECTION II – WORKING GROUPS

B-72. The CEWO and the CEMA section participate in several of the staff working groups. The CEWO is the staff lead for the CEMA working group (see chapter 4). Other working groups in which the CEMA section and CEWO participate include—

- Information collection working group.
- Targeting working group.

- Targeting coordination board.
- Protection working group.
- Assessment working group.

Note. During periods of high operating tempo, the chief of staff and the staff principals may combine working groups to synchronize efforts and increase efficiencies while minimizing requirements on the staff. Examples include combining the civil-military operations working group, information operations working group, and CEMA working group to streamline coordination prior to the targeting working group.

INFORMATION COLLECTION WORKING GROUP

B-73. The CEWO is a key participant in the information collection working group led by the G-2 or S-2. The working group develops and maintains the unit's information collection plan to ensure effective use of the unit's collection assets. During the information collection working group, the CEWO provides status of collection efforts against the collection plan and nominates information requirements and recommendations for EW elements to integrate into the collection plan.

B-74. The CEWO's inputs must address—

- The technical capabilities and limitations of available organic electromagnetic support assets.
- What electromagnetic support assets will be available and can be leveraged by phase of the operation.
- The primary, alternate, contingency, and emergency communication plan for information dissemination by asset.
- A rollup of the targets identified and processed since the last working group.
- Recommendations for potential collection efforts until the next working group.

B-75. The CEWO should be prepared to deconflict efforts with other collection assets to best suit the commander's collection priorities. The cyberspace and EW running estimate should include maintenance cycles for each EW system and set reasonable expectations for up and down times to the rest of the information collection working group.

B-76. Key inputs for the information collection working group include—

- Commander's guidance.
- Commander's critical information requirements.
- Future operations requirements.
- Subordinate unit requirements.
- Air tasking order nomination.

B-77. Key outputs of the information collection working group include—

- Priorities and recommendations for collection.
- An updated collection plan.
- Recommended changes to commander's critical information requirements.
- Input for fragmentary orders.

B-78. Table B-8 on page 133 shows an example of information collection working group activities and agenda at the division level. Refer to ATP 2-01 for more information about collection management.

Table B-8. Sample information collection working group activities

General Information	*Participants*
Title: Information collection working group. **Purpose:** Coordinate for, integrate, and synchronize information collection in support of the concept of operations. **Frequency:** Daily. **Duration:** One hour. **Location:** G-2 work area. **Medium:** Face-to-face; Defense Collaboration Service.	**Staff lead:** G-2. **Chair:** Chief of staff. **Members:** G-3 (current operations); G-3 (future operations); G-9; deputy fire support coordinator; air liaison officer; G-39; CEWO; staff judge advocate representative, liaison officers; and others as required.
Inputs and Outputs	***Agenda (Responsible Party)***
Inputs: Commander's guidance. CCIRs. Future operations requirements. Subordinate unit requirements. Targeting requirements. Air tasking order nomination. **Outputs:** Priorities and recommendations for collection. Updated information collection plan. Recommended changes to CCIRs. Fragmentary order input.	Roll call (G-2). Past information collection plan review (G-2). Weather update (staff weather officer). Intelligence update (G-2). Operations update (G-3). Future operations requirements (G-3). Subordinate unit requirements (G-3). Targeting requirements (targeting officer). Allocation of collection resources and assets availability (collection manager). Summary (G-2). Guidance (chief of staff).
Legend: CCIR commander's critical information requirement CEWO cyber electromagnetic warfare officer G-2 assistant chief of staff, intelligence G-3 assistant chief of staff, operations G-39 assistant chief of staff, information plans and operations G-9 assistant chief of staff, civil affairs operations	

TARGETING WORKING GROUP

B-79. The chief of fires (at the theater army), deputy fire support coordinator (at corps or division), or fire support officer (at brigade) leads the targeting working group. Members of the targeting working group perform the detailed staff work associated with targeting. Based on the commander's guidance and priorities, the targeting working group determines which targets to engage and how, where, and when to engage them. The staff then assigns friendly capabilities to locate and track targets and engage those targets to produce the desired effect on each target. Members present the results of their work to the commander at the targeting coordination board. The CEWO helps integrate cyberspace and EW operations in the Army targeting methodology to—

- **Decide**—providing a running estimate of high-priority target vulnerabilities in cyberspace and the electromagnetic spectrum and nominating targets based on their value in cyberspace or the electromagnetic spectrum.
- **Detect**—using electromagnetic support assets.
- **Deliver effects**—using electromagnetic attack or other fires capabilities.
- **Assess effects**—using electromagnetic support assets.

B-80. The CEWO must be prepared to provide technical guidance in the decide phase of the Army targeting methodology. As in the information collection working group, the CEWO briefs the capabilities and limitations of available organic and supporting non-organic EW assets and nominates potential detection assets moving into the detect phase. The CEWO provides continuing recommendations for the delivery of

electromagnetic attack or other fires capabilities that can effectively create desired effects according to the commander's high-payoff target list. The targeting working group must synchronize these effects with other information activities to maximize the commander's available detection and delivery capabilities.

B-81. Table B-9 on page 135 shows sample targeting working group activities at the division or corps level. The composition and activities of the targeting working group may require adjustment for the theater army or brigade combat team.

Table B-9. Sample targeting working group activities at division or corps

General Information	*Participants*
Purpose: Determine targets for planning and refinement based on priority within the operational environment. Match the appropriate asset required to create the desired effect on each target. Synchronize target nominations (lethal and nonlethal) across the staff and at echelon. **Frequency:** As needed. **Duration:** As needed (≤ 60 minutes). **Location:** Echelon headquarters. **Information/refinement cut-off time:** Refer to battle rhythm or SOP.	**Proponent:** Targeting officer or fire support officer. **Chair:** Fire support coordinator. **Key Attendees:** Fire support officer; air liaison officer; field artillery intelligence officer; G-2, G-3, G-4, G-5, and G-6 representatives; staff weather officer; CEWO; aviation officer; space officer; special operations liaison officer; staff judge advocate; operations research and systems analyst; engineer; support operations officer; liaison officers.
Inputs and Outputs	
Inputs: • Commander's targeting guidance and resource priorities. • Running estimates. • Last targeting cycle battle damage assessment and assessments. • Enemy event template. • Enemy situation. • Friendly situation and maneuver plan. • HPTL, named areas of interest, and target nominations.	**Outputs:** • Refined and updated HPTL. • Refined and updated named areas of interest. • Proposed information collection plan. • Recommended target nominations. • Recommended resource allocation.
Agenda	
• Roll call. • Current priority intelligence requirements. • Weather: 5-day forecast. • Air tasking order crosswalk. **Assess** • Review operational timeline. • Battle damage assessments. • Tasks to effect or review. • Decisions to be made. **Execution** • Enemy situation template updates. • HPTL crosswalk review and refinement. • Intelligence collection matrix review and refinement. • TSM review and refinement.	**Review and Validate** • Review targeting guidance. • Enemy situation template updates. • HPTL crosswalk review and refinement. • Intelligence collection matrix review and refinement. • TSM review and refinement. **Approval** • Enemy situation template assessment. • Proposed HPTL crosswalk. • Proposed intelligence collection matrix. • Proposed target nominations. • Proposed TSM. **Guidance** • Proposed targeting objectives. • Proposed HPTL. • Proposed collection priorities. • Proposed initial targeting effects requests.

Legend:

CEWO	cyber electromagnetic warfare officer	G-6	assistant chief of staff, signal
G-2	assistant chief of staff, intelligence	HPTL	high-payoff target list
G-3	assistant chief of staff, operations	SOP	standard operating procedure
G-4	assistant chief of staff, logistics	TSM	targeting synchronization matrix
G-5	assistant chief of staff, plans		

B-82. The CEWO's targeting, responsibilities include—

- Assisting the G-2 or S-2 with the electromagnetic attack and the electromagnetic support portions of intelligence preparation of the operational environment—identifying threat spectrum-dependent capabilities and targets.
- Briefing the electromagnetic attack plan.
- Recommending electromagnetic attack methods of target engagement and assisting the targeting working group in determining electromagnetic attack requirements against identified targets.
- Ensuring electromagnetic attack can create the desired effects.
- Planning and coordinating taskings and requests to satisfy electromagnetic attack and electromagnetic support requirements.
- Coordinating with SIGINT elements through the collection manager to satisfy electromagnetic support collection requirements (in the information collection working group).
- Recommending to the G-3 or S-3 and chief of fires, or fire support coordinator whether to engage a target with electromagnetic attack.
- Expediting joint spectrum interference resolution reports to the targeting working group and targeting coordination board.

TARGETING COORDINATION BOARD

B-83. The targeting coordination board is a formal meeting to gain the commander's decision on the recommendations of the targeting working group. The targeting coordination board follows the same agenda as the targeting working group and is chaired by the commander or designated representative. The targeting coordination board should be nested with the higher headquarters' targeting.

B-84. At the completion of the targeting coordination board, the approved targeting products are disseminated to subordinate units. The targeting products include—

- The approved high-payoff target list, attack guidance matrix, and target selection standards. These, with data from the information collection plan, may be combined into a unit-specific targeting synchronization matrix.
- Approved information collection plan. The G-2 or S-2 reorients acquisition assets and updates and disseminates the information collection plan.
- Tasks to subordinate units and assets. The G-3 or S-3 should prepare and issue a fragmentary order to subordinate elements to execute the planned attack and assessment of targets developed by the targeting working group and targeting coordination board.

PROTECTION WORKING GROUP

B-85. The chief of protection at echelons division and above leads the protection working group. At the brigade, the S-3 leads the protection working group. The protection working group uses information derived from the commander's guidance, intelligence preparation of the operational environment, targeting, risk management, warning orders, the critical and defended asset lists, and mission analysis to identify critical assets. The protection working group determines and prioritizes critical assets for protection. The CEWO provides—

- Input to the critical asset list and defended asset list.
- Subject matter expertise in threat cyberspace and EW capabilities.
- Subject matter expertise on cyberspace defense and electromagnetic protection measures and capabilities.

B-86. A critical output of the protection working group is an updated protection running estimate. Table B-10 on page 137 shows example protection working group activities. Refer to ADP 3-37 for more information about the protection working group.

Table B-10. Sample protection working group activities

Purpose and frequency	**Purpose:** • Determine likely threats and hazards. • Determine vulnerabilities. • Establish and recommend protection priorities. • Provide recommendations for the critical asset list and defended asset list. • Review and coordinate unit protection measures. • Recommend force protection conditions and random antiterrorism measures. • Make recommendations to commanders on protection issues that require a decision. • Perform tasks required for a force protection working group and a threat protection working group. • Assess assets and infrastructure that are designated as critical by higher headquarters. • Analyze and provide recommendations for the protection of civilians in the assigned area. • Develop and refine the protection running estimate. • Develop a scheme of protection, ensuring that it nests with the operational concept. • Establish the personnel recovery coordination center. • Develop personnel recovery guidance and isolated Soldier guidance. • Provide input and recommendations for cyberspace network protection. • Identify risks to the mission. **Frequency:** Every other day	
Inputs and outputs	**Inputs:** • Commander's guidance and intent. • Operation and warning orders. • Current scheme of protection. • Threat and hazard assessment. • Vulnerability assessment. • Criticality assessment. • Risk management. • Critical asset list. • Defended asset list.	**Outputs:** • Update protection assessment. • Scheme of protection. • Protection running estimate. • Protection prioritization list. • Recommended force protection condition. • Recommended EMCON condition. • Recommended protection guidance and mitigation measures. • Recommended changes to essential elements of friendly information. • Recommended changes to the critical asset list and defended asset list.
Legend: EMCON emission control		

ASSESSMENT WORKING GROUP

B-87. A key aspect of any operation is determining progress toward completing tasks, achieving objectives, and obtaining a desired end state. Commanders establish an assessment working group to assist them in identifying changes in an operational environment and determining whether actions are achieving objectives. While assessment occurs throughout the headquarters, including assessing current operations and conducting battle damage assessment, the assessment working group's focus is toward the mid- to long-range planning horizons. Products from the assessment working group serve as inputs to boards, other working groups, and planning teams as well as collated, synthesized, and refined information into a collective staff assessment for the commander (FM 6-0). The CEMA chief or CEWO is not a permanent member of the assessment working group but may participate as required.

This page intentionally left blank.

Appendix C

Effects Requests

This appendix discusses how Army units request external cyberspace operations and electromagnetic warfare support from higher echelon Army or joint forces. Army forces may require offensive cyberspace operations support for identified targets that require engagement using an offensive cyberspace capability. Defensive cyberspace operations support may be necessary when an identified threat in friendly cyberspace is beyond the defensive capabilities of local network defenders. Electromagnetic warfare support may be required when an Army unit needs augmentation, when their electromagnetic warfare capabilities or authorities cannot fulfill their mission requirements, or when the required support must be delivered by airborne electromagnetic warfare platforms.

SECTION I – ELECTROMAGNETIC ATTACK

C-1. Typically, Army units at echelons division and brigade combat team have the organic capabilities to conduct EW within their assigned areas. The joint force commander typically delegates electromagnetic attack control authority to subordinate commanders to conduct EW missions within their assigned areas. Commanders must ensure EW has been integrated and synchronized across the staff and according to the higher commander's attack guidance. Refer to ATP 3-12.3 for more information about electromagnetic attack control authority.

C-2. Units may require an EW capability not organically available or additional EW beyond their organic capabilities to meet requirements identified during targeting. The commander and the CEWO may request augmentation through a higher, adjacent, or lower headquarters to meet requirements. This section describes procedures for requesting airborne electromagnetic support through the DD Form 1972 (*Joint Tactical Airstrike Request*). It also discusses the use of the five-line electromagnetic attack request for immediate airborne electromagnetic attack support.

JOINT TACTICAL AIRSTRIKE REQUEST

C-3. In a joint environment, Army units can request an airborne electromagnetic attack or electromagnetic support. Airborne electromagnetic attack capabilities can prosecute both deliberate and dynamic targets. For deliberate targeting, the requesting unit submits the DD Form 1972, accompanied by an airborne electromagnetic attack or electromagnetic support request tool. Each of these requests has unique information requirements and request flows. The requesting unit's fire support element adds the target to its target nomination list. The target is also added to the joint integrated prioritized target list at the joint task force headquarters and forwarded to the joint force air component command with its assigned DD Form 1972 number (refer to ATP 3-09.32). Once the joint force air component command approves the Joint Tactical Air Strike Request, the request is forwarded to the air operations center to execute the attack.

C-4. Table C-1 on page 140 is an example of the request tool that accompanies the DD Form 1972 to request airborne electromagnetic attack or electromagnetic support capabilities.

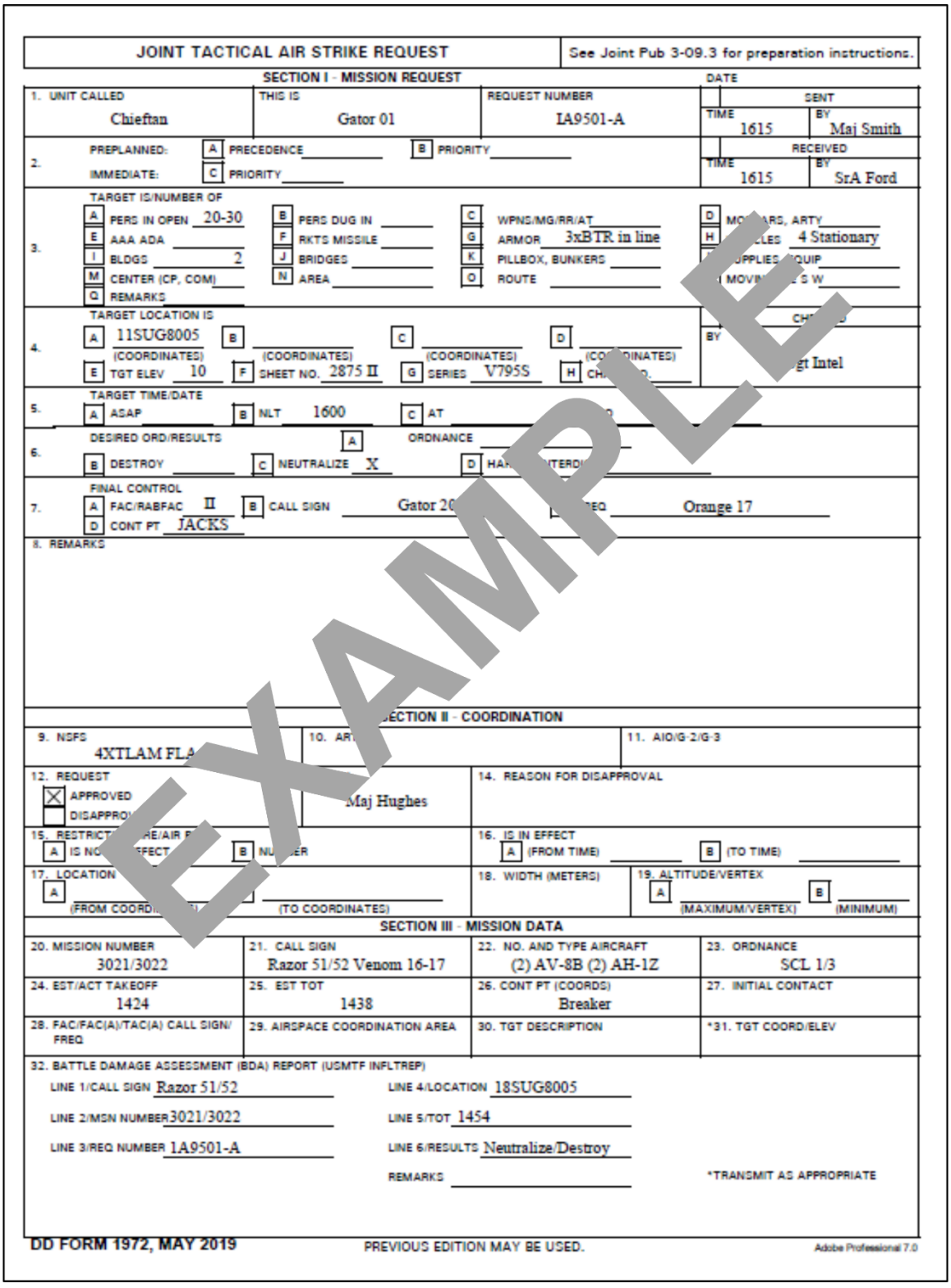
Table C-1. Example airborne electromagnetic attack or electromagnetic support request tool

Nonlethal Effect Discipline (Space, Airborne EA, Airborne ES, or cyber)	Applic-able phase or find, fix, track, target, engage, and assess	Non-lethal Effect	***Risk***			Approval timeline	Employ-ment timeline (initial access to effect ready to fire)	Auth. Level (for use in AOR)	Execution authority (tactical employ-ment)
			Tech. gain/ loss	Intel gain/ loss	Cdr's acceptable level of risk				
---	---	---	---	---	---	---	---	---	---
Airborne EA	Target	Jam	Gain	Gain	Acceptable	180 minutes	180 minutes	Local	Local
---	---	---	---	---	---	---	---	---	---

Legend:

AOR	area of responsibility	ES	electromagnetic support
Auth	authorization	Intel	intelligence
EA	electromagnetic attack	Tech.	technical
Cdr	commander		

C-5. Figure C-1 on page 141 illustrates an example joint tactical airstrike request.



JOINT TACTICAL AIR STRIKE REQUEST

See Joint Pub 3-09.3 for preparation instructions.

SECTION I - MISSION REQUEST

1. UNIT CALLED: Chieftan | THIS IS: Gator 01 | REQUEST NUMBER: IA9501-A | DATE SENT: TIME 1615 BY Maj Smith

2. PREPLANNED: [A] PRECEDENCE ____ [B] PRIORITY ____ IMMEDIATE: [C] PRIORITY ____ | DATE RECEIVED: TIME 1615 BY SrA Ford

3. TARGET IS/NUMBER OF
[A] PERS IN OPEN 20-30 [B] PERS DUG IN ____ [C] WPNS/MG/RR/AT ____ [D] MOR/ARS, ARTY ____
[E] AAA ADA ____ [F] RKTS MISSILE ____ [G] ARMOR 3xBTR in line [H] VEHICLES 4 Stationary
[I] BLDGS 2 [J] BRIDGES ____ [K] PILLBOX, BUNKERS ____ [L] SUPPLIES/EQUIP ____
[M] CENTER (CP, COM) ____ [N] AREA ____ [O] ROUTE ____ [P] MOVING VEHICLES W ____
[Q] REMARKS ____

4. TARGET LOCATION IS
[A] 11SUG8005 (COORDINATES) [B] ____ (COORDINATES) [C] ____ (COORDINATES) [D] ____ (COORDINATES)
[E] TGT ELEV 10 [F] SHEET NO. 2875 II [G] SERIES V795S [H] CHART NO. ____
CHECKED BY ____ Intel

5. TARGET TIME/DATE
[A] ASAP ____ [B] NLT 1600 [C] AT ____

6. DESIRED ORD/RESULTS
[A] ORDNANCE ____
[B] DESTROY ____ [C] NEUTRALIZE X [D] HARASS/INTERDICT ____

7. FINAL CONTROL
[A] FAC/RABFAC II [B] CALL SIGN Gator 20 [C] FREQ Orange 17
[D] CONT PT JACKS

8. REMARKS

SECTION II - COORDINATION

9. NSFS 4XTLAM FLA | 10. ARTY ____ | 11. AIO/G-2/G-3

12. REQUEST [X] APPROVED [ ] DISAPPROVED Maj Hughes | 14. REASON FOR DISAPPROVAL

15. RESTRICTIVE FIRE/AIR [A] IS NOW IN EFFECT [B] NUMBER | 16. IS IN EFFECT [A] (FROM TIME) ____ [B] (TO TIME) ____

17. LOCATION [A] (FROM COORDINATES) ____ (TO COORDINATES) | 18. WIDTH (METERS) | 19. ALTITUDE/VERTEX [A] (MAXIMUM/VERTEX) ____ [B] (MINIMUM) ____

SECTION III - MISSION DATA

20. MISSION NUMBER	21. CALL SIGN	22. NO. AND TYPE AIRCRAFT	23. ORDNANCE
3021/3022	Razor 51/52 Venom 16-17	(2) AV-8B (2) AH-1Z	SCL 1/3
24. EST/ACT TAKEOFF	25. EST TOT	26. CONT PT (COORDS)	27. INITIAL CONTACT
1424	1438	Breaker	
28. FAC/FAC(A)/TAC(A) CALL SIGN/ FREQ	29. AIRSPACE COORDINATION AREA	30. TGT DESCRIPTION	*31. TGT COORD/ELEV

32. BATTLE DAMAGE ASSESSMENT (BDA) REPORT (USMTF INFLTREP)

LINE 1/CALL SIGN Razor 51/52 | LINE 4/LOCATION 18SUG8005
LINE 2/MSN NUMBER 3021/3022 | LINE 5/TOT 1454
LINE 3/REQ NUMBER 1A9501-A | LINE 6/RESULTS Neutralize/Destroy
REMARKS ____

*TRANSMIT AS APPROPRIATE

DD FORM 1972, MAY 2019 PREVIOUS EDITION MAY BE USED. Adobe Professional 7.0

EXAMPLE

Figure C-1. Example joint tactical airstrike request

ELECTROMAGNETIC ATTACK REQUEST FORMAT

C-6. Dynamic targeting is used to prosecute targets of opportunity, including both unscheduled targets and unanticipated targets. Immediate airborne electromagnetic attack may be required, for example, when a maneuver plan needs enemy communications or sensors jammed before engagement. A unit can request immediate support using the five-line electromagnetic attack request.

C-7. Electromagnetic attack requests fall within three operational categories: preplanned, preplanned on-call, and immediate. The CEWO enters requests for electromagnetic attack effects through the targeting working group using the electromagnetic attack request format (see table C-1 on page 140). Requests for preplanned electromagnetic attack support are similar to requests for close air support. Requests for electromagnetic attack effects use DD Form 1972 (see paragraph C-3) with detailed electromagnetic attack effects requests attached in an electromagnetic attack request format.

C-8. The joint task force headquarters, the joint force land component command, the joint force air component command, and the air operations center must collaboratively plan airborne attack before an operation. This planning and coordination provide the joint force air component command the necessary time to identify and prepare an EW squadron that will remain on standby throughout the mission or operation. Figure C-2 depicts an example electromagnetic attack request format.

Requesting command:	
Requesting Unit:	
Contact Information: *This person will be responsible for verifying the approved request before the mission starts and relaying the information to the executing unit*.	
Joint Tactical Air Strike Request Number: *Enter the joint tactical air strike request number for submission with the electromagnetic attack request format*.	
Concept of Operations: *Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to objectives for the integrated tasking order*.	
Electromagnetic Attack Concept of Operations: *Define the desired effect(s) and timeline*.	
CEASE BUZZER Procedures: *This will be in accordance with theater special instructions. Provide frequency to communicate between the electromagnetic attack control authority and the electromagnetic attack asset. VHF and UHF are the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be internet relay chat capable*.	
Friendly Frequency Use for Operation:	
Target Communications System(s) to be Jammed or Denied:	Target requested—*list the type and frequency, if known*. Intelligence assessment (*required—do not copy and paste frequencies from one day to the next without intelligence validation assessment*). Target location in latitude and longitude or military grid reference system.
Jamming Date-Time Group(s): *From and to, in Zulu time (preferred).*	
Type of Electromagnetic Attack Requested: *Preplanned and scheduled; on-call*.	
Legend: VHF very high frequency UHF ultrahigh frequency	

Figure C-2. Example electromagnetic attack request format

C-9. Units may submit requests for immediate or on-call electromagnetic attack using the electromagnetic attack brief (figure C-3 on page 143) for electromagnetic attack support when pre-planning is not possible

due to dynamic or emergent requirements. The electromagnetic attack brief prepares the aircrew providing the electromagnetic attack support (refer to ATP 3-09.32).

Electromagnetic Attack Brief

Do not transmit line numbers. Units of measure are standard unless briefed.

Lines 1, 2, and 3 are mandatory readback (*). The JTAC may request additional readback.

1. EACA: * Foxfire 06 (aircraft call sign), this is Forward 09 (JTAC call sign)
2. Target or effect description: * Disrupt
   a. Rapper or target name radio transmitter
   b. Frequency (if known) 107.1 MHz
   c. Modulation FM
3. Target location: N 46° 47’ 33.1978” / W 120° 9’ 47.2332”
4. Remarks: No current remarks or special instructions

EXAMPLE

Legend:

EACA	electromagnetic attack control authority	MHz	megahertz
FM	frequency modulation	N	north
JTAC	joint terminal attack controller	W	west
MGRS	Military Grid Reference System		

Figure C-3. Example electromagnetic attack brief

SECTION II – CYBERSPACE EFFECTS

REQUESTING OFFENSIVE CYBERSPACE OPERATIONS SUPPORT

C-10. For offensive cyberspace operations missions, the CEMA working group nominates high-payoff targets that have met the commanders’ targeting guidance in the targeting working group. Once approved, the targeting working group adds these targets to the unit’s target selection standards, targeting synchronization matrix, and attack guidance matrix. The CEMA working group will also make recommendations to the no-strike list and restricted target list that support the commanders targeting guidance.

C-11. Combat mission teams provide offensive cyberspace capabilities to units at echelons corps and below through the request for service process. Upon the commander’s approval, the CEMA section submits a CERF, along with the high-payoff target list, no-strike list, and restricted target list, to their higher headquarters as nominations for the joint targeting cycle and joint no-strike list or restricted target list.

C-12. The joint task force headquarters or combatant command uses the information from the CERF to generate a USCYBERCOM request for service. Once the joint task force or combatant command headquarters approves cyberspace targets identified in the corps’ high-payoff target list, they will add them to the joint targeting cycle. The joint task force or combatant command then continues the request for service process to request offensive cyberspace support from Joint Force Headquarters-Cyber (see figure C-4 on page 144).

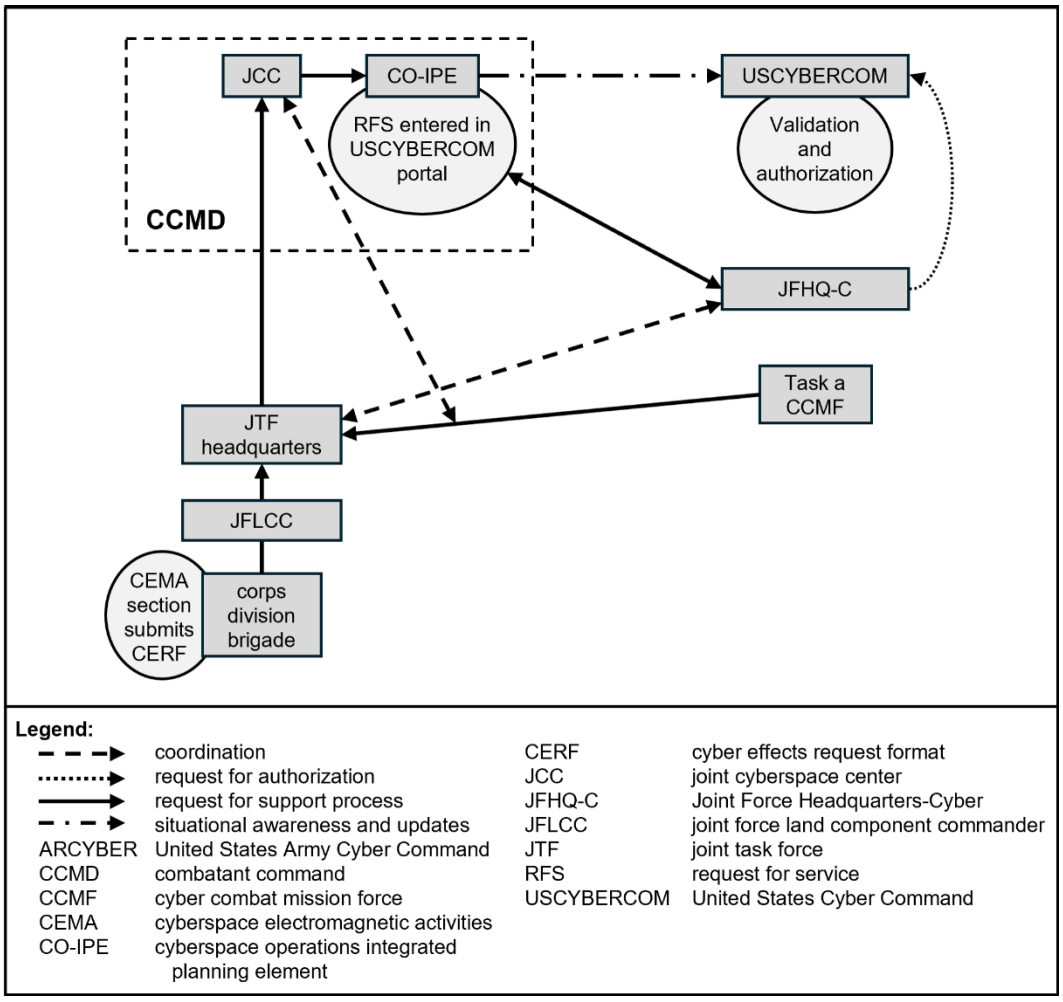


Figure C-4. Routing chain for offensive cyberspace operations support requests

REQUESTING DEFENSIVE CYBERSPACE OPERATIONS SUPPORT

C-13. Defensive cyberspace operations support may be required to counter threat malicious cyberspace activities that are beyond the capabilities of local network defenders and cybersecurity personnel to mitigate. Units at echelons corps and below have limited organic capabilities to perform defensive cyberspace operations tasks. Units request defensive cyberspace operations support as a reactive measure to defend against malicious cyberspace activity through the CERF and request for service. The G-6 or S-6 coordinates with the G-3 or S-3 to develop a CERF to request defensive cyberspace operations support.

C-14. Upon the commander's approval, the CERF is submitted, validated, and routed through higher headquarters, until it reaches the joint task force or combatant command, where it is converted to a request for service. In parallel, the requesting unit notifies a cybersecurity service provider (Defense Information Systems Agency or NETCOM) of the malicious cyberspace activity.

C-15. The joint task force headquarters or combatant command routes the request for service; the cybersecurity service provider also notifies DOD Cyber Defense Command of the identified malicious cyberspace activity. The combatant command has assigned cyber protection teams to defend friendly cyberspace. The combatant commander has the authority to conduct defensive cyberspace operations missions within their assigned area of responsibility without requesting authorization from USCYBERCOM.

C-16. The cyber protection teams' primary focus is conducting cyberspace defense throughout the area of responsibility and may be unavailable to provide support to requesting units at echelons corps and below. If

the cyber protection teams are unavailable, the combatant command joint cyberspace center forwards the request for service through the cyberspace operations-integrated planning element to DOD Cyber Defense Command through the USCYBERCOM portal. The cyberspace operations-integrated planning element provides USCYBERCOM situational understanding of all defensive cyberspace operations missions conducted in a combatant commander's area of responsibility.

C-17. When local network defenders become aware of malicious activity on the network, they forward the information to DOD Cyber Defense Command. DOD Cyber Defense Command uses the notice from the local network defenders to begin the process of employing a cyber protection team (either joint or Service-retained) before receiving the request for service through the routing channels. However, the requesting unit is still responsible for both initiating the request for service process and informing a cybersecurity service provider.

C-18. DOD Cyber Defense Command has directive authority for cyberspace operations to conduct defensive cyberspace operations globally within the DODIN. DOD Cyber Defense Command provides USCYBERCOM situational understanding information for all defensive cyberspace operations missions.

C-19. DOD Cyber Defense Command exercises tactical control of all Service cyberspace component commands for DODIN operations and defensive cyberspace operations. DOD Cyber Defense Command has assigned cyber protection teams that conduct defensive cyberspace operations; however, their primary focus is generally monitoring and implementing proactive internal defensive measures to mitigate malicious cyberspace activity on the DODIN globally.

C-20. Initiating cyberspace defense to respond to malicious cyberspace activity uses a top-down approach. Proactive cyberspace defense occurs when DOD Cyber Defense Command identifies malicious activity on the DODIN before receiving a request for service or being informed by a cybersecurity service provider and proactively deploys a cyber protection team to counter malicious cyberspace activity.

C-21. If the DOD Cyber Defense Command cyber protection teams are unavailable to satisfy the request for service, DOD Cyber Defense Command oversees a joint approval process to task one of the Service cyberspace component commands to provide a cyber protection team to conduct cyberspace defense to support the unit's request. The assigned cyber protection team may perform defensive tasks remotely or co-locate with the joint task force headquarters or requesting unit. When co-located with the unit, the cyber protection team remains under the command of its parent unit. Figure C-5 on page 146 illustrates the routing chain for defensive cyberspace operations support requests for echelons corps and below.

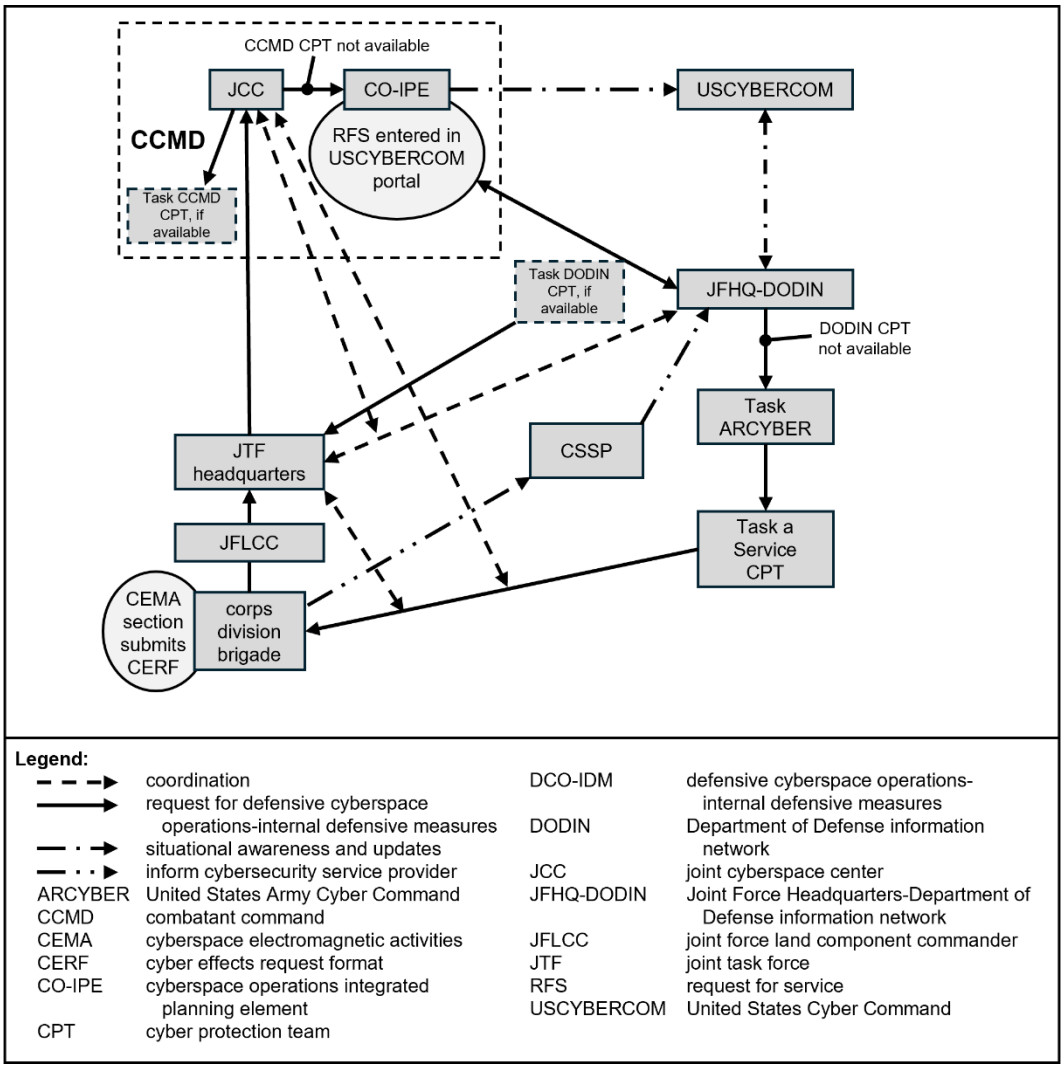


Figure C-5. Routing chain for defensive cyberspace operations support requests

CYBER EFFECTS REQUEST FORMAT

C-22. Corps and below Army units use the CERF to request cyberspace operations support. Support in response to a CERF may come from joint cyberspace forces such as the combat mission teams or from joint or other Service capabilities.

C-23. During the operations process at echelons corps and below, the commander and staff identify the effects desired in and through cyberspace to support operations against specified targets. If the requesting and higher echelons determine their current capabilities are insufficient, the commander and staff validate and process the CERF. The routing process continues through each echelon until the CERF reaches the joint task force or combatant command, where it is converted to a USCYBERCOM request for service.

APPROVAL PROCESS

C-24. The CERF approval process at echelons corps and below follows the below steps:

- Identify targets for cyberspace effects.
- Determine whether organic cyberspace capabilities can create desired effects.
- Validate target for cyberspace effects.
- Forward to the next higher Army echelon for deconfliction and synchronization.

- Determine whether other organic capabilities can create desired effects if organic cyberspace capabilities do not exist.
- If current capabilities can fulfill the requirement, synchronize operations.
- If current capabilities cannot fulfill the requirement, approve target for cyberspace effects.
- Forward to next higher Army echelon for approval until the CERF enters the joint process as a USCYBERCOM request for service.
- Synchronize the operation with the requested cyberspace effect (if possible).

PREPARATION

C-25. Although the requesting unit may not have detailed target network topology information, it should provide as much current target information as available. The approval process for cyberspace effects may take longer than other fires capabilities. Each of the three sections in the CERF are described below in bullet form. The requesting unit provides all information from the bullet lists below to their higher headquarters through the CEMA working group or other designated targeting processes.

Section 1 – Requesting Unit Information

C-26. The requesting unit provides the following identifying information in section 1:

- **SUPPORTED MAJOR COMMAND.** Enter the major command authorized to validate and prioritize the CERF. For Army units at echelons corps and below, this entry will usually be the combatant command.
- **DATE SENT.** Enter the date the requesting unit submitted the CERF to the next higher headquarters.
- **TIME SENT.** Enter the time the requesting united submitted the CERF to higher headquarters.
- **REQUESTING UNIT.** Enter the name of the requesting unit.
- **BY.** Enter the rank, last, and first name of the requesting unit's point of contact that time-stamped and processed the CERF.
- **CLASSIFICATION.** Enter the overall classification of the document. Ensure classification markings are applied to each section and all supporting documents.
- **POINT OF CONTACT.** Enter the rank, last, and first name of the requesting unit's point of contact. Also, enter the phone number and e-mail address.
- **REQUEST FOR SERVICE NUMBER.** Leave blank. The request for service number is assigned by the joint task force or combatant command headquarters when the CERF is converted to a request for service for forwarding to USCYBERCOM.

Section 2 – Supported Operation Information

C-27. The requesting unit provides the following information about the supported operation in section 2:

- **SUPPORTED OPLAN/CONPLAN/ORDER.** Describe key details within the plan the requested cyberspace attack will support.
- **SUPPORTED MISSION STATEMENT.** Describe the unit's essential task or tasks and the purpose the requested effect will support.
- **SUPPORTED COMMANDER'S INTENT.** Describe key information within the commander's intent the requested effect will support.
- **SUPPORTED COMMANDER'S END STATE.** Describe key information within the commander's end state the requested effect will support.
- **SUPPORTED CONCEPT OF OPERATIONS.** Describe key information within the concept of operations the requested effect will support.
- **TASK, PURPOSE, METHOD, END STATE.** Describe the supported objective or objectives the requested effect will directly support. Describe the tactical objectives and tasks the requested effect will directly or indirectly support. Describe the supported objective or objectives the requested effect will directly support.
- **SUPPORTED UNIT POINT OF CONTACT.** Provide contact information for the supported unit (or requesting unit if they are the same).
- **CERF TRACKING NUMBER.**

- **REVISION NUMBER.**
- **TARGET LIST NUMBER.**
- **BASIC ENCYCLOPEDIA NUMBER.**
- **RELATED REQUESTS FOR INFORMATION.**
- **REMARKS.**

Section 3 – Target Specified Information

C-28. The requesting unit provides the following information about the specified target in section 3:

- **TYPE OF TARGET.**
  - Facility.
  - Individual.
  - Virtual.
  - Equipment.
  - Organization.
- **TARGET PRIORITY.**
  - Emergency.
  - Priority.
  - Routine.
- **TARGET DESCRIPTION.**
- **TARGET FUNCTION.**
- **TARGET LOCATION.**
- **DESIRED EFFECT.**
- **TARGET SIGNIFICANCE.**
- **TARGET DETAILS.**
- **CONCEPT OF OPERATIONS.**
- **TARGET EXPECTATION STATEMENT.**

Remarks

C-29. The following information is required in the remarks section:

- Time of target and duration of effect.
- No earlier than and no later than time.
- Trigger event or conditions for effect.
- Persistence requirement.

C-30. The following information is optional in the remarks section:

- Command and control requirements.
- Self-destruct or auto delete requirement.
- Level of attribution requirement.
- Level of detectability allowed.
- Level of co-optability allowed.
- Remote monitoring requirement.
- Reversibility requirement.

Appendix D

Recognizing and Responding to Electromagnetic Attacks and Malicious Cyberspace Activity

This appendix addresses the means to recognize and overcome threat electromagnetic attacks and malicious cyberspace activity in a contested environment. It includes an overview of peer threat tactics, techniques, and procedures and methods to prevent, identify, and react to threat electromagnetic attacks and malicious cyberspace activity.

SECTION I – THREAT TACTICS, TECHNIQUES, AND PROCEDURES

D-1. A peer threat's information warfare activities will integrate computer warfare (malicious cyberspace activity) electromagnetic attack, military deception, lethal fires, perception management, and information attack to deny U.S. and allied forces access to cyberspace and the electromagnetic spectrum in a contested environment.

D-2. Understanding threat capabilities in cyberspace and the electromagnetic spectrum is key to sound plans. Enemy attacks on friendly command and control nodes may combine electromagnetic attacks, other information warfare effects, and lethal fires to deny friendly forces the use of spectrum-dependent devices. To accomplish this goal, enemy forces gather technical and combat information about friendly forces capabilities. As enemy forces locate and identify friendly units, enemy information warfare elements establish priorities to—

- Jam communications assets.
- Deceptively enter radio networks.
- Interfere with the normal flow of U.S. and allies' communications.

MEASURES TO PREVENT THREAT EFFECTS

D-3. Understanding threat capabilities is critical to hardening the deployed network against enemy cyberspace, EW, and SIGINT activities. If an enemy cannot detect command posts and communications systems, it cannot target the capabilities with malicious cyberspace activity, electromagnetic attack, or lethal fires.

LIMITING ELECTROMAGNETIC SIGNATURES

D-4. To protect against a peer threat's ability to locate and target radio signals, the G-6 or S-6 must plan signal support in a way that limits the electromagnetic signature of command posts, other communications sites, and maneuver formations. Measures to reduce electromagnetic signatures include—

- Careful positioning of radio equipment.
- Employment of directional antennas.
- Operation using minimum power required to communicate.
- Limiting radio transmissions.
- Using a random schedule.
- Emission control.
- Selective radio silence.

D-5. Electromagnetic protection actions can also help mask electromagnetic signatures. The CEWO can assist the G-6 or S-6 in planning electromagnetic protection to reduce electromagnetic signatures.

Terrain Masking

D-6. Terrain masking can effectively block radio signals from reaching enemy direction finding capabilities. Positioning communications systems with large terrain features or manmade structures between the communications system and the forward line of own troops effectively blocks an enemy from detecting the

signal. Careful route selection may be able to take advantage of natural and manmade terrain to mask electromagnetic signatures from enemy sensors on a convoy or movement to contact.

Camouflage Net Masking

D-7. Radar reflective camouflage netting is an effective means of blocking stray electromagnetic radiation from directional antennas. Camouflage netting placed to the sides and back of a line of sight or satellite communications antenna ensures only the main beam of the antenna radiates. Since the main beam is directional, it is much harder for the enemy to detect; the enemy would need to be directly in the transmission path. Planners consider minimum safe distance from transmitters to prevent electromagnetic interference and mitigate hazards of electromagnetic radiation to personnel.

Line of Sight

D-8. High-throughput line of sight radios can carry high bandwidth data over distances up to 40 kilometers (25 miles) when unobstructed by terrain or manmade structures. Planners should engineer links to minimize chances of detection, targeting, and jamming. If the line of sight path is parallel to the forward line of own troops, an enemy is less likely to detect the signal, and enemy jammers cannot reach the antenna with a strong enough signal to jam the radio.

Satellite Site Selection and Radio Frequency Interference

D-9. Satellite communications systems may suffer from natural and manmade interference. Natural sources of interference include solar activity, dense vegetation, thick cloud cover, heavy precipitation, and sandstorms. Manmade sources of interference include vehicles, buildings and other structures that obstruct the line of sight path to the satellite, electromagnetic jamming, and radio frequency interference.

D-10. Commanders and staffs need to identify and minimize the command post footprint and electromagnetic signature. Planners and operators should identify physical surroundings to minimize interference and mask the electromagnetic signatures of deployed communications systems. See chapter 1 for more information about electromagnetic interference.

D-11. Signal elements operating from locations without masking terrain features or structures can use power settings and radio frequency management techniques to control interference and avoid detection. When establishing satellite communications links, the equipment operator should communicate with satellite network controllers to determine the minimum required power level. The possibility of interference, detection, and signal jamming increases as output power increases. Refer to ATP 6-02.53 and ATP 3-12.3 for more information about terrain masking and low power settings.

Remote Antennas

D-12. Large command posts and high-throughput communications systems emit significant electromagnetic energy. While planners and operators can mask some of this energy with directional antennas, site selection, and terrain masking techniques, some detectable energy remains. Because command and control capabilities are a priority target for peer threats, anything near the communications system is at risk of destruction from lethal fires.

D-13. Commanders and planners should consider locating major communications assemblages as far from the supported command post as practical. Selecting a site with terrain features, manmade structures, or distance between communications systems and command posts protects the command post from lethal fires. Commanders and planners must consider the additional physical security and site defense requirements for a remote site during planning.

Frequent Command Post Dislocation

D-14. Despite efforts to reduce and mask the electromagnetic signature of a command post, a peer threat may eventually locate it. Moving a command post frequently reduces its chance of destruction. This is especially important when operating within the range of enemy artillery. Peer threats can mass lethal fires to destroy an area target quickly.

D-15. Maintaining continuity during displacement of a command post or catastrophic loss requires designating alternate command posts and passing control between command posts. During training exercises, units must practice frequent command post dislocation and handoff between the main and tactical command posts.

SECTION II – RECOGNIZING AND RESPONDING TO THREAT EFFECTS

D-16. Because peer threats consider friendly command and control capabilities to be high priority targets, they have developed capabilities to deny friendly use of the electromagnetic spectrum for communications. Signal Soldiers and leaders must learn to identify and respond to threat effects in cyberspace and the electromagnetic spectrum.

ELECTROMAGNETIC JAMMING

D-17. Electromagnetic jamming is an effective way for the enemy to disrupt friendly communications. An enemy only needs a transmitter tuned to a U.S. frequency with enough power to overpower friendly signals to effectively jam U.S. systems.

D-18. Jammers operate against receivers, not transmitters. The two modes of jamming are spot and barrage jamming. Spot jamming concentrates power on one channel or frequency. Barrage jamming is power spread over several frequencies or channels at the same time. It is important to recognize jamming, but it can be difficult to detect. Refer to ATP 3-12.3 and ATP 6-02.53 for more information about electromagnetic jamming.

COMMUNICATIONS JAMMING

D-19. Radio operators must learn to recognize and react to electromagnetic jamming. This is not always an easy task, since electromagnetic interference can be either internal or external. Other sources having nothing to do with enemy jamming may cause electromagnetic interference. Unintentional electromagnetic interference may be caused by one or more of—

- Other radios (friendly and enemy).
- Other electronic, electrical, or electromechanical equipment.
- Space weather phenomena.
- Atmospheric conditions.
- Equipment malfunction.

D-20. Radio operators must train to differentiate internal and external interference quickly. Refer to ATP 6-02.53 for more information about isolating and eliminating internal sources of interference.

D-21. Electromagnetic jamming most commonly affects single-channel radio systems. These radios include high frequency (HF), very high frequency (VHF), and ultrahigh frequency (UHF) radios. Jamming effects may be obvious or subtle. Obvious jamming is normally simple to detect. When experiencing jamming, it is more important to recognize and overcome the incident than to identify it formally.

D-22. Subtle jamming is less obvious because subtle jamming signals produce no sound from the receivers. Although everything may appear normal to the radio operator, the receiver cannot receive an incoming friendly signal. Often, users assume their radios are malfunctioning instead of recognizing subtle jamming. Table D-1 on page 152 lists some common jamming signals.

Table D-1. Common jamming signals

Signal	*Description*
Random Noise	Synthetic radio noise. It is indiscriminate in amplitude and frequency. It is similar to normal background noise and can degrade all types of signals. Operators often mistake random noise jamming for receiver or atmospheric noise and fail to take appropriate electromagnetic protection actions.
Stepped Tones	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are effective against single-channel amplitude modulation or frequency modulation voice circuits.
Spark	Bursts are of short duration and high intensity; they are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications. Spark jamming is easy to produce and one of the most effective jamming signals.
Gulls	Quickly rising and slowly falling variable radio frequency. The effect produced is similar to the cry of a seagull. Gulls produce a nuisance effect and are very effective against voice radio communications.
Random Pulse	Pulses of varying amplitude, duration, and rate. Pulses disrupt teletypewriter, radar, and various data transmission systems.
Wobbler	A single frequency, modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.
Recorded Sounds	Any audible sound, especially of a variable nature. Recorded sounds can distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.
Preamble Jamming	A tone resembling the synchronization preamble of the speech security equipment broadcast over the operating frequency of secure radio sets. Results in all radios being locked in the receive mode. Preamble jamming is especially effective when employed against radio networks that use speech security devices.

Preventive Measures

D-23. Measures operators and planners can use to reduce susceptibility to enemy jamming include—

- Minimize radio transmissions—try to keep radio transmissions to six seconds or less.
- Use anti-jam techniques, such as frequency hopping.
- Train for operation using radio silence.
- Use low power setting on radios for normal operation to reduce the probability of detection.
- Use terrain masking to reduce the probability of detection and block potential sources of enemy jamming.

Indicators

D-24. The enemy strives to perfect and use new and more confusing forms of jamming, which requires radio operators to be increasingly alert to the possibility of jamming. Training and experience allow operators to determine whether a particular signal is a jamming signal. During operations, radio operators should remain alert to possible jamming indicators. Observable indications of jamming include—

- Apparently random noise or static over voice channels.
- Recorded sounds—messages or music—over voice channels.
- No answer to a radio transmission.

Reaction

D-25. Communications jamming requires prompt corrective action to restore critical communications capabilities. Possible reactions to jamming include—

- **Continuing to operate**. Enemy jamming usually involves a period of jamming followed by a brief listening period. Operator activity during this short period indicates to enemies whether their jamming efforts were successful. Continuing to operate normally gives the enemy no indication of success for failure. If the enemy hears discussion of the problem on the air, or radio operation

terminates, the enemy may assume their jamming was effective. Operators should never terminate operation of a radio network unless ordered to do so. Operators should be careful not to disclose adverse effects of enemy jamming. This means normal operations should continue even when degraded by jamming.

- **Increasing transmitter power output.** Using low power for normal operation minimizes the chance of detection. Once the enemy begins jamming radios, the risk of detection becomes secondary to the radio delivering required communications. Higher radio power may overcome the enemy's jamming signal, but it also increases the risk of location by enemy direction-finding capabilities.
- **Improving the signal-to-jamming ratio.** The signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. If the desired signal is much stronger than the jamming signal, the jamming does not significantly degrade communications. To improve the signal-to-jamming ratio operators and signal leaders can consider—
  - **Adjusting or changing the antenna.** When jamming occurs, the radio operator should adjust the antenna to receive the maximum incoming signal strength. Depending on the antenna, some methods include reorienting the antenna, changing antenna polarization at all stations, or installing an antenna with a greater range.
  - **Establishing a retransmission site.** A retransmission site can increase the effective range and power of a signal between radio stations without increasing transmit power.
  - **Relocating the antenna.** Operators may use terrain masking to block the incoming jamming signal. This may require relocating the antenna and associated radio set up to several hundred meters from its previous location.
- **Changing frequencies.** If a communications network cannot overcome enemy jamming, the commander may direct use of an alternate or spare frequency. Preplanned and well-coordinated actions are required for practical dummy stations to continue to operate on the jammed frequency, to mask the change to an alternate frequency. During a jamming incident, it may be difficult to coordinate a frequency change. All radio operators require knowledge of when, and under what circumstances, they should switch to a backup frequency. If the frequency change is not smooth, the enemy may discover what is happening and try to degrade communications on the new frequency.
- **Executing the primary, alternate, contingency, and emergency communication plan.** Quickly changing to the alternate or contingency means of communication reduces the disruption of the command and control system.
- **Using electromagnetic support or SIGINT or capabilities to locate the jamming signal.** Leveraging EW or SIGINT capabilities requires coordination and collaboration between the CEMA section and the G-2 or S-2.

D-26. If none of the corrective actions mitigate the enemy jamming, operators should continue operation of the network and submit a meaconing, intrusion, jamming, and interference feeder (MIJIFEEDER) report to higher headquarters. If the higher headquarters cannot resolve the interference, they should initiate joint spectrum interference resolution reporting. Joint spectrum interference resolution reports document a historical record of problems and help identify possible causes for subsequent interference. Maintaining a historical record of interference helps develop countermeasures for future jamming incidents. See appendix E for the MIJIFEEDER report format. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting.

Note. Joint spectrum interference resolution is not implemented on a tactically-relevant timeline and requires SIPRNET access to submit reports.

POSITIONING, NAVIGATION, AND TIMING JAMMING

D-27. Peer threats have capabilities to contest the space domain and attack the on-orbit, link, and terrestrial segments of U.S. positioning, navigation, and timing satellites. These attacks may have significant impacts across all warfighting functions and many weapon platforms.

D-28. Electromagnetic jamming of positioning, navigation, and timing satellite capabilities affects not only communications, but also many other capabilities in tactical formations. Systems affected include—

- Communications systems.
- Friendly force tracking.
- Navigation.
- Reconnaissance.
- Radar systems.
- Precision guided munitions.

Preventive Measures

D-29. Measures to reduce susceptibility to and mitigate the effects of enemy jamming of positioning, navigation, and timing include—

- Using only encrypted positioning, navigation, and timing systems.
- Antenna masking.
- Terrain masking.
- Training and maintaining the ability to navigate using a map and compass.

Indicators

D-30. User indications that an enemy may be jamming positioning, navigation, and timing satellites include—

- Loss of satellite signal.
- Red Global Positioning System icon on the network management system.
- Loss of timing or incorrect time displayed on equipment.
- Incorrect location displayed on the map.
- Jamming environment warning message.

Reaction

D-31. Because of the diverse and widespread effects of enemy positioning, navigation, and timing jamming, a prompt, coordinated response is necessary. Operators of all affected systems should—

- **Navigate using map and compass.** While this does not restore system timing and situational awareness displays, navigation using a map and compass cannot be jammed.
- **Increase distance between affected systems and jammer.** If the jammer operates from a known location, increased distance or terrain masking may mitigate interference.
- **Use electromagnetic support or SIGINT capabilities to locate the jamming signal.** Leveraging EW or SIGINT capabilities requires coordination and collaboration between the CEMA section and the G-2 or S-2.
- **Report jamming to higher headquarters.** Submitting a joint spectrum interference resolution report to higher headquarters documents a history of problems and helps identify possible causes for subsequent interference.

RADAR JAMMING

D-32. U.S. radar systems are subject to jamming. Radar system operators must learn to recognize indications of jamming and respond appropriately. Affected systems include—

- Fire-finder radars.
- Surveillance radars.
- Air defense radars.

Preventive Measures

D-33. Measures to reduce susceptibility to, and mitigate the effects of, enemy jamming of radar systems include—

- Radar cueing cycle.
- Use jam-resistant operating modes.
- Survivability moves.

- Use low power settings.
- Terrain masking.

Indicators

D-34. Indicators of radar jamming include—

- Radar-generated jamming report.
- Radar operating in degraded mode.

Reaction

D-35. Operators of affected radar systems should—

- **Increase distance between radar and forward line of own troops.** Increasing the distance between the radar and the forward line of own troops, and thus the threat jammer, may reduce the jamming signal to a level the radar can overcome.
- **Use alternate radar.** Switching to an alternate radar while allowing the threat to continue jamming the original radar.
- **Change radar frequency.** If a radar cannot overcome enemy jamming, the commander may direct use of an alternate or spare frequency. Preplanned and well-coordinated actions are required for practical dummy stations to continue to operate on the jammed frequency, to mask the change to an alternate frequency.
- **Use electromagnetic support or SIGINT capabilities to locate the jamming signal.** Leveraging EW or SIGINT capabilities requires coordination and collaboration between the CEMA section and the G-2 or S-2.
- **Report jamming to higher headquarters.** Submitting a joint spectrum interference resolution report to higher headquarters documents a history of problems and helps identify possible causes for subsequent interference.

SATELLITE COMMUNICATIONS JAMMING

D-36. Expeditionary forces rely heavily on satellite communications capabilities for beyond line of sight network transport. Systems and capabilities affected by satellite communications jamming include—

- Friendly force tracking.
- Command post networks.
- Narrowband (single-channel) tactical satellite radios.
- Wideband satellite communications ground terminals.
- Intelligence reporting systems.

Preventive Measures

D-37. Operational and employment measures to prevent jamming of narrowband (single-channel) tactical satellite include—

- Minimizing transmissions on single-channel tactical satellite radios—operators should try to keep radio transmissions to six seconds or less.
- Terrain masking.
- Camouflage net masking.

Note. Most wideband satellite jamming is directed at the satellite. Preventive measures for wideband satellite jamming are limited. Refer to Army doctrine for space operations for more information about mitigating satellite jamming.

Indicators

D-38. Possible operator indications of satellite jamming include—

- Seemingly random noise or static on narrowband (single-channel) tactical satellite radios.
- Recorded sounds, such as messages or music, over single-channel tactical satellite radios.

- Loss of SATLOCK indication.
- Loss of data from the satellite.
- Low signal-to-noise indicated on wideband satellite terminal.
- Unexplained increase in receive power level.

Reaction

D-39. The reactive measures here apply mostly to narrowband (single-channel) satellite communications systems. When a single-channel tactical satellite radio operator recognizes a jamming attempt, they may—

- **Increase transmit power.** Only increase power on wideband satellite communications terminals if directed by the satellite controller.
- **Change to a preapproved alternate frequency.**
- **Execute the primary, alternate, contingency, and emergency communication plan.** Quickly changing to the alternate or contingency means of communication reduces the disruption of the command and control system.
- **Use electromagnetic support or SIGINT capabilities to locate the jamming signal.** Leveraging EW or SIGINT capabilities requires coordination and collaboration between the CEMA section and the G-2 or S-2.
- **Report jamming to higher headquarters.** The higher headquarters' frequency manager and CEWO can correlate reports from units across the assigned area to isolate enemy jammers and plan countermeasures, including nominating targets for lethal or nonlethal fires.
- **Use line of sight systems for network transport.** Units will be unable to communicate beyond line of sight, or through significant obstructions.
- **Cease transmission or lower power on satellite terminal.** Lower or eliminate transmit power while observing the suspect link on a spectrum analyzer. If the signal remains, this could indicate the threat matching the friendly waveform.

D-40. Satellite network controllers at the wideband satellite communications operations center coordinate all interference resolution and reporting on DOD wideband satellite networks.

JOINT SPECTRUM INTERFERENCE RESOLUTION

D-41. Joint spectrum interference resolution reporting addresses electromagnetic interference and jamming incidents affecting the DOD. The objective of joint spectrum interference resolution is to document and assist in resolving electromagnetic attack and recurring electromagnetic interference.

INCIDENT RESOLUTION

D-42. Spectrum managers and EW Soldiers attempt to resolve incidents at the lowest possible level using organic assets. G-6 or S-6 spectrum managers assist affected equipment operators through the electromagnetic interference resolution process, guiding them through the troubleshooting process. This assistance may require on-site emitter surveys and on-site investigation by unit or higher headquarters spectrum managers. Spectrum managers use Service- or unit-procured portable handheld spectrum analyzers to perform the required analysis. An emitter survey is an on-site analysis to validate all emitters within a given area against Spectrum XXI records. On-site investigations effectively compare the emitter survey results against anomalous radio frequency signals to identify the source of harmful electromagnetic interference.

D-43. If the spectrum manager and CEWO cannot resolve an incident locally, they submit a joint spectrum interference resolution report through the chain of command. Each successive echelon attempts to resolve the incident at their level before forwarding the report to the next higher headquarters.

D-44. Corps and division spectrum management chiefs coordinate regional and local interference resolution. The impact of each interference incident is unique, so no standard procedure establishes or guarantees resolution in every case. A systematic approach reduces the time and cost required to resolve interference situations. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting.

ELECTROMAGNETIC INTERFERENCE RESOLUTION SYSTEMS

D-45. The Spectrum XXI assignment database is, by joint doctrine, the primary source of information about spectrum use for all DOD operations. Near real-time maintenance of this database is critical to its effective use for electromagnetic interference resolution. Failure to maintain the Spectrum XXI database will also degrade the ability to make interference-free frequency assignments.

D-46. Intelligence elements and S-2 staffs can access information sources, such as intercept databases, that are not available to spectrum managers. They also have analysts who can assist in interpreting unfamiliar signals. The intelligence community can task in-theater assets or interface with national-level agencies to leverage in-theater assets to geolocate interfering signals. Spectrum managers at all echelons should establish a working relationship with their intelligence counterparts.

REPORTING PROCEDURE

D-47. Interference is always reported from a receiver perspective. Interference reports need to identify specific factors:

- The affected unit.
- The affected spectrum-dependent device.
- The receiver frequency.
- The affected location or locations.
- Impact on the mission.

D-48. Spectrum managers should not delay reports due to a lack of complete information. They can submit an initial report while attempting to resolve the incident, and follow-up reports to provide additional information, as it becomes available.

D-49. Joint spectrum interference resolution reporting takes place through secure channels. The submitter of a joint spectrum interference resolution report determines the appropriate security classification by evaluating the sensitivity of the electromagnetic interference on the affected system and considering the classification of the text comments. Army units report through their chain of command to the combatant command and the United States Army Communications-Electronics Services Office.

D-50. Message precedence of a joint spectrum interference resolution report depends on the urgency of the reported situation. Normally reports are routine or priority precedence, unless the originating unit believes the incident is hazardous to military operations. In this case, the unit reports using immediate precedence.

THREAT MALICIOUS CYBERSPACE ACTIVITY

D-51. U.S. networks face continuous risk of malicious cyberspace activity. Cyberspace risk increases substantially when operating against a peer threat in a contested environment. DODIN operations personnel implementing cybersecurity measures can prevent many malicious cyberspace activities. If threat malicious cyberspace activity breaches cybersecurity measures, it may require defensive cyberspace operations support to mitigate.

DENIAL-OF-SERVICE

D-52. A denial-of-service attack seeks to make a computer or network resource unavailable to its intended users by disrupting services of a host connected to the Internet. An attacker floods the target computer or network resource with more requests than it can handle to overload the system and prevent it from fulfilling legitimate requests.

D-53. Denial-of-service attacks can affect any Internet Protocol network system, including—

- Command and control information systems.
- Logistics systems.
- Administrative systems.
- End user devices, such as computer workstations.

Preventive Measures

D-54. Good cybersecurity practices can prevent or lessen the effects of a denial-of-service attack. Cybersecurity personnel should—

- Maintain current antivirus software and virus definition files.
- Maintain properly configured network firewalls.

Indicators

D-55. Operator indications of a denial-of-service attack may include—

- Abnormally slow network performance when opening files or accessing websites.
- Request timeouts.
- Widespread unavailability of a website or network system.

Reaction

D-56. When faced with the symptoms of a denial-of-service attack, DODIN operations personnel should—

- Report to the next higher echelon S-6, G-6, or J-6 to determine whether the system slowdown is due to known activity on the network.
- Report suspected attacks to the G-2 or S-2 and G-3 or S-3.
- Continue operation using alternate or contingency means of communication.

MALWARE

D-57. Malware is software designed to interfere with a computer's normal functioning. Malware can be targeted to damage a computer, server, or computer network. Malware attacks can affect any automated information system, including—

- Command and control information systems.
- Logistics systems.
- Administrative systems.
- End user devices, such as computer workstations.

Preventive Measures

D-58. Cybersecurity personnel attempt to prevent malware attacks by—

- Using and maintaining up to date antivirus software and virus definition files.
- Keeping system software updated and patched.
- Ensuring compliance with the most recent security technical implementation guides.
- Maintaining properly configured network firewalls.

Indicators

D-59. Possible indicators of a malware attack include—

- Destruction of, or unexplained changes to, files.
- Spontaneous restart of computers.
- Erratic, delayed, or unexpected computer or network activity.
- Antivirus software warnings.

Reaction

D-60. If operators or DODIN operations personnel observe indications of a possible malware attack, they should—

- Disconnect the affected system.
- Report to the next higher echelon G-6 or J-6.
- Continue operation using alternate or contingency means of communication.
- Report to the G-2 or S-2 and G-3 or S-3.

D-61. DODIN operations personnel should not reconfigure computers or network systems in response to an attack unless directed by their next higher echelon.

DATA EXFILTRATION AND COLLECTION

D-62. *Exfiltration* is the unauthorized transfer of information from a system (NIST SP 800-53). Data exfiltration may be either electronic—removing files through the network, or physical—removing paper or electronic copies from sensitive areas. Either method may disclose sensitive operational information and plans. Exfiltration of sensitive data may place operations at risk.

D-63. All automated information systems may be targeted for data exfiltration and collection. Affected systems include—

- Command and control information systems.
- Logistics systems.
- Administrative systems.
- End user devices, such as computer workstations.

Preventive Measures

D-64. Cybersecurity measures and physical security combine to prevent data exfiltration and collection by—

- Implementing strict identity, credential, and access management controls for network systems.
- Enforcing strict physical security controls.
- Implementing access control restrictions for classified workspaces.
- Employing data loss prevention software.
- Encrypting data-at-rest.
- Maintaining strong passwords for network access.

Indicators

D-65. Indicators of threat data exfiltration and collection efforts include—

- Attempted or successful unauthorized physical access to sensitive areas.
- Unusually high volume of outgoing network traffic.

Reaction

D-66. The effects of data exfiltration can be catastrophic. If an enemy can steal enough documents, they can develop a complete assessment of U.S. capabilities, troop strength, logistics, and even operation plans. If any member of the unit suspects an enemy data exfiltration attempt, they should—

- Report to the G-2 or S-2 and G-3 or S-3.
- Report to the next higher echelon.
- Consider changing the maneuver course of action if exfiltration compromises an operation or support plan.

SOCIAL ENGINEERING

D-67. Social engineering includes methods such as phishing to obtain personal or confidential information which can then be used illicitly. Social engineering uses techniques that rely on weakness in human nature rather than hardware or software. The goal is to deceive people into revealing passwords and other information that compromise the security of automated information systems and networks. Threats may also use social engineering techniques to identify and develop targets for more advanced social engineering attacks, such as spear phishing and whaling.

D-68. The target of a social engineering attack is an individual. A successful social engineering attack may compromise any system to which the affected individual has access.

Preventive Measures

D-69. All users should maintain operations security and cybersecurity awareness to avoid falling victim to a social engineering attack. They should—

- Confirm the identity of individuals asking for personal information or access credentials.
- Pay close attention to website addresses embedded in e-mails.

D-70. Users should avoid disclosing any information to unknown or unverified individuals. Disclosing even seemingly innocuous information could make subsequent social engineering or spear phishing attempts against other targeted individuals seem much more legitimate.

Indicators

D-71. Indicators of social engineering attempts include—

- Unexpected phone calls from unknown callers requesting sensitive information.
- Websites that do not look normal, that contain broken links, or that have a mismatch between the display text and the Internet address.
- Unauthorized personnel shoulder surfing.

Reaction

D-72. If personnel suspect a social engineering attempt, they should—

- Confirm the requestor's identity before disclosing information.
- Report the attempt to supervisors, network managers, and the G-2 or S-2 and the G-2 or S-2.
- Report social engineering attempts to next higher echelon.

D-73. Promptly reporting attempts at social engineering can raise awareness and prevent others from falling victim to the same techniques.

PHISHING, SPEAR PHISHING, AND WHALING

D-74. Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details for malicious reasons by posing as a trustworthy entity in electronic communications. Spear phishing is a targeted phishing attempt, usually against key individuals or personnel with elevated or special access privileges. Whaling is a sophisticated phishing attack that targets high-ranking personnel to steal especially sensitive information.

D-75. Anyone may fall victim to a phishing attack. Key leaders and network administrators are also subject to spear phishing. Senior leaders may be targeted in a whaling attack.

Preventive Measures

D-76. All personnel should protect themselves from phishing attacks by following established best practices outlined in annual cybersecurity refresher training. Depending on the cyber protection condition level, the command may—

- Maintain awareness of personal use of commercial e-mail.
- Restrict the use of personal e-mail, as required.
- Block access to commercial e-mail providers.
- Not use hyperlinks in the bodies of e-mail messages.

Indicators

D-77. Most common phishing techniques share certain traits, including—

- E-mails with generic greetings—note that spear phishing and whaling attempts are likely be more refined and address the targeted individual by name.
- E-mails requesting personal information or login credentials.
- E-mails requesting or demanding an urgent response.
- E-mails with spoofed links—where the display text does not match the Internet address shown when hovering over the link.

Reaction

D-78. If an individual suspects a phishing, spear phishing, or whaling attempt, they should—

- Report the attempt to the chain of command, automation support section, and the G-2 or S-2.
- Confirm the identity of the sender before taking any action.

D-79. Individuals can further protect themselves from fraudulent links by never accessing their personal accounts through links in e-mails. For instance, if an e-mail claims to be from the individual's bank or credit card company, they should access their account only through the legitimate secure website, not through a hyperlink provided in an e-mail.

D-80. Commanders should not threaten punishment against individuals who inadvertently fall victim to phishing attempts. Fear of punishment could prevent individuals from reporting attacks.

SOCIAL MEDIA ATTACKS

D-81. Threats may conduct social media attacks in support of their information collection and information warfare goals. All individuals using any form of social media are potential targets.

Preventive Measures

D-82. To minimize the likelihood of falling victim to a social media attack—

- Individuals should strictly limit personal information posted to their social media accounts. The compromise of this information could either be damaging in itself, or it could strengthen a threat's subsequent social engineering or spear phishing attacks.
- Individuals should restrict who can view their social media profiles and activities using the social media platform's privacy settings.
- Individuals and public affairs personnel must carefully weigh operations security considerations when they engage on social media platforms.
- Individuals and group administrators should not accept friend or group membership requests from unknown or unverifiable users.
- Commands should consider limiting or restricting access to social media platforms using government systems as mission or operations security concerns dictate.

Indicators

D-83. Indicators of social media attacks include—

- Friend requests from unknown persons, or duplicate friend requests that mimic a known person.
- Unknown users commenting on social media posts.

Reaction

D-84. If a social media attack is known or suspected, personnel should—

- Report the suspected compromise to the G-2 or S-2.
- Immediately change any compromised passwords.
- Watch for indicators of identity theft.

ATTACKS AGAINST PERSONAL ELECTRONIC DEVICES

D-85. Widespread use of personal electronic devices creates significant vulnerabilities when operating against a peer threat. Peer threats have demonstrated advanced capabilities to exploit personal electronic devices, seize control of cellular communications networks, and locate personal cellular phones with precision. This gives them the ability to collect information, conduct information warfare activities, and direct accurate lethal fires. Any personal electronic device capable of connecting to Wi-Fi, Bluetooth, or cellular communications systems is vulnerable to attack.

Preventive Measures

D-86. Measures to protect against personal electronic device attacks include—

- Maintaining strict control and accountability of personal electronic devices.
- Downloading only trusted apps from approved sources.
- Maintaining current security updates on devices and apps.

- Disabling Bluetooth, Wi-Fi, and near field communication features when they are not in use.
- Encrypting sensitive files and personal information.
- Allowing only government-provided personal electronic devices to connect to the DOD network.
- Commanders should consider restricting or banning the use of personal electronic devices, based on the tactical situation.

Indicators

D-87. Some possible indicators of attacks against personal electronic devices are—

- Enemy attacks that seem to correlate with personal electronic device usage.
- Incoming lethal attacks that occur with unexplained precision.
- Receiving a barrage of text messages—up to several per second—preventing the intended use of the device.
- Incoming propaganda or psychological warfare messages from unknown numbers.

Reaction

D-88. If a unit suspects it has come under attack, commanders should—

- Quickly displace the element under attack and direct all personnel to turn off personal electronic devices.
- Disable personal electronic devices and confiscate them, if necessary.
- Report to the next higher echelon.

Appendix E

Message Formats

This appendix gives the formats for various electromagnetic warfare messages and electromagnetic warfare reprogramming messages.

ELECTROMAGNETIC WARFARE MESSAGES

STOP JAMMING MESSAGE

E-1. To stop jamming, the CEWO submits a stop jamming message as illustrated in figure E-1.

STOP JAMMING MESSAGE
GENERAL INSTRUCTIONS: Use to terminate a jamming task conducted by an electromagnetic attack (EA) asset.
LINE 1 – DATE AND TIME: (date-time group of when jamming should be terminated).
LINE 2 – UNIT: (unit supported by jamming mission and is requesting termination).
LINE 3 – FREQUENCY: (enter the radio frequency being jammed or enter 'ALL' if jamming is to stop on all jammed frequencies).
LINE 4 – NARRATIVE: (any additional information required for clarification).
LINE 5 – AUTHENTICATION: (message authentication if unit standard operating procedures require authentication).
Legend:
EA electromagnetic attack

Figure E-1. Stop jamming message format

ELECTROMAGNETIC WARFARE FREQUENCY DECONFLICTION MESSAGE

E-2. The CEWO completes an EW frequency deconfliction message (see figure E-2 on page 164) to identify and categorize frequencies to be used by friendly forces and to prevent frequency fratricide. The EW frequency deconfliction message promulgates a list of TABOO, protected, and guarded frequencies to prevent adverse impact to friendly operations. Guarded frequencies are enemy frequencies that are, for a specified time period, being exploited for combat information and intelligence or jammed after the commander has weighed the potential operational gain against the loss of technical information. See paragraph 4-51 for a description of TABOO and protected frequencies.

ELECTROMAGNETIC WARFARE FREQUENCY DECONFLICTION MESSAGE [EWDECONFLICT]

REPORT NUMBER: E010 {USMTF #F402}

GENERAL INSTRUCTIONS: Use to promulgate a list of protected, guarded, and TABOO frequencies to ensure friendly force use of the frequency spectrum without adverse impact from friendly electromagnetic attack.

LINE 1 – DATE AND TIME _____ (DTG)
LINE 2 – UNIT _____ (unit making report)
LINE 3 – TYPE _____ (TABOO, protected, or guarded)
LINE 4 – STATUS _____ (restricted status of frequency: NEW, CHANGE, CANCEL, OR RENEW)
LINE 5 – FREQUENCY _____ (frequency/frequencies)
LINE 6 – ON TIME _____ (start DTG of frequency restriction)
LINE 7 – OFF TIME _____ (end DTG of frequency restriction)
LINE 8 – LOCATION _____ (UTM or six-digit grid coordinate with MGRS grid zone designator)

****Repeat lines 3 through 8 as a group to accommodate multiple reports. Assign sequential line numbers to succeeding iterations; for example, first iteration 3 through 9; second iteration 3a through 8a; and so on.**

LINE 9 – NARRATIVE _____ (free text for additional information required for report clarification)
LINE 10 – AUTHENTICATION _____ (report authentication)

Legend:

DTG	date-time group	MGRS	Military Grid Reference System
EWDECONFLICT	electromagnetic warfare frequency deconfliction	USMTF	United States message text format

Figure E-2. Electromagnetic warfare frequency deconfliction message

ELECTROMAGNETIC WARFARE MISSION SUMMARY

E-3. The CEWO maintains a record of EW missions. The record is the EW mission summary (see figure E-3 on page 165).

Electromagnetic Warfare Mission Summary [EWMSNSUM]

REPORT NUMBER: E015 {USMTF # G424}

GENERAL INSTRUCTIONS: Use to summarize significant EW missions and the status of offensive EW assets.

Reference: ATP 3-12.3

LINE 1 – DATE AND TIME	(DTG)
LINE 2 – UNIT	(Unit making report)
LINE 3 – FROM	(Beginning DTG Zulu of period summarized)
LINE 4 – THROUGH	Ending DTG Zulu of period summarized)
LINE 5 – COUNTRY	(Nationality of the target emitter of concern)
LINE 6 – LOCATION	(UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 7 – EMITTER	(Emitter call sign and name or nomenclature)
LINE 8 – FUNCTION	(Primary function of target)
LINE 9 – NOTATION	(Notation or sorting code)
LINE 10 – SIGNAL	(Type of signal of target emitter)
LINE 11 – ON TIME	(DTG that planned EA activity was initiated)
LINE 12 – OFF TIME	(DTG that planned EA activity was terminated)
LINE 13 – PRIORITY	(Relative importance of EA mission)
LINE 14 – TYPE	(Type of EA used against the emitter)
LINE 15 – PRIMARY FREQUENCY	(Primary frequency of EA target signal)
LINE 16 – SECONDARY FREQUENCY	(Secondary frequency of EA target signal)
LINE 17 – LOW FREQUENCY	(Lower frequency limit of target equipment class)
LINE 18 – HIGH FREQUENCY	(Upper frequency limit of target equipment class)
LINE 19 – BANDWITH	(Target frequency bandwidth expressed in MHz)
LINE 20 – PULSE REPETITION	(Pulse repetition interval or frequency)
LINE 21 – SYSTEM USED	(Name/nomenclature of EW asset used to perform the task)
LINE 22 – OPERATIONAL	(Number of units that can perform primary EW mission)
LINE 23 – NONOPERATIONAL	(Number of units that cannot perform primary EW mission)
LINE 24 – DESTROYED	(Number of units that were destroyed in combat)
LINE 25 – CHAFF	(Type of chaff)
LINE 26– LOWER FREQUENCY	(Lower frequency of a range of frequencies that was blanked by chaff or the lower EA frequency)
LINE 27 – UPPER FREQUENCY	(Upper frequency of a range of frequencies that was blanked by chaff or the lower EA frequency)
LINE 28 – LOW LEVEL	(Lower altitude in hundreds of feet of airspace that was blanked by chaff)
LINE 29 – UPPER LEVEL	(Upper altitude in hundreds of feet of airspace that was blanked by chaff)
LINE 30 – TECHNIQUE	(EA technique employed)
LINE 31 – COUNTRY	(Country in which chaff was employed)
LINE 32 – ON TIME	(DTG that the chaff drop was initiated)
LINE 33– OFF TIME	(DTG that the chaff drop was terminated)
LINE 34 – START LOCATION	(Start location of the chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 35 – STOP LOCATION	(Stop location of the chaff drop in UTM or six-digit grid coordinate with grid zone designator)
LINE 36 – NARRATIVE	(Free text for additional information required for clarification of report)
LINE 37 – AUTHENTICATION	(Report authentication)

LEGEND

DTG	date-time group	MGRS	military grid reference system
EA	electromagnetic attack	MHz	megahertz
EW	electromagnetic warfare	UTM	Universal Transverse Mercator

Figure E-3. Electromagnetic warfare mission summary

ELECTROMAGNETIC WARFARE TASKING MESSAGE

E-4. The CEWO uses the EW tasking message format (see figure E-4 beginning below and continued on page 167) to task an EW asset to provide a requested effect.

ELECTROMAGNETIC WARFARE REQUESTING/TASKING MESSAGE [EWRTM]

REPORT NUMBER: E020 {USMTF #A426}

GENERAL INSTRUCTIONS: Use (1) to task component commanders to perform EW operations to Support the overall EW plan, (2) to support component EW operations, and (3) to request EW support From sources outside their commands.

Reference: ATP 3-12.3

LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(Unit making report)
LINE 3 – EA _____	(Electromagnetic activity)
LINE 4 – TASKED _____	(Designator of tasked unit if the JOC is tasking The unit)
LINE 5 – COUNTRY _____	(Nationality of the target emitter of concern)
LINE 6 – LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid Zone designator)
LINE 7 – EMITTER _____	(Emitter call sign and name or nomenclature)
LINE 8 – FUNCTION _____	(Primary function of target)
LINE 9 – NOTATION _____	(Notation or sorting code)
LINE 10 – SIGNAL _____	(Type of signal of target emitter)
LINE 11 – ON TIME _____	(DTG that planned EA activity was initiated)
LINE 12 – OFF TIME _____	(DTG that planned EA activity will be terminated)
LINE 13 – PRIORITY _____	(Relative importance of EA mission)
LINE 14 – TYPE _____	(Type of EA and technique used against the emitter)
LINE 15 – PRIMARY FREQUENCY _____	(Primary frequency of EA target signal)
LINE 16 – SECONDARY FREQUENCY _____	(Secondary frequency of EA target signal)
LINE 17 – LOW FREQUENCY _____	(Lower frequency limit of EA target class)
LINE 18 – HIGH FREQUENCY _____	(Upper frequency limit of EA target class)
LINE 19 – BANDWIDTH _____	(Target frequency bandwidth Expressed in MHz)
LINE 20 – PULSE REPETITION _____	(Pulse repetition interval or frequency)
LINE 21 – ES _____	(Electromagnetic support)
LINE 22 – COUNTRY _____	(Nationality of the target emitter of concern)
LINE 23 – LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid Zone designator)
LINE 24 – EMITTER _____	(Emitter call sign and name or nomenclature)
LINE 25 – FUNCTION _____	(Primary function of target)
LINE 26 – NOTATION _____	(Notation or sorting code)
LINE 27 – SIGNAL _____	(Type of signal of target emitter)
LINE 28 – PRIMARY FREQUENCY _____	(Primary frequency of ES target signal)
LINE 29 – SECONDARY FREQUENCY _____	(Secondary frequency of ES target signal)
LINE 30 – LOW FREQUENCY _____	(Lower frequency limit of target equipment class)

Legend:

DTG	date-time group	JOC	joint operations center
EA	electromagnetic attack	MGRS	Military Grid Reference System
ES	electromagnetic support	MHz	megahertz
EW	electromagnetic warfare	UTM	Universal Transverse Mercator

Figure E-4. Electromagnetic warfare requesting/tasking message

LINE 31 – HIGH FREQUENCY	(Upper frequency limit of target class)
LINE 32 – BANDWIDTH	(Target frequency bandwidth expressed in MHz)
LINE 33 – PULSE REPETITION	(Pulse repetition interval or frequency)
LINE 34 – ON TIME	(DTG that planned ES activity was initiated)
LINE 35 – OFF TIME	(DTG that planned ES activity was terminated)
LINE 36 – ESSENTIAL	(EEI category indicator)
LINE 37 – PRIORITY	(Relative importance of ES mission)
LINE 38 – CHAFF	(Type of chaff)
LINE 39 – LOWER FREQUENCY	(Lower frequency of a range of frequencies that is to be blanked by chaff or the lower EA frequency)
LINE 40 – UPPER FREQUENCY	(Upper frequency of a range of frequencies that is to be blanked by chaff or the lower EA frequency)
LINE 41 – LOW LEVEL	(Lower altitude in hundreds of feet of airspace to be blanked by chaff)
LINE 42 – UPPER LEVEL	(Upper altitude in hundreds of feet of airspace to be blanked by chaff)
LINE 43 – TECHNIQUE	(EA technique to be employed)
LINE 44 – COUNTRY	(Country in which chaff is to be employed)
LINE 45 – ON TIME	(DTG that the planned chaff drop will be initiated)
LINE 46 – OFF TIME	(DTG that the planned chaff drop will terminate)
LINE 47 – START LOCATION	(Start location of the chaff drop in UTM or six-digit Grid coordinate with grid zone designator)
LINE 48 – STOP LOCATION	(Stop location of the chaff drop in UTM or six-digit Grid coordinate with grid zone designator)
LINE 49 – NARRATIVE	(Free text for additional information required for report clarification)
LINE 50 – AUTHENTICATION	(Report authentication)

Legend:

DTG	date-time group	ES	electromagnetic support
EA	electromagnetic attack	MHz	megahertz
EEI	essential elements of information	UTM	Universal Transverse Mercator

Figure E-4. Electromagnetic warfare requesting/tasking message (continued)

MEACONING, INTRUSION, JAMMING, AND INTERFERENCE FEEDER REPORT

E-5. The meaconing, intrusion, jamming, and interference feeder report (figure E-5 on page 168) is used for immediate tactical reporting of electromagnetic interference. Elements submitting the report should forward the report to the G-6 or S-6 spectrum manager.

MEACONING, INTRUSION, JAMMING, AND INTERFERENCE FEEDER REPORT [MIJIFEEDER]

REPORT NUMBER: M020 {USMTF #C120}

GENERAL INSTRUCTIONS: Use to share MIJI incidents in a timely manner and to provide for joint exchange of tactical MIJI information including electro-optical interference.

LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(unit making report)
LINE 3 – INTERFERENCE _____	(strength and characteristics)
LINE 4 – LOCATION _____	(UTM or six-digit grid coordinate with MGRS grid zone designator of incident)
LINE 5 – ON TIME _____	(start DTG)
LINE 6 – OFF TIME _____	(end DTG)
LINE 7 – EFFECTS _____	(operations or equipment affected)
LINE 8 – FREQUENCY _____	(frequency or frequency range affected)
LINE 9 – NARRATIVE _____	(free text for additional information required for report clarification)
LINE 10 – AUTHENTICATION _____	(report authentication)

Legend:

DTG	date-time group
MGRS	Military Grid Reference System
MIJI	meaconing, intrusion, jamming, and interference
MIJIFEEDER	meaconing, intrusion, jamming, and interference feeder
USMTF	United States message text format
UTM	Universal Transverse Mercator

Figure E-5. Meaconing, intrusion, jamming, and interference feeder report format

ELECTROMAGNETIC WARFARE REPROGRAMMING MESSAGES

E-6. There are a variety of EW reprogramming messages that coincide with the phases of the integrated reprogramming cycle:

- **Determine the requirement**—threat information message or operational change request.
- **Determine the response**—system impact message.
- **Create the response**—reprogramming impact message.
- **Implement the response**—unit loading message.

MESSAGE PRIORITY

E-7. Reprogramming messages are submitted with routine, urgent, or emergency priority, depending on the strategic context and tactical situation. Units should generally assign priority to reprogramming messages and based on these criteria:

- **Routine**—assigned during competition below armed conflict.
- **Urgent**—assigned during crisis.
- **Emergency**—assigned during armed conflict.

PRIORITY OF PROGRAMMING ACTIONS

E-8. Priority of a reprogramming action may change if a crisis occurs or ends in the middle of the action. Recipients of reprogramming messages should perform reprogramming actions as required by the implementation authority based on message priority and the commander's guidance.

- **Routine**—Considered normal day-to-day operations. Units may schedule implementation of the reprogramming action around the daily training and maintenance schedule.

Note. A not-later-than date for completion may be specified in the reprogramming message. Units should adhere to these dates even for routine reprogramming actions.

- **Urgent**—Urgent changes should be accomplished during normal duty hours but should take precedence over other activities until completed. Urgent reprogramming changes should generally be implemented within 72 hours after message publication. The actual implementation timeline may vary depending on mission requirements and implementation authority guidance.
- **Emergency**—Responsible personnel should immediately perform reprogramming actions as specified in the reprogramming message. Emergency changes require 24-hour operations until completed, with the goal of implementing the reprogramming action for all affected systems within 24 hours after message publication. Commanders make the final determination whether training or operational missions can be conducted without the specified reprogramming action being completed.

THREAT INFORMATION MESSAGE

E-9. The Army Reprogramming Analysis Team uses the threat information message (see figure E-6) to disseminate information regarding system- or region-specific threat EW capabilities.

CLASSIFICATION

PRIORITY: [ROUTINE, URGENT, OR EMERGENCY]

DTG: (U) YYYY/MM/DD HHMMZ

FROM: ARAT-PO

TO: AMSO/EW PERSONNEL

SUBJECT: ARMY THREAT INFORMATION MESSATE (TIM) YYYY-MM-DD-## [NAME OF EW THREAT]

1. ( ) ATTENTION: DISSEMINATE TO SUBORDINATE [AVIATION OR GROUND] UNITS. PASS TO UNIT [AVIATION MISSION SURVIVABILITY OFFICER (AMSO) OR ELECTROMAGNETIC WARFARE PERSONNEL]. THIS MESSAGE CONTAINS INFORMATION ON AN ELECTROMAGNETIC WARFARE THREAT. THIS TIM AFFECTS UNITS OPERATING IN THE [REGION, COUNTRY, OR AREA OF OPERATIONS].

2. ( ) [EW THREAT INFORMATION CONTENT].

3. ( ) CONTACT ARAT-PO AT DSN [PHONE NUMBER] OR COMMERCIAL [PHONE NUMBER], [E-MAIL CONTACT INFORMATION] WITH TECHNICAL QUESTIONS.

CLASSIFICATIONI

Legend:

ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
EW	electromagnetic warfare
M	month
Y	year
Z	Zulu

Figure E-6. Threat information message format

OPERATIONAL CHANGE REQUEST

E-10. An operational change request (see figure E-7) is a formal request from an Army unit, routed through their respective theater army and combatant command, which identifies the inability of an electromagnetic warfare system to meet operational requirements and specifies a need for new mission data to address the operational requirement. The Army Reprogramming Analysis Team Program Office treats the operational change request as a request for reprogramming support.

CLASSIFICATION

PRIORITY: [ROUTINE, URGENT, OR EMERGENCY]

DTG: (U) YYYY/MM/DD HHMMZ

FROM: [AFFECTED UNIT]

TO: ARAT-PO

SUBJECT: OPERATIONAL CHANGE REQUEST (OCR) FOR [SYSTEM [VERSION]

( ) REFERENCE A: [IF APPLICABLE] ARMY THREAT INFORMATION MESSAGE (TIM) 2020-0101 (Example)

1. ( ) THIS IS AN ARMY ELECTROMAGNETIC WARFARE OPERATIONAL CHANGE REQUEST.

2. ( ) REQUESTED CHANGE: [PROVIDE DESCRIPTION OF THE SPECIFIC PROBLEM (FOR EXAMPLE, REQUEST CHANGE TO AGP V.001 PFM AB-001-01 AND AN/APR-39D(V)2 MDS 1234 BASED ON TIM 2020-01-01].

3. ( ) SYSTEM: [COMPLETE NOMENCLATURE OF THE SYSTEM AND SOFTWARE VERSION (FOR EXAMPLE, AGP V.001 PFM AB-001-01 AND AN/APR-39D(V)2 MDS 1234].

4. ( ) REQUEST APPROVAL AND THAT THE ARAT-PO BEGIN WORK (BASED ON THE PRIORITY).

5. ( ) NEED BY DATE: [YYYY/MM/DD HHMMZ]

6. ( ) POC FOR THIS MESSAGE IS:

[NAME, RANK]

[UNIT]

[DUTY POSITION]

DSN: [PHONE NUMBER], COMM: [PHONE NUMBER]

E-MAIL: [.MIL E-MAIL], [SIPRNET E-MAIL]

7. ( ) DUTY HOURS/AFTER DUTY HOURS CONTACT INFORMATION: PLEASE CONTACT THE ABOVE POC DURING NORMAL DUTY HOURS [ZULU TIME]. AFTER HOURS PLEASE CONTACT THE DUTY OFFICER AT DSN: [PHONE NUMBER], COMM: [PHONE NUMBER].

DERIVED FROM: (U) [SYSTEM SCG]

DECLASSIFY ON: (U) [DATE]

DATE OF SOURCE: (U) [DATE OF SCG]

CLASSIFICATION

Legend:

ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
EW	electromagnetic warfare
M	month
POC	point of contact
SCG	security classification guide
SIPRNET	SECRET Internet Protocol Router Network
Y	year
Z	Zulu

Figure E-7. Operational change request message format

SYSTEM IMPACT MESSAGE

E-11. The Army Reprogramming Analysis Team uses the system impact message (see figure E-8 on page 171) to disseminate information about the impact of threat system changes, correlated with the capabilities of an EW system, approved changes to tactics, techniques, and procedures, and operational and tactical considerations.

CLASSIFICATION

PRIORITY: [ROUTINE, URGENT, OR EMERGENCY]

DTG: (U) YYYY/MM/DD HHMMZ

FROM: ARAT-PO

TO: AMSO/EW PERSONNEL

SUBJECT: ARMY SYSTEM IMPACT MESSAGE (SIM) YYYY-MM-DD-## FOR [EW SYSTEM]

1. ( ) ATTENTION: DISSEMINATE TO SUBORDINATE [AVIATION OR GROUND] UNITS. PASS TO UNIT [AVIATION MISSION SURVIVABILITY OFFICER (AMSO) OR ELECTROMAGNETIC WARFARE PERSONNEL]. THIS MESSAGE HAS THE POTENTIAL TO IMPACT ALL [AVIATION OR GROUND] UNITS IN THE [REGION] USING [EW SYSTEM].

2. ( ) DESCRIPTION OF ISSUE: (DESCRIBE THE THREAT CHANGE OR PROBLEM [FOR THREAT CHANGE, PROVIDE THE ELNOT, SYSTEM NAME, FUNCTION, OR PARAMETRIC CHANGE] AND ITS SPECIFIC IMPACT ON THE AFFECTED EW SYSTEM).

3. ( ) DISCUSSION: (DESCRIBE THE INDICATION, OR LACK OF INDICATION THE EW SYSTEM USER CAN EXPECT AND THE SPECIFIC OPERATIONAL IMPACT).

4. ( ) ADVISEMENT: (INCLUDE RECOMMENDED TTP VETTED THROUGH TRADOC, AN INTERIM COURSE OF ACTION, LONG-RANGE COURSE OF ACTION, AND FOLLOW ON ARAT-PO ACTION TO ADDRESS THE PROBLEM).

5. ( ) [OTHER INSTRUCTIONS / UNIT LOADING MESSAGE (ULM) RESPONSE REQUIREMENTS].

6. ( ) CONTACT ARAT-PO AT DSN [PHONE NUMBER] OR COMMERCIAL [PHONE NUMBER], [E-MAIL CONTACT INFORMATION] WITH TECHNICAL QUESTIONS.

CLASSIFICATION

Legend:

ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
ELNOT	electromagnetic intelligence notation
EW	electromagnetic warfare
M	month
TRADOC	United States Army Training and Doctrine Command
Y	year
Z	Zulu

Figure E-8. System impact message format

REPROGRAMMING IMPACT MESSAGE

E-12. A reprogramming impact message (see figure E-9 on page 172) provides notification to aviation mission survivability officers and EW personnel of available new or updated EW mission data or software, special instructions, and implementation guidance. The Army distributes mission data, software, and tactics, techniques, and procedures via the Army Reprogramming Analysis Team Portal.

CLASSIFICATION

FROM: ARAT-PO

TO: AMSO/CEWO/OTHER APPLICABLE STAFF

SUBJECT: ARMY REPROGRAMMING IMPACT MESSAGE (RIM) YYYY-MM-DD FOR [SYSTEM]

1. ( ) ATTENTION: DISSEMINATE TO SUBORDINATE [AVIATION OR GROUND] UNITS. PASS TO UNIT [AVIATION MISSION SURVIVABILITY OFFICER (AMSO), CYBER ELECTROMAGNETIC WARFARE OFFICER, AND OTHER APPLICABLE STAFF]. THIS MESSAGE HAS THE POTENTIAL TO IMPACT ALL [AVIATION, GROUND, OR OTHER] UNITS IN THE [REGION, COUNTRY, AREA OF OPERATIONS, OR PLATFORM] USING THE [SYSTEM].

2. ( ) DESCRIPTION OF ISSUE: AN UPDATED [RELEASE TYPE] FOR [REGION, COUNTRY, AREA OF OPERATIONS, OR PLATFORM], [RELEASE NAME] HAS BEEN PRODUCED. [RELEASE NAME] REPLACES [RELEASE NAME]. (DESCRIBE THE UPDATE). THE FOLLOWING AREAS ARE AFFECTED. (LIST AFFECTED AREAS).

3. ( ) INSTRUCTIONS:

A. ( ) [RELEASE NAME IS AVAILABLE FOR DOWNLOAD FROM THE CLASSIFIED ARAT PORTAL. (HTTP://ARAT.ARMY.SMIL.MIL.

B. ( ) [AMSO, CEWO, OR OTHER APPLICABLE STAFF] SHOULD OBTAIN [RELEASE NAME] FROM THE ABOVE SOURCE. UNIT [SYSTEM] REPROGRAMMING IS AT THE DISCRETION OF THE TACTICAL COMMANDER.

C. ( ) THE FILES INTAINED IN [RELEASE NAME] ARE (LIST FILES OR REFERENCE EXTERNAL DOCUMENTS).

D. ( ) DETAILED INFORMATION ON [RELEASE NAME] IS AVAILABLE IN (LIST REFERENCE DOCUMENTS). FOR DETAILED INFORMATION SPECIFIC TO THE [SYSTEM], [AMSO OR EW PERSONNEL] MUST REVIEW [DOCUMENTS].

E. ( ) [OTHER INSTRUCTIONS / UNIT LOADING MESSAGE (ULM) RESPONSE REQUIREMENTS].

4. ( ) IF ELECTRONIC DISSEMINATION OF [RELEASE NAME] IS NOT AVAILABLE, PLEASE CONTACT THE ARAT OPERATIONS CENTER AT DSN [PHONE NUMBER] OR COMMERCIAL [PHONE NUMBER].

5. ( ) CONTACT ARAT-PO AT DSN [PHONE NUMBER] OR COMMERCIAL [PHONE NUMBER], [E-MAIL CONTACT INFORMATION] WITH TECHNICAL QUESTIONS.

CLASSIFICATION

Legend:

ARAT	Army Reprogramming Analysis Team
ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
EW	electromagnetic warfare
M	month
Y	year

Figure E-9. Reprogramming impact message format

UNIT LOADING MESSAGE

E-13. Units use the unit loading message (see figure E-10 on page 173) to notify the Army Reprogramming Analysis Team when they complete implementation of a reprogramming action. The unit describes any anomalies or issues they observed during implementation. When required, instructions for submitting a unit loading message are included in the applicable system impact message or reprogramming impact message.

CLASSIFICATION

DTG: (U) YYYY/MM/DD HHMMZ

SUBJECT: (U) UNIT LOADING MESSAGE (ULM) IN RESPONSE TO RIM 2019-10-02 (EXAMPLE)

REFERENCE A: (U) RIM 2019-01-01, AN/APR-39D(V)2 MDS 1234 (EXAMPLE)

REFERENCE B: [IF APPLICABLE]

1. (U) THIS IS AN ARMY UNIT LOADING MESSAGE.

2. ( ) [UNIT NAME] HAS COMPLETED LOADING SOFTWARE CHANGE IN REFERENCE B. LOADING WAS COMPLETED ON: YYYY/MM/DDDD HHMMZ.

3. ( ) [IF DIRECTED BY RELEVANT SIM OR RIM] ATTACHED IS A LIST OF TAIL NUMBERS/SERIAL NUMBERS AFFECTED.

4. ( ) [ANY PERTINENT INFORMATION CONCERNING DELAYS IN LOADING, PROBLEMS IN LOADING, OR ANOMALIES OBSERVED].

5. (U) POC FOR THIS MESSAGE IS:

[NAME, RANK, SERVICE]

[UNIT]

[POSITION TITLE]

DSN: [PHONE NUMBER], COMMERCIAL: [PHONE NUMBER]

E-MAIL: [NIPRNET ADDRESS]; [SIPRNET ADDRESS]

6. (U) DUTY HOURS/AFTER DUTY HOURS CONTACT INFORMATION: PLEASE CONTACT THE ABOVE POC DURING NORMAL DUTY HOURS [ZULU TIME]. AFTER HOURS, PLEASE CONTACT THE DUTY OFFICER AT DSN: [PHONE NUMBER], COMM: [PHONE NUMBER].

DERIVED FROM: (U) [SYSTEM SCG]

DECLASSIFY ON: (U) [DATE]

DATE OF SOURCE: (U) [DATE OF SCG]

CLASSIFICATION

Legend:

ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
EW	electromagnetic warfare
M	month
NIPRNET	Nonclassified Internet Protocol Router Network
SCG	security classification guide
SIPRNET	SECRET Internet Protocol Router Network
Y	Year
Z	Zulu

Figure E-10. Unit loading message format

ARMY REPROGRAMMING ANALYSIS TEAM INFORMATION MESSAGE

E-14. The Army Reprogramming Analysis Team information message (see figure E-11 on page 174) contains general information of importance to units and personnel conducting EW operations that does not fall under one of the other message formats.

CLASSIFICATION

PRIORITY: [ROUTINE, URGENT, OR EMERGENCY]

DTG: (U) YYYY/MM/DD HHMMZ

FROM: ARAT-PO

TO: AMSO/EW PERSONNEL

SUBJECT: ARMY REPROGRAMMING ANALYSIS TEAM INFORMATION MESSAGE (AIM) YYYY-MM-DD: [GENERAL SUBJECT]

1. ( ) ATTENTION: DISSEMINATE TO SUBORDINATE [AVIATION OR GROUND] UNITS. PASS TO UNIT [AVIATION MISSION SURVIVABILITY OFFICER (AMSO) OR ELECTROMAGNETIC WARFARE PERSONNEL]. THIS MESSAGE CONTAINS VALUABLE INFORMATION THAT IS NON-SYSTEM SPECIFIC.

2. ( ) [GENERAL INFORMATION CONTENT].

3. CONTACT ARAT-PO AT DSN [PHONE NUMBER] OR COMMERCIAL [PHONE NUMBER], [E-MAIL CONTACT INFORMATION] WITH QUESTIONS.

CLASSIFICATION

Legend:

ARAT-PO	Army Reprogramming Analysis Team Program Office
D	day
DSN	Defense Switched Network
EW	electromagnetic warfare
M	month
Y	year

Figure E-11. Army Reprogramming Analysis Team information message format

Appendix F

Echelons Above Corps Cyber and Electromagnetic Warfare Organizations

This appendix discusses the national, Department of Defense, and Reserve Components organizations that conduct or support cyberspace and electromagnetic warfare operations. This appendix also provides an overview of United States Cyber Command and its subordinate joint organizations that deliver cyberspace operations and electromagnetic warfare support to Army commanders using cyber mission forces.

NATIONAL ORGANIZATIONS

F-1. The United States Constitution establishes the President's authority as Commander in Chief of the Armed Forces and gives authority for Congress to fund and regulate the Armed Forces. The President, as Commander in Chief, commands the missions of the Armed Forces and, according to the laws passed by Congress, administers the Armed Forces. The president is also the head of the executive branch of government. As executive branch agencies, the Department of Justice and the Department of Homeland Security also have active roles in national cyberspace security.

DEPARTMENT OF JUSTICE

F-2. The Department of Justice leads the national effort to investigate cyber-based terrorism, espionage, computer intrusions, and major cyber fraud, and is responsible for protecting commercial domains such as .com, .net, and .org. The Federal Bureau of Investigation conducts domestic national security operations; investigates, attributes, and disrupts cyber crime; and collects, analyzes, and disseminates domestic cyber intelligence.

DEPARTMENT OF HOMELAND SECURITY

F-3. The Department of Homeland Security oversees protection of the .gov domain and provides expertise and assistance to private sector network owners and operators. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency collaborates with the government, industry, academia, and the international community to make cyberspace security a national priority and shared responsibility. Refer to JP 3-12 for additional information on Department of Homeland Security cyberspace defense responsibilities.

DEPARTMENT OF DEFENSE ORGANIZATIONS

F-4. The DOD provides cyberspace defense for the .mil domain. Each of the Armed Services has law enforcement and counterintelligence organizations that conduct many of the Federal Bureau of Investigation and Department of Homeland Security functions within their respective Services. These organizations include the Department of the Army Criminal Investigation Division, INSCOM, the Naval Criminal Investigative Service (for the Navy and Marine Corps), and the Air Force Office of Special Investigations (for the Air Force and Space Force).

F-5. The DOD uses cyberspace capabilities to shape cyberspace and conduct cyberspace missions to defend the nation under the authorities of the Secretary of Defense. Authorities for cyberspace operations undertaken by the Armed Forces derive from the Constitution and federal law. Key public laws that apply to the DOD include—

- Title 10, United States Code: Armed Forces.
- Title 32, United States Code: National Guard.
- Title 50, United States Code: War and National Defense.

F-6. The following DOD agencies provide direct or indirect support for cyberspace operations:

- The National Security Agency/Central Security Service.

- The Defense Intelligence Agency.
- The National Geospatial-Intelligence Agency.
- The National Reconnaissance Office.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

F-7. The National Security Agency and Central Security Service provide SIGINT and cyberspace security guidance and assistance to DOD organizations engaged in collecting, processing, analyzing, producing, and disseminating SIGINT data and information for foreign intelligence and counterintelligence purposes. They support national and departmental missions and provide SIGINT support for military operations as assigned by the Secretary of Defense.

F-8. The National Security Agency collaborates with other national-level organizations and agencies (Central Intelligence Agency, National Geospatial-Intelligence Agency, and Defense Intelligence Agency) to continually identify, catalog, and update the electromagnetic order of battle of threats. The National Security Agency/Central Security Service serves as an operationally focused analytical clearinghouse for all SIGINT databases that support combatant commands, subordinate commands, and the Joint Force.

F-9. The National Security Agency provides cybersecurity policy guidance and assistance to DOD components, the defense industrial base, and national customers. They also provide technical support, including encryption and cross-domain network solutions to support cyberspace security.

DEFENSE INTELLIGENCE AGENCY

F-10. The Defense Intelligence Agency satisfies military and military-related intelligence requirements of the Secretary and Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Director of National Intelligence. The Defense Intelligence Agency provides military intelligence contributions to national foreign intelligence and counterintelligence.

F-11. The Defense Intelligence Agency plans, manages, and executes intelligence operations during peacetime, crisis, and war. The Defense Intelligence Agency serves as the DOD lead for coordinating intelligence support to meet combatant command requirements, leads efforts to align analysis and information collection activities with all operations, and links and synchronizes military defense and national intelligence capabilities. In conjunction with other national-level intelligence organizations, the Defense Intelligence Agency updates the database of known threat signals in the electromagnetic order of battle.

F-12. The Defense Intelligence Agency conducts all-source intelligence analysis to support cyberspace operations, including dynamic threat assessments and campaign intelligence estimates that contribute to combatant command development of cyberspace aspects of joint intelligence preparation of the operational environment.

F-13. The Defense Intelligence Agency is the DOD lead for counterintelligence investigations in cyberspace. In conjunction with the Military Departments and DOD agencies, the DIA attempts to identify and neutralize all counterintelligence cyberspace threats to the DOD. The Defense Intelligence Agency's counterintelligence activities promote cyberspace superiority and provide worldwide situational awareness of cyberspace counterintelligence.

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

F-14. The National Geospatial-Intelligence Agency is a combat support agency and an intelligence community member organization subordinate to the Secretary of Defense, the Under Secretary of Defense for Intelligence, and the Director of National Intelligence. The National Geospatial-Intelligence Agency produces timely, relevant, and accurate geospatial intelligence to the joint force and is the primary source for geospatial intelligence analysis, products, data, and services at the national level. The National Geospatial-Intelligence Agency provides advisory tasking recommendations for Service-operated airborne and surface-based geospatial intelligence collection platforms and sensors.

F-15. National Geospatial-Intelligence Agency support teams provide direct support to a joint force commander's intelligence operations center and maintains National Geospatial-Intelligence Agency support teams for each of the Services, DOD agencies, and several non-DOD agencies. The National Geospatial-

Intelligence Agency manages satellite-based intelligence collection and develops distribution protocols for the National System for Geospatial Intelligence.

RESERVE COMPONENTS

F-16. The Army National Guard and the United States Army Reserve benefit from their associated civilian, academic, industry, and interagency communities to obtain Soldiers with specialized cyberspace operations skills, capabilities, and experience. The active Army leverages the Reserve Components' cyberspace capabilities by providing expanded capabilities in areas that are often too expensive and too time-consuming for Reserve Components to handle alone.

NATIONAL GUARD BUREAU

F-17. The National Guard Bureau coordinates Army National Guard and Air National Guard efforts to secure the nation, protect critical state infrastructure, and respond to state cyber emergencies in coordination with the Department of Homeland Security and responsible state and local officials. Many states have established cyber response teams capable of responding to cyber emergencies in the country.

F-18. The National Guard Bureau Chief serves as an advisor to Commander, USCYBERCOM. The National Guard Bureau supports planning and coordination for cyberspace and EW missions requested by combatant commanders or the Chairman of the Joint Chiefs of Staff. The National Guard Bureau channels communications between USCYBERCOM and the 50 states, the Commonwealth of Puerto Rico, the District of Columbia, Guam, and the U.S. Virgin Islands on all National Guard matters.

ARMY NATIONAL GUARD

F-19. The Army National Guard is a vital component of the Army's total force cyberspace and EW capabilities. It performs cyberspace operations in the 54 state-level joint force headquarters supporting both the Army and the states pursuant to United States Code Title 10 and Title 32 authorities. Their priority is to establish and maintain a secure cyber environment in the states by—

- Protecting critical cyberspace nodes.
- Developing cyberspace situational awareness.
- Supporting civil authorities for incident response and critical infrastructure protection.

F-20. The Army National Guard is the Army's expert for protecting critical infrastructure and essential resources. It supports the Army and USCYBERCOM with cyber network operations, cyber support, and cyber warfare capabilities. When deployed in a Title 10 status and allocated to a combatant command, Army National Guard CEMA sections and EW formations support the combatant commander in shaping operational environments.

UNITED STATES ARMY RESERVE

F-21. The United States Army Reserve is an expeditionary force that provides cyberspace capabilities to support ARCYBER and USCYBERCOM requirements. The United States Army Reserve provides trained and ready personnel to perform cyberspace operations to support joint, Army, and combatant commander mission requirements. United States Army Reserve personnel bring maturity and depth of experience, providing ready support to current and future operations. Uniquely, the United States Army Reserve will directly link to USCYBERCOM contingency plans, allowing them to mobilize personnel to support ARCYBER plans and operations.

UNITED STATES CYBER COMMAND

F-22. USCYBERCOM exercises coordinating authority for all DOD cyberspace operations, including operations to operate, secure, and defend the DODIN. USCYBERCOM accomplishes its missions within three primary lines of operation:

- Secure, operate, and defend the DODIN.
- Defend the nation from attack in cyberspace.
- Provide cyberspace support as required by a combatant commander.

F-23. USCYBERCOM directs security and defense of the DODIN using directive authority for cyberspace operations. When directed, USCYBERCOM also conducts cyberspace operations external to the DODIN (offensive cyberspace operations and defensive cyberspace operations-response actions) to support national objectives. Refer to JP 3-12 for more information about USCYBERCOM's roles and responsibilities.

F-24. DOD cyberspace forces include forces assigned to USCYBERCOM through the global force management process and Reserve Component forces. Cyberspace forces also include personnel who perform cybersecurity service provider roles established by the Services and DOD agencies to protect segments of the DODIN. Cybersecurity service providers are generally DOD-certified civilians and contractors who perform DODIN protection tasks such as analytics, infrastructure support, incident response, auditing, and service provider management.

CYBER MISSION FORCE

F-25. Commander, USCYBERCOM exercises combatant command authority over the Cyber Mission Force. Commander, USCYBERCOM uses Cyber Mission Force units to conduct national strategic missions or assigns units to support combatant commander missions through a Service joint force headquarters-cyber. The Cyber Mission Force consists of—

- Cyber Combat Mission Force.
- Cyber Protection Force.
- Cyber National Mission Force.

Cyber Combat Mission Force

F-26. The Cyber Combat Mission Force conducts offensive cyberspace operations and related technical and analytical activities in support of combatant command operations. When authorized and directed, the Cyber Combat Mission Force conducts cyberspace attacks in neutral and threat cyberspace to affect threat capabilities. The Cyber Combat Mission Force consists of combat mission teams and combat support teams.

F-27. Combat mission teams are tactical teams that conduct cyberspace surveillance and reconnaissance and cyberspace attacks in neutral and enemy cyberspace. Combat support teams are technical teams that support combat mission teams through intelligence analysis, cyberspace capability development, linguist support, and planning.

Cyber Protection Force

F-28. The Cyber Protection Force conducts defensive cyberspace operations-internal defensive measures within the DODIN or, when authorized and directed, in friendly cyberspace beyond the DODIN. The Cyber Protection Force consists of cyber protection teams organized, trained, and equipped to defend assigned cyberspace in coordination with and supporting segment owners, cybersecurity service providers, and users. The types of cyberspace protection teams are—

- National cyber protection teams—assigned to and directed by Cyber National Mission Force Headquarters.
- DODIN cyber protection teams—assigned to and directed by DOD Cyber Defense Command.
- Combatant command cyber protection teams—assigned to and directed by combatant commands.
- Service cyber protection teams—assigned to and directed by their assigned Service cyber component.

Cyber National Mission Force

F-29. The Cyber National Mission Force conducts defensive cyberspace operations to protect against malicious cyberspace activity based on USCYBERCOM and national priorities. The Cyber National Mission Force may conduct defensive cyberspace operations within the DODIN or, when authorized, outside of the DODIN in friendly or neutral cyberspace. The Cyber National Mission Force consists of national mission teams, national support teams, and national cyber protection teams.

F-30. National mission teams are tactical teams that conduct defensive cyberspace operations-response actions. National support teams support national mission teams with intelligence analysis, cyberspace capability development, linguist support, and planning. National cyber protection teams conduct national-

level defensive cyberspace operations-internal defensive measures that can extend to defend non-DOD mission partner or critical infrastructure networks when ordered by the Secretary of Defense. The Cyber National Mission Force is assigned to and directed by the Cyber National Mission Force Headquarters. Table F-1 outlines the relationships between Cyber Mission Force elements, associated cyberspace operations and actions, and typical operating locations in friendly, neutral, and threat cyberspace.

Table F-1. Elements of the Cyber Mission Force and their associated teams

Type of Cyberspace Operation	*Cyberspace Force Conducting the Operation*	*Location in Cyberspace*	*Type of Cyberspace Actions*
DODIN operations	Service-retained Cyber Mission Forces	The DODIN	Cyberspace security
Offensive cyberspace operations	Cyber Combat Mission Force, consisting of combat mission teams supported by combat support teams	Neutral and threat cyberspace	Cyberspace attack and cyberspace exploitation
Defensive cyberspace operations-internal defensive measures (DODIN)	Cyber Protection Force, consisting of Service, DODIN, and combatant command cyberspace protection teams	Friendly cyberspace	Cyberspace defense
Defensive cyberspace operations-internal defensive measures (non-DODIN)	Cyber Protection Force, consisting of national cyberspace protection teams	Non-DODIN friendly cyberspace	Cyberspace defense
Defensive cyberspace operations-response actions	Cyber National Mission Force, consisting of national mission teams supported by national support teams	Neutral and threat cyberspace	Cyberspace attack and cyberspace exploitation
Legend: DODIN Department of Defense information network			

DEFENSE INFORMATION SYSTEMS AGENCY/DEPARTMENT OF DEFENSE CYBER DEFENSE COMMAND

F-31. The Defense Information Systems Agency conducts DODIN operations and defensive cyberspace operations-internal defensive measures missions at the global and enterprise-level within the Defense Information Systems Network, complying with the Commander, USCYBERCOM directives through the Commander, DOD Cyber Defense Command.

F-32. The Defense Information Systems Agency provides engineering, architecture, and provisioning support for integrated DODIN operations, including enterprise management, content management, and digital freedom of maneuver. The Defense Information Systems Agency conducts defensive cyberspace operations-internal defensive measures missions in the joint portion of the DODIN to mitigate vulnerabilities and restore services at the global and enterprise-levels.

F-33. The Director, Defense Information Systems Agency serves in a dual role as Commander, DOD Cyber Defense Command. DOD Cyber Defense Command leads the DOD's unified force approach to DODIN operations (including cybersecurity) and cyberspace defense across DOD networks. In this role, Commander, DOD Cyber Defense Command exercises global command and control to ensure mission assurance. The command's mission covers a broad range of activities on behalf of USCYBERCOM, including proactive, threat-informed steps to reduce cyberspace risk and leading defensive cyberspace operations-response actions to counter threat malicious cyberspace activity against the DODIN.

ARMY ORGANIZATIONS

F-34. In addition to its role as a force provider to the Cyber Mission Force, the Army has certain Service-retained cyberspace and EW forces. These units conduct defined missions to support Army mission requirements.

UNITED STATES ARMY CYBER COMMAND

F-35. ARCYBER serves as the Army Service component command and as a force provider to USCYBERCOM. ARCYBER operates and defends Army networks and delivers cyberspace effects when authorized by USCYBERCOM. ARCYBER develops and deploys cyberspace capabilities for future use against resilient, adaptive threats. ARCYBER is also the designated cybersecurity service provider for the Army.

Army Information Warfare Operations Center

F-36. The Army Information Warfare Operations Center integrates intelligence, fires, space operations, psychological operations, strategic communications, public affairs, special technical operations, cyberspace operations, EW, and military information support operations to create relative information advantages across the competition continuum. The Army Information Warfare Operations Center integrates these information activities across the staff into the command's current operations and plans processes.

F-37. The Army Information Warfare Operations Center maintains global and regional situational understanding of cyberspace while exercising command and control over assigned or allocated Army cyber and information forces.

United States Army Network Enterprise Technology Command

F-38. NETCOM secures, configures, operates, extends, maintains, and sustains the DODIN-A. NETCOM supports defensive cyberspace operations-internal defensive measures to preserve the confidentiality, integrity, and availability of the Army network. NETCOM's core mission encompasses all aspects of unclassified and classified network transport, information sharing, and data storage. NETCOM's Army DODIN Operations Center—

- Exercises technical control of the DODIN-A.
- Oversees operational synchronization of DODIN operations for the Army.
- Provides continuous, real-time monitoring and reporting of global DODIN operations.
- Provides problem identification and resolution across the global network.

Regional Cyber Centers

F-39. Regional cyber centers exercise overall responsibility for protecting the DODIN-A in their assigned areas. Regional cyber centers conduct continuous DODIN operations and enable defensive cyberspace operations-internal defensive measures as needed within their assigned portions of the DODIN-A to ensure Army and joint forces' freedom of action in cyberspace. The regional cyber centers are globally postured in the continental United States, Europe, Korea, Pacific, and Southwest Asia to provide continuous service in each theater of operations. Regional cyber centers are the points of contact for Army forces to report cyber incidents.

Network Enterprise Centers

F-40. The *network enterprise center* is the facility that provides and acquires telecommunications and information management services on Army installations (ATP 6-02.71). Network enterprise centers implement and manage enterprise services (including e-mail, user storage, office automation, collaboration, cloud access, and cybersecurity) according to current policy, procedural guidance, and management procedures.

F-41. A network enterprise center provides overall DODIN operations oversight on its post, camp, station, or joint base, or within a designated geographic area. Local network defenders at the network enterprise center monitor the installation network to detect malicious cyberspace activity and coordinate with the

regional cyber center to implement defensive cyberspace operations-internal defensive measures to neutralize the malicious activity and reconstitute systems.

780th Military Intelligence Brigade (Cyber)

F-42. 780th Military Intelligence Brigade (Cyber) conducts cyberspace operations to deliver effects in support of Army and joint requirements. The brigade's primary objective is to enable and execute cyberspace operations. Elements of the brigade use SIGINT operational tasking authority delegated through Commander, ARCYBER, open source intelligence authority delegated through Commander, INSCOM, and cyberspace collection authorities delegated through Commander, USCYBERCOM to conduct cyberspace intelligence and reconnaissance. The brigade serves as a force provider for ARCYBER and the Cyber National Mission Force.

Cyber Protection Brigades

F-43. The cyber protection brigades defend key terrain in cyberspace to deter threats and ensure freedom of action in cyberspace for friendly forces. The cyber protection brigades organize, train, equip, direct, and deploy cyber protection teams worldwide to augment supported organizations' local network defenders for operations and exercises, and conduct unit cyber defensive readiness assessments and assistance. The cyber protection brigade commander is authorized by standing order to conduct defensive cyberspace operations-internal defensive measures missions to reestablish the security of degraded, compromised, or otherwise threatened friendly cyberspace.

11th Cyber Battalion

F-44. The 11th Cyber Battalion is a scalable cyberspace operations and EW battalion consisting of expeditionary CEMA teams. Expeditionary CEMA teams provide specialized EW and cyberspace effects for supported units against operational and tactical targets. Expeditionary CEMA teams include cyberspace forces, EW personnel, information operations officers, a targeting cell, and intelligence personnel. The 11th Cyber Battalion's intelligence personnel collect information to support internal cyberspace and EW operations and conduct intelligence analysis to support expeditionary CEMA teams.

MULTI-DOMAIN TASK FORCE

F-45. The multi-domain task force is a theater-level element designed to synchronize precision effects and precision fires in all domains against threat antiaccess and area denial capabilities in the air, land, maritime, space, and cyberspace domains and the electromagnetic spectrum. The multi-domain task force plays a key role during competition and crisis to establish conditions in theater for armed conflict. The multi-domain task force is designed to deliver long-range precision joint strike, integrated air and missile defense, EW, space, cyberspace, and information effects.

Operational Priorities

5-148. The multi-domain task force has three main operational priorities in competition: sense and understand the operational environment, demonstrate capability, and synchronize with partners. The multi-domain task force accomplishes these priorities by executing multidomain reconnaissance through—

- Intelligence fusion.
- Multidomain targeting through support to the joint targeting cycle.
- Synchronizing multidomain effects with the integration of multinational partner capabilities.

Multi-Domain Effects Battalion

F-46. The multi-domain task force's multi-domain effects battalion provides cyberspace, EW, space, and information effects to support the task force's larger mission. Multi-domain effects battalion activities in support of combatant command, theater army or joint task force mission objectives include—

- Conducting intelligence collection and analysis.
- Supporting information advantage activities.
- Conducting offensive and defensive cyberspace actions.

- Conducting EW.
- Employing offensive and defensive space operations capabilities.
- Integrating civil affairs and psychological operations capabilities.

F-47. The multi-domain effects battalion employs electromagnetic support and SIGINT sensors and leverages joint and national assets to detect, identify, characterize and geolocate threat communications and non-communications emitters, including weapon systems for targeting with lethal or nonlethal fires. The multi-domain effects battalion's deep sensing capabilities play a key role in developing situational understanding of threats and targeting activities in competition and crisis to support delivery of converged effects to overcome enemy antiaccess and area denial and support joint forcible entry at the onset of armed conflict.

ARMY REPROGRAMMING ANALYSIS TEAM PROGRAM OFFICE

F-48. The Army Reprogramming Analysis Team Program Office is part of the CECOM Software Engineering Center and the Army's designated Service reprogramming center. The Army Reprogramming Analysis Team Program Office—

- Creates and distributes EW reprogramming software for the Army.
- Generates and distributes EW reprogramming messages (see appendix E).
- Supports EW reprogramming products.

Appendix G

Training

This appendix discusses training to prepare Soldiers to execute missions to shape operational environments, prevent conflict, and support large-scale combat operations against peer threats. Training for cyber and electromagnetic warfare Soldiers includes institutional training, continuous home-station training, combat training center rotations, and deployments.

OVERVIEW OF TRAINING

G-1. Commanders ensure Soldiers and units train under challenging and realistic conditions that closely replicate an operational environment while incorporating the Army principles of training (refer to FM 7-0):

- Commanders are the primary trainers.
- Noncommissioned officers train individuals, crews, and small teams and advise commanders on all aspects of training.
- Train using multi-echelon techniques to maximize time and resource efficiency.
- Train as a combined arms team.
- Train to standard using appropriate doctrine.
- Train as you fight.
- Sustain levels of training proficiency over time.
- Train to maintain.
- Fight to train.

G-2. Individual training occurs in all three training domains—institutional, operational, and self-development. Institutional training includes initial and ongoing individual training aligned with each cyber and EW professional's individual development plan. Additionally, Soldiers conduct individual and collective training during home-station training and combat training center rotations to stay abreast of continually evolving techniques, technologies, and trends in cyberspace and the electromagnetic spectrum.

INSTITUTIONAL TRAINING

G-3. Commissioned officers, warrant officers, and enlisted Soldiers seeking a career in cyberspace and EW operations benefit from intensive institutional training before reporting to their first unit of assignment. Institutional training continues throughout these Soldiers' careers. Cyber Common Technical College and Electromagnetic Warfare College reside at the United States Army Cyber School. These colleges provide institutional training to active Army, United States Army Reserve, and Army National Guard cyber and EW Soldiers thorough understanding of cyberspace operations, EW, and associated doctrine.

G-4. Cyber Soldiers learn how to combine Army operations, intelligence, and small unit tactics with foundational skills in cyberspace offensive and defensive tasks. EW Soldiers learn Army operations and small unit tactics with foundational skills in electromagnetic attack, electromagnetic protection, and electromagnetic support. Events conducted during institutional training ensure cyber and EW Soldiers' basic proficiency in their respective military occupational specialties and include such training events as—

- Classroom instruction from civilian and military institutional instructors.
- Training lanes.
- Capstone training events.

HOME-STATION TRAINING

G-5. The CEWO coordinates with other staff elements to conceive and implement an annual home-station training plan. The CEWO aligns home-station training with the unit's mission-essential task list and the essential individual and collective tasks Soldiers must accomplish. The CEWO aligns home-station training with how the unit will operate during evaluations at a combat training center. The home-station training plan

includes subject matter to ensure cyber and EW professionals' continued proficiency in their respective military occupational specialties and can consist of such training events as—

- Classroom training and instruction from mobile training teams.
- Training lanes.
- Field training exercises.

CLASSROOM TRAINING

G-6. Training and instruction from mobile training teams allow cyber and EW Soldiers to meet with military and commercial experts. Mobile training teams provide added real-world insight and practices to establish and maintain professional networks for increased operational efficiency at home station.

G-7. Local network defenders require continual training to maintain perishable skills and remain up-to-date with current threat cyberspace capabilities, tactics, techniques, and procedures. Classroom training for local network defenders should include defensive cyberspace operations-internal defensive measures instruction, including—

- Threat tactics, techniques, and procedures.
- Securing Windows operating systems.
- Computer forensic investigation.
- Incident response.
- Intrusion detection in-depth.
- Hacker techniques.
- Exploit and incident mitigation and prevention.
- Network penetration testing.
- Ethical hacking.
- Auditing networks, perimeters, and information technology systems.

G-8. At a minimum, classroom training for EW Soldiers should include—

- General mathematics and algebra.
- Radio frequency fundamentals and calculations.
- Antenna theory.
- Direction-finding fundamentals.
- Principles of detecting and identifying frequencies of interest.
- Compilation of EW running estimates.
- Joint spectrum interference resolution and electromagnetic interference reporting procedures.
- Digital signal processing.
- Electromagnetic Warfare Planning and Management Tool familiarity and scenario planning.
- Fundamentals of maneuver.
- Threat EW capabilities.
- Visual identification of threat vehicles and EW systems.

LANE TRAINING

G-9. Training lanes provide cyber and EW Soldiers the opportunity to exercise combined efforts that culminate home-station training and assist with ensuring unit readiness and survivability. Training lanes can include simulated communications jamming to emphasize the importance of primary, alternate, contingency, and emergency communication plans. Subordinate units can use information from training events by conducting after action reviews to develop primary, alternate, contingency, and emergency communication plans.

FIELD TRAINING EXERCISES

G-10. Most field training exercises will not include a cyber opposing force, so the opportunity to practice defensive cyberspace operations are limited. During field training exercises, local network defenders maintain the network's cybersecurity compliance. Units practice electromagnetic protection actions during exercises, including—

- Terrain masking.

- Camouflage net masking.
- EMCON—
  - Limiting electromagnetic emissions.
  - Exercising EMCON plans, including triggers and transitions between EMCON conditions.

COMBAT TRAINING CENTERS

G-11. Combat training center rotations simulate real-world operations by imitating conditions units may encounter during deployment. The combat training center opposing force imposes realistic threat tactics, techniques, and procedures on units. Combat training centers evaluate rotational training units for combat readiness determined by the proactive and reactive measures taken to prevent or mitigate obstacles presented during the training rotation.

G-12. In a combined arms training scenario, cyberspace and EW operations are essential to gaining and maintaining tactical advantages needed for a favorable resolution. Combat training centers continuously observe the rotational training unit's performance in an operational environment that includes simulated conflict and competition. Combat training centers help commanders assess their units' overall combat readiness; proficiency in mission-essential tasks; and those critical and essential tasks that require additional training. Commanders oversee the implementation of necessary changes during home-station training to improve their units' proficiency.

This page intentionally left blank.

Appendix H

Network Hardening Guide

The network hardening guide organizes procedures around four distinct but interrelated areas: domain management and security; network device management and security; network traffic monitoring and alerts; and endpoint (host and server) security. This guide should provide a unit the necessary tools to conduct a risk-based assessment of its cybersecurity posture.

SECTION I – DOMAIN MANAGEMENT AND SECURITY

OVERVIEW

H-1. Configuring a hardened tactical network requires both time and technical expertise to apply cybersecurity measures using a variety of tools and security devices. There is no formal template for the implementation and configuration of these tools and devices. The guide in this appendix provides units to help establish their cybersecurity baseline.

CREATE AND DESIGN ORGANIZATIONAL UNIT

H-2. 'Organizational unit' is a construct used to represent an organization whose resources are logically separate from resources of other, similar organizations. Network administrators use organizational units to control access to system resources and segregate data according to sensitivity and access rights. Creating and designing an organizational unit assists administrators to logically group users, computers, and other objects. This enables the targeted application of cybersecurity policies and access controls to specific groups based on function or department and minimizes the risk of unauthorized access and simplifies security management.

H-3. A brigade combat team should consist of one domain assigned by the Defense Information Systems Agency. Domain administrators should reside in the brigade combat team S-6. Battalion S-6s should not be given domain administrator credentials to prevent them inadvertently erasing the brigade domain.

H-4. Each battalion in the brigade combat team should be a subordinate organizational unit in the brigade domain. System administrators in the battalion S-6 should have delegated control over their respective subordinate organizational units. Within each organizational unit, there should be three standardized primary subordinate organizational units:

- Users—every user assigned to the battalion organizational unit.
- Computers—every workstation that belongs to the organizational unit.
- Groups (otherwise known as security groups)—provide a mechanism to create sub-organizations within the organizational unit to provide access to resources on a least-privilege basis.

H-5. Users, besides existing within the 'users' organizational unit will be nested within appropriate groups within the 'groups' organizational unit. System administrators should be designated in a security group to grant them the appropriate elevated permissions separate from other users. The administrator steps to design and create an organizational unit are—

- Assign users.
- Assign computers.
- Join computers to the domain.
- Create security groups and assign users.
- Delegate control.

SECURITY ACCESS

H-6. Security access manages and controls who can access sensitive systems, networks, and data. This ensures only authorized users can access network resources while preventing unauthorized users from gaining entry to devices or the network. Identity, credential, and access management helps protect against cyberspace risks such as data breaches and unauthorized access. Administrators should grant system access

based on least privilege through role-based authentication. In establishing security access controls, administrators configure—

- Security group access to folders.
- Security group access to printers.
- File enumeration policy.

Note. To enforce least privilege access, standard users should only be given 'read,' 'read and execute,' and 'list folder contents' permissions. 'Read and execute' permissions allow users to create, modify, and save documents. These users can only delete files they created.

SECURITY GROUP ACCESS TO A FOLDER

H-7. Administrators should be given 'modify' permissions. Only the domain administrator should be granted 'full control' permissions. Full control allows a user to delete folders and all their contents. Deleted folders are unrecoverable.

SECURITY GROUP ACCESS TO A PRINTER

H-8. To access a networked printer, users need to be part of a security group with assigned print permissions. Security group access to a printer allows the administrator to control which users or devices on a network can access the shared printer. This prevents unauthorized individuals from printing sensitive documents and mitigates potential data leaks commonly associated with open printer access.

FILE ENUMERATION POLICY

H-9. File enumeration limits access to files and folders based on a user's role and need to know. A file enumeration property ensures that users can only see files and folders to which they have been granted security permission.

FILE SERVER RESOURCE MANAGER

H-10. The File Server Resource Manager is a set of tools in Windows Server that help administrators manage stored data on file servers. The File Server Resource Manager allows administrators to manage file storage quotas, file screens (the types of files a user can store), and storage reports (to identify trends and misuse of space). This allows administrators to automatically manage access to sensitive files, effectively limiting vulnerabilities related to data storage and unauthorized access. File Server Resource Manager elements include—

- Quota management.
- File screening.
- Storage reports.

QUOTA MANAGEMENT

H-11. Recommended storage allocation for staff sections depends on the level of usage anticipated for each section and the total file storage space available. Quota management allows administrators to limit the amount of server storage space for users. Examples include hard limit, template-based, auto apply, and size limit quotas.

FILE SCREENING

H-12. In custom properties, the administrator can select either active or passive file screening. Active screening blocks access and passive screening logs the access. Administrators can also configure notification thresholds and properties similar to quota management.

STORAGE REPORTS

H-13. Storage reports graph how much space is in use in each folder relative to its capacity and storage trends over time. These reports provide comprehensive views of disk space consumption across different folders and users on a file server. This can highlight potential storage issues as users approach their quota limits.

DISTRIBUTED FILE SYSTEM (SHARED DRIVES)

H-14. A distributed file system allows users to access files from multiple servers or locations. Distributed file systems store and manage data across the network. This distributes data across multiple servers, increasing redundancy when faced with server failure, and prevents unauthorized access and data loss from a single point of failure through encryption, access control, and data replication. It also allows users to share and work from the same version of a file.

PRINT SERVERS

H-15. Print servers act as security gateways to help prevent unauthorized access. They allow administrators to centrally manage printers for the domain and limit unauthorized access to the network via a printer. Print servers centrally manage printer access and allow administrators to implement user authentication, encryption, and print job tracking.

GROUP POLICY OBJECTS

H-16. A group policy object is a collection of policy settings. Group policy objects restrict actions a user can perform on a workstation and the actions a workstation can perform on a domain. Establishing group policy objects allows administrators to centrally enforce cybersecurity policies across all users and machines within a domain, effectively preventing unauthorized access and maintaining consistent security configurations.

H-17. A best practice is to create one group policy object per rule to be implemented. It is generally inadvisable to establish one group policy object to apply all rules because of undue complexity and single points of failure. Domain administrators should apply these group policy objects to the network:

- Disable wireless access.
- Disable command prompt.
- Disable power shell.

DISABLE WIRELESS ACCESS

H-18. Disabling wireless access prevents unauthorized users from connecting to Wi-Fi access points and restricted networks. Disabling access helps mitigate risks of data breaches and unauthorized access to sensitive information.

DISABLE COMMAND PROMPT

H-19. Disabling the command prompt prevents users from executing system commands. This helps eliminate potential compromises in security and allows only authorized administrators to access advanced system functions.

DISABLE POWER SHELL

H-20. Disabling the PowerShell function enhances security by limiting access to tools that can be exploited by malicious actors. This is important for users who do not require advanced system administration capabilities and allows the administrator to implement least privilege access.

Note. Administrators should be in a separate organizational unit to allow them to execute PowerShell scripts. This organizational unit will only work for PowerShell version 5 or higher.

FOLDER REDIRECTION

H-21. Folder redirection automatically routes standard folders to a different storage location. Folder redirection allows data created by key users to be saved to a server so they can access their data on any workstation within the domain. This centralizes user data on a network server, allowing for stricter access control, easier backups, and reduced risk of data loss. The domain administrator should establish folder redirection for identified key personnel in the brigade.

- Commander.
- Command sergeant major.

- Executive officer.
- S-3.
- Battalion commanders.

READ-ONLY DOMAIN CONTROLLER

H-22. A read-only domain controller hosts a copy of the Active Directory database without the ability to add or change entries. A read-only domain controller serves locations that cannot adequately secure a full domain controller. The read-only domain controller reduces the attack surface and mitigates the risk of unauthorized changes to user accounts or critical system settings.

DEPLOYMENT

H-23. Read-only domain controllers are generally deployed for the following reasons:

- Physical security is not guaranteed in an austere or remote environment. If a malicious actor manages to access a read-only domain controller, they cannot make database changes. If they somehow change the database, they cannot compromise Active Directory because those changes do not replicate to writable domain controllers.
- Most battalion S-6 sections lack sufficient personnel with the required information technology certifications to maintain writable domain controllers. Since a read-only domain controller only provides user authentication, it does not have the same ongoing maintenance requirements (such as hardware updates, site-link changes, and user credential changes) as a writable domain controller.
- Some remote units have poor network connectivity or low bandwidth to the brigade network infrastructure. In this instance, a read-only domain controller is deployed so the remote users need not authenticate themselves from the writable domain controller over the wide-area network. This reduces the time required for remote users to log on.

ALLOWED AND DENIED PASSWORD REPLICATION GROUPS

H-24. A read-only domain controller communicates with a writable domain controller for user authentication because by default, account credentials are not cached locally on a replication group. If branch office users from the replication group log in, they are authenticated locally if their credentials are already cached. For security purposes, to prevent privileged users (domain and enterprise administrators) from being cached locally on a read-only domain controller, they are normally added to a denied password replication group.

READ-ONLY DOMAIN CONTROLLER PREREQUISITES

H-25. Before installing and configuring a read-only domain controller, the domain administrator should ensure—

- The administrator account has a strong password.
- Static Internet Protocol is configured.
- The latest Microsoft updates are installed.
- Firewall is turned off.
- Domain Name System server Internet Protocol address properties are correct and point to a writable domain controller. To verify, the administrator resolves the domain name from command prompt.

INSTALLATION AND CONFIGURATION

H-26. This process enhances network security in remote locations where physical security is considered weak. Installing and configuring the read-only domain controller helps to prevent unauthorized users from modifying sensitive Active Directory data by only allowing read access to the domain information.

CONFIGURATION TESTING

H-27. Once the domain administrator configures and reboots the read-only domain controller, they should test and verify the configuration. The administrator should verify—

- Connection to the read-only domain controller and not a writable domain controller.
- They cannot create or delete accounts.
- Related grayed out (non-selectable) icons.

- Allowed and denied password replication groups.

TEST ENVIRONMENT FOR GROUP POLICY OBJECTS AND SECURITY CHANGES

H-28. A test environment allows administrators to change group policy objects and security settings without affecting the active security domain. This allows administrators to safely evaluate the impact of planned configuration changes offline before deploying them on the network. By using a test environment, administrators can minimize disruptions or security vulnerabilities when deploying updates across the network.

H-29. After the new Active Directory domain is established, administrators should create an object in the test environment to evaluate the effects of the planned changes. When an object is added to the appropriate organizational unit, the administrator should apply security controls only to the organization to ensure test changes do not propagate across the entire domain.

LOCAL CHANGE CONTROL BOARD

H-30. A local change control board reviews and approves proposed changes to the network. A local change control board helps the S-6 section manage and control changes to balance network functionality and security. Well-documented changes assist in troubleshooting network problems when they arise. The local change control board ensures proposed changes are carefully reviewed, assessed, and approved before implementation. The local change control board mitigates the risk of unauthorized modifications that could compromise network security.

SECTION II – NETWORK DEVICE MANAGEMENT AND SECURITY

SOLAR WINDS NETWORK CONFIGURATION MANAGER

H-31. SolarWinds provides information technology infrastructure management software and services. SolarWinds helps organizations plan, manage, and optimize cloud environments. SolarWinds helps identify potential security breaches, investigate suspicious activity, and mitigate threats. SolarWinds includes a suite of software tools that enable—

- Continuous monitoring of network activity.
- Log collection.
- Vulnerability analysis.
- Automated response.

H-32. SolarWinds Network Configuration Manager can be configured either through auto-discovery or manually. This streamlines network device configuration management and helps information technology teams track, compare, and modify configurations across various network devices.

AUTO-DISCOVERY METHOD

H-33. Auto-discovery maps the network infrastructure across different environments automatically. Auto-discovery—

- Saves time by eliminating the need to manually enter device configurations.
- Provides a comprehensive view of the network topology.
- Enables proactive monitoring of devices and potential issues.

H-34. Disadvantages of auto-discovery include—

- Potential inaccuracies in discovered data.
- Network impact from scanning.
- Less granular control over monitored devices.

MANUAL CONFIGURATION

H-35. While SolarWinds is primarily designed for automatic network configuration, administrators may choose to configure devices manually. This is beneficial when quick, specific changes are required or when dealing with unique device configurations not supported by auto-discovery. Conversely, manual configuration can be time-consuming, is susceptible to data input errors, and suffers from inconsistency across the network, which may result in security vulnerabilities or operational inefficiencies.

UNIFIED THREAT MANAGEMENT

H-36. Unified Threat Management combines multiple network security features into a single device. This consolidates security features such as firewalls, antivirus, content filtering, and intrusion detection. By consolidating these features, Unified Threat Management allows centralized management and monitoring and simplifies comprehensive network protection. There are four methods to configure Unified Threat Management:

- Add from network (auto-discovery).
- Add new device (manual).
- Load from comma-separated values file.
- Load from a text configuration file.

ADD FROM NETWORK (AUTO-DISCOVERY)

H-37. Auto-discovery will only detect routers using Cisco Internetwork Operating System up to version 12.3. This method is typically used when the administrator wants to automatically identify and configure network devices within the target network, streamlining the setup process by detecting available devices and their settings. Auto-discovery can lead to over-detection of devices and network traffic, which may result in unnecessary alerts and degraded network performance.

ADD NEW DEVICE (MANUAL)

H-38. Manual addition works regardless of whether the device is active on the network. Manually adding devices may be required for highly specialized configurations, legacy systems integration, or when faced with cost constraints. Drawbacks to using this method can include increased complexity, inefficient monitoring, and the possibility of misconfiguration.

ADD DEVICE FROM COMMA-SEPARATED VALUES FILE

H-39. Add from file adds devices to the network security system by importing the details from a comma-separated values file. Adding a device from a file helps streamline configuration by bulk importing device settings. This method is popular because the data is human-readable. Some disadvantages include the creation of a single point of failure, less than granular settings, and overreliance on a single service provider.

ADD DEVICE FROM CONFIGURATION FILE

H-40. Add from configuration file adds devices to the network security system by importing the details from a text file. Adding a device from configuration file streamlines configuration of multiple devices by bulk importing device settings. This method can work with most Windows machines, typically using the Microsoft Notepad application. Disadvantages include creating a possible single point of failure, less granular settings, and overreliance on a single service provider.

CURRENT DEVICE CONFIGURATIONS

H-41. Administrators should load the current configurations of network devices in Unified Threat Management. This establishes the baseline configuration of Internet Protocol addresses, subnet masks, default gateways, Domain Name System servers, and other configuration settings. Documenting current device configurations ensures all devices—

- Follow the latest security protocols.
- Have updated firmware installed.
- Have unnecessary or unauthorized services disabled.

CONFIGURE LAYER 2 SECURITY FEATURES

H-42. Layer 2 security features control which devices can access the network. This provides a critical layer of protection against network attacks. Layer 2 security features help control access to the network switch level and prevent unauthorized devices from connecting to the protected network. This helps isolate network segments and limit the impact of breaches. Layer 2 security features include—

- Dynamic Host Configuration Protocol helper address.
- Dynamic Host Configuration Protocol snooping.
- Dynamic Address Resolution Protocol inspection for Dynamic Host Configuration Protocol-enabled networks.
- Dynamic Address Resolution Protocol inspection for non-Dynamic Host Configuration Protocol networks.
- Port security features.

DYNAMIC HOST CONFIGURATION PROTOCOL HELPER ADDRESS

H-43. Administrators should configure a Dynamic Host Configuration Protocol helper address on each network switch to let those devices know where to find the trusted Dynamic Host Configuration Protocol server. The helper address can be configured either through the SolarWinds Network Configuration Manager or individually on each device.

DYNAMIC HOST CONFIGURATION PROTOCOL SNOOPING

H-44. This process will eliminate the possibility of having a rogue Dynamic Host Configuration Protocol server assigning Internet Protocol addresses to clients on the network. The switch will only trust packets coming from an authorized source (tier 2 router or switch).

DYNAMIC ADDRESS RESOLUTION PROTOCOL INSPECTION FOR DYNAMIC HOST CONFIGURATION PROTOCOL ENABLED NETWORKS

H-45. Dynamic Address Resolution Protocol Inspection (DAI) is a layer 2 security feature that prevents Address Resolution Protocol spoofing or cache poisoning attacks. DAI relies on Dynamic Host Configuration Protocol snooping to build a database of trusted Internet Protocol and media access control address pairs for validation of Address Resolution Protocol requests.

H-46. Dynamic Host Configuration Protocol snooping must be configured before implementing DAI (see paragraph H-47 for configuring DAI on networks that do not use Dynamic Host Configuration Protocol). DAI is applied to specific virtual local area networks and relies on specifying trusted and untrusted interfaces. With DAI enabled, interfaces are configured as untrusted (meaning that DAI will be applied) by default. To ensure traffic can still flow, it is necessary to configure trunked interfaces (interfaces to higher switches) as trusted interfaces. If an interface is trusted, no inspection will take place. Access ports associated with the target virtual local area network should remain untrusted. This configuration implies that DAI should occur only once at the lowest level switch a user connects through. It is important that all switches in the same virtual local area network have DAI configured to minimize security gaps.

DYNAMIC ADDRESS RESOLUTION PROTOCOL INSPECTION FOR NON-DYNAMIC HOST CONFIGURATION PROTOCOL NETWORKS

H-47. In the case of a network configured without Dynamic Host Configuration Protocol, it is still possible to configure DAI using Address Resolution Protocol access control lists. Access control lists allow the administrator to statically specify Internet Protocol and media access control address pairs that create the trusted database to validate requests and connections.

H-48. If devices are already present on the network, the easiest method to generate an access control list is to pull the Address Resolution Protocol cache on the tier 2 switch and filter entries by the desired virtual local area network for implementation. This can be accomplished via a script or manually, depending on network restrictions. If attempting to implement DAI before the network is active, Internet Protocol and media access control address pairs should be designated from the unit's Lightweight Directory Access Protocol Data Interchange Format. Media access control addresses for each workstation should be recorded during imaging.

PORT SECURITY FEATURES

H-49. A best practice for access ports is to implement the sticky media access control security feature with a limit of three learnable media access control addresses—this allows for an Internet Protocol telephone attached to a workstation. The port should be configured for shutdown upon violation. Additionally, implementing Bridge Protocol Data Unit guard on access ports prevents connection of unauthorized switches or extensions to the network.

ADDITIONAL LAYER 2 SECURITY CONFIGURATIONS

H-50. Additional layer 2 security configurations control which devices can access the network. This protects against network attacks by controlling access to network switches to prevent unauthorized device connections. This helps isolate network segments and limits the impact of breaches.

H-51. Certain layer 2 security features should be pre-configured on network systems. Administrators should verify these configurations to ensure they comply with best practices. Key layer 2 security configurations include—

- Type 7 passwords.
- Simple Network Management Protocol strings.
- Simple Network Management Protocol traps and poll times.
- Policy-based routing.

TYPE 7 PASSWORDS

H-52. If Type 7 passwords are cryptologically broken, it is possible to enter any type 7 password hash into various online sources and find the corresponding plain text value. At the beginning of router and switch configuration, the administrator should check the properties of every username and password assigned to the system.

SIMPLE NETWORK MANAGEMENT PROTOCOL STRINGS

H-53. During equipment fielding, equipment is generally configured with Simple Network Management Protocol login credentials with pre-formatted, easy to social-engineer passwords. Factory default administrator passwords for many network appliances and systems are easily discoverable by a simple Internet search. Administrators must change these passwords from the fielded default. Additionally, Simple Network Management Protocol strings named ‘public’ and ‘private’ must be removed for all devices on the network, including printers.

Note. Cybersecurity rules require changing vendor default passwords on all network devices. Even though program managers generally change passwords on routers and switches from the factory defaults when fielding commercial off-the-shelf equipment, this rule still applies to the program manager-applied default passwords.

SIMPLE NETWORK MANAGEMENT PROTOCOL TRAPS AND POLL TIMES

H-54. Simple Network Management Protocol traps specify the level of information sent to the viewer. As a best practice, if the network can support the bandwidth (generally minimal), Simple Network Management Protocol traps should be enabled on the network.

POLICY-BASED ROUTING

H-55. Policy-based routing should be set by default on tactical communications systems. If it is not, the administrator should contact the field service representative or program manager for the default settings. Configuring policy-based routing is beyond the skill set of most brigade networking technicians.

SECTION III – NETWORK TRAFFIC MONITORING AND ALERTS

NETFLOW TRAFFIC ANALYZER

H-56. NetFlow Traffic Analyzer provides a deeper understanding of network activity. It achieves this by examining data gathered from various network devices. By collecting detailed information about network traffic, NetFlow offers valuable insights into patterns and trends. NetFlow Traffic Analyzer helps administrators identify unusual or unexpected traffic patterns, that might indicate malicious cyberspace activity. This enables the detection and mitigation of security exploits, such as unauthorized access attempts or data breaches. It also helps identify vulnerabilities within the network infrastructure, allowing for timely remediation and strengthening overall security posture. NetFlow Traffic Analyzer uses Cisco's NetFlow Protocol to detect and record information about the data flowing through the network. This tool helps network administrators understand how data moves within the network. By looking at the data map, administrators can—

- Identify problems: They can see unusual patterns or suspicious activity that might indicate a hacker or a network issue.
- Prevent security breaches: By identifying vulnerabilities, they can take steps to protect the network from attacks.
- Improve performance: Understanding traffic patterns helps them optimize the network for better speed and efficiency.

H-57. Administrators can set up NetFlow Traffic Analyzer through either—

- Auto-discovery—the tool can search and connect to network devices on its own.
- Manual setup—administrators can manually input the information for each device.

AUTO-DISCOVERY

H-58. Auto-discovery streamlines setup of network monitoring. This method automatically identifies and integrates network devices. By eliminating the need to manually configure each device, auto-discovery significantly reduces the time and effort required for implementation. This simplifies setup and enhances the system's scalability, allowing for easier management of expanding networks.

H-59. Despite its advantages, auto-discovery has certain limitations. There is a possibility of inaccurate data collection due to device compatibility issues or misconfiguration. Initial setup for auto-discovery can be complex, requiring careful configuration to ensure accurate device identification. Additionally, auto-discovery may impact network performance due to the increased volume of data being processed. Finally, there is a risk of false negatives, where legitimate traffic is mis-identified as suspicious, or false positives, where malicious activity goes undetected. Administrators must carefully weigh these potential drawbacks against the benefits of simplified setup and increased scalability. Auto-discovery allows the tool to automatically find and connect to any device on the network that can send NetFlow data. Auto-discovery has both advantages and drawbacks:

- **Advantages—**
  - Simplifies network setup—administrators do not have to manually connect each device, saving time and effort.
  - Fast and easy monitoring—auto-discovery makes it much quicker to start monitoring network traffic.
  - Better network view—auto-discovery can easily handle a large number of devices, giving a clearer picture of the entire network.
- **Drawbacks—**
  - Potential for errors—the auto-discovery feature can misinterpret information, leading to inaccurate data.
  - Tricky initial setup—initially getting the auto-discovery feature working correctly place can be complicated.
  - Performance hiccups—the automatic search for devices might slow down the network during discovery.
  - False alarms—there is a chance of getting false alarms—the tool might flag something as a problem when it is not, or it might miss a real issue.

MANUAL

H-60. Manually configuring NetFlow Traffic Analyzer requires an administrator to individually set up each network device. This setup involves instructing each device to transmit its NetFlow data to a designated collector, which aggregates and analyzes the information.

H-61. Manual configuration offers some advantages. It provides administrators with granular control over the data collection process. Additionally, isolating potential issues becomes easier since each device is configured independently.

H-62. However, manual configuration also presents some drawbacks. It requires more resources in terms of time and personnel. Configuring each device individually can be time-consuming, particularly in large networks. Manual configuration offers administrators more control over data collection. This approach requires individually configuring each network device to specify the transmission of NetFlow data to a designated collector. The primary advantage of manual configuration lies in its granularity. Administrators can meticulously define data points collected from each device, tailoring the monitoring system to their unique requirements. This facilitates troubleshooting by isolating specific network segments or devices for analysis.

H-63. However, the manual configuration method does come with certain drawbacks. It is labor-intensive to implement, particularly in large and complex networks. The time required for manual configuration increases proportionally with the number of devices, making it less scalable compared to auto-discovery.

Note. When using the manual configuration, each device must be physically connected to the network and powered on. Only then will the device appear within the NetFlow Traffic Analyzer interface, allowing for configuration.

CONFIGURING DEVICES TO SEND LOG ENTRIES AND ALERTS

H-64. Configuring network devices to transmit log entries and alerts to a central system logging protocol (syslog) server is an important aspect of network management. This information can include log entries, alerts, system messages, and various notifications. Centralizing this data offers several advantages:

- Efficient troubleshooting—by reviewing the sequence of events recorded in logs, administrators can swiftly identify the root cause of network problems.
- Performance monitoring—analyzing device logs allows administrators to monitor performance metrics and ensure optimal network health.
- Compliance adherence—maintaining comprehensive logs is often essential for meeting cybersecurity compliance requirements.
- Centralized management—consolidating logs from multiple devices into a single location simplifies network management tasks.
- Proactive issue response—timely alerts notify administrators of critical issues requiring immediate attention.

H-65. As a starting point, administrators should configure NetFlow on the outbound interfaces of tier 2 routers. This initial setup allows for an assessment of network activity and helps determine whether further expansion is necessary. Domain controllers and client devices do not require this configuration. Administrators need login credentials for Enterprise Security Manager to access and manage the collected data effectively to accomplish this configuration.

CONNECTORS IN ENTERPRISE SECURITY MANAGER

H-66. Connectors are essential software components within Enterprise Security Manager that facilitate communication between the platform and various devices within the unit's portion of the network. These connectors allow the domain manager to interact with and gather information from diverse devices and applications. By establishing these connector configurations, organizations can leverage the full capabilities of Enterprise Security Manager for proactive threat detection and response.

H-67. Domain managers use connectors to collect device logs and alerts. These connectors establish secure and authenticated communication channels, ensuring the confidentiality and integrity of data transmitted between the devices and Enterprise Security Manager.

H-68. This secure communication enhances network security. By aggregating and analyzing logs and alerts from various sources, Enterprise Security Manager can effectively detect and respond to potentially malicious cyberspace activity in a coordinated manner. Domain managers should prioritize configuring connectors for—

- Routers and switches—these network infrastructure devices provide valuable insights into network traffic patterns and potential anomalies.
- Domain controllers and clients (syslog)—integrating domain controllers and client devices via syslog connectors enables comprehensive monitoring of user activity and system events.

ROUTERS AND SWITCHES

H-69. Connectors on routers and switches facilitate secure collection and transmission of network traffic data to the Enterprise Security Manager. This allows monitoring and analysis of network activity for security risks by providing detailed visibility into network communications across different devices.

DOMAIN CONTROLLERS AND CLIENTS (SYSLOG)

H-70. A key connector in many enterprise environments is the Active Directory connector. Active Directory functions as a proxy service, facilitating communication between cloud-based applications and the unit's Active Directory domain controllers.

H-71. The Active Directory connector plays a vital role in user authentication and data access. When a user attempts to access a cloud application integrated with this connector, the connector acts as an intermediary. Instead of requiring a direct connection to the unit domain controller, the cloud application communicates with the connector. The connector, in turn, securely queries the domain controllers to verify the user's credentials and retrieve necessary information.

H-72. This architecture enhances security by eliminating the need for direct connections between cloud applications and sensitive unit systems. It also simplifies access management for cloud applications by leveraging the existing user accounts and permissions stored in the unit's Active Directory server.

Note. Administrator credentials are required to retrieve syslog data from devices. The domain manager should connect the device before finalizing settings to ensure Enterprise Security Manager can communicate with the device.

ENTERPRISE SECURITY MANAGER LOG FORWARDING

H-73. Enterprise Security Manager automatically sends security logs to a central location for analysis and monitoring. This allows the organizational unit to centrally collect security logs. The domain manager configures Enterprise Security Manager for log forwarding to the regional cyber center or higher-echelon network operations and security center. Log forwarding enables—

- Monitoring for malicious cyberspace activity
- Analysis of security incidents and events.
- A single point of visibility to monitor cybersecurity compliance.

Note. Firewall modifications are generally required to forward Enterprise Security Manager logs to the regional cyber center or higher-level command.

ENTERPRISE SECURITY MANAGER ALERTS AND DASHBOARD CONFIGURATIONS

H-74. Enterprise Security Manager alerts and dashboard configurations allow for the monitoring of key security areas such as—

- Network traffic.
- User activity.
- System events.
- Malicious cyberspace activity.

H-75. Alerts and dashboard configurations allow security teams to visualize critical information, prioritize alerts, and investigate possible malicious cyberspace activity. Alerts help determine patterns, activity, and other suspicious behavior. Dashboards display real-time information for analysis and response. There are five primary Enterprise Security Manager dashboards cybersecurity personnel should examine on a regular basis.

- Triggered alarms.
- Asset threat summary.
- Recent threat summary.
- Vulnerability summary.
- Event analysis dashboard.

TRIGGERED ALARMS

H-76. The triggered alarms may indicate malicious cyberspace activity that poses a risk to local systems. For example, a triggered alarm may indicate a denial-of-service attempt. When examining individual events, the domain manager can create a case to enter notes and information about the event.

ASSET THREAT SUMMARY

H-77. The asset threat summary view should normally be blank. If something appears, that item requires immediate investigation and communication to the regional cyber center or higher echelon network operations and security center.

RECENT THREAT SUMMARY

H-78. The recent threat summary view should normally be blank. If something appears, that item requires immediate investigation and communication to the regional cyber center or higher echelon network operations and security center.

VULNERABILITY SUMMARY

H-79. The vulnerability summary view displays a consolidated list of security alerts on the network to identify vulnerabilities. The data is displayed on a dashboard with key metrics and insights to help prioritize remediation efforts and improve the unit's cybersecurity posture.

EVENT ANALYSIS DASHBOARD

H-80. Domain managers can apply event filters to separate benign events versus malicious events. Domain managers can apply event filters to parse out benign versus malicious events. The event analysis dashboard provides a comprehensive view of security events within a system, highlighting both logged and blocked activities. This dashboard offers a more detailed alternative to the triggered alarms dashboard. Domain managers can apply event filters to differentiate between harmless and potentially harmful events. This enables them to identify and prioritize security risks, facilitating timely investigation and response.

SECURITY ONION

H-81. Security Onion is an open-source Linux distribution for intrusion detection, enterprise security monitoring, and log management that is approved for use on Army Systems. Security Onion detects malicious cyberspace activity before it can cause significant damage. It is built on a modified distributed client-server model. Security Onion provides a comprehensive security monitoring platform that allows network security teams to identify and investigate possible malicious cyberspace activity in real-time.

SECTION IV – ENDPOINT SECURITY

H-82. Host Based Security System secures individual network and end user devices. This allows network managers to monitor and manage all devices on the network. Network administrators should pre-configure Host Based Security System agents to a standard workstation image. Host Based Security System secures individual network and end user This allows network managers to monitor and manage all devices on the network. Network administrators should pre-configure Host Based Security System agents to a standard workstation image.

HOST BASED SECURITY SYSTEM DEPLOYMENT

H-83. If the Host Based Security System agent does not point to the correct ePolicy Orchestrator server, it will not receive updates or communicate alerts. A misconfigured Host Based Security System agent requires reconfiguring the client installations across the entire domain. Rule sets associated with Host Based Security System are generally managed by echelons above brigade. For detailed instructions for deploying Host Based Security System, refer to the cybersecurity tools section on the Cyber Lessons and Best Practices Website.

HOST BASED SECURITY SYSTEM DASHBOARDS

H-84. Dashboards display real-time data and insights into the security status of individual network devices. Dashboards help administrators identify possible malicious cyberspace activity and enable timely intervention and remediation.

H-85. There are multiple views or dashboards that can be configured in Host Based Security System. With the standard dashboards, administrators can create filters to display alerts for the most important information. Administrators can also configure custom dashboards.

Note. The effectiveness of a dashboard is dependent on properly configuring the host agents that report to the ePolicy Orchestrator server.

H-86. In its default configuration, the threat events view displays possible malicious cyberspace activity—instances that have triggered an alert or blocked an action. Typical filters that can be applied to this dashboard include filtering by event generated time (for example, 1 day, 1 week, or 1 month), or event type. Building filters should be done over time as traffic and alerts are identified as benign or malicious. Administrators should configure alerts so that identified benign events no longer display.

ASSURED COMPLIANCE ASSESSMENT SOLUTION DEPLOYMENT AND SCANNING

H-87. Assured Compliance Assessment Solution consists of two primary components—Security Center and Nessus Scanners. These components allow an organizational unit to identify and assess security vulnerabilities. Assured compliance measures provide detailed information about vulnerabilities, enabling their prioritization and remediation. This improves the security posture and cybersecurity compliance of the network.

H-88. Security Center resides on a virtual server in the network operations and security center. The Security Center deployment in the network operations and security center also has a Nessus scanner. Nessus Scanners are installed on virtual machines on every major networking assemblage at the battalion and brigade.

INSTALLATION AND CONFIGURATION

H-89. Administrators configure Assured Compliance Assessment Solution to scan systems for vulnerabilities and assess the system for cybersecurity compliance. Installation and configuration involve—

- Deploying Assured Compliance Assessment Solution software on a network.
- Defining scanning targets.
- Configuring compliance checks.
- Establishing reporting mechanisms to monitor and remediate security issues.

Installing Security Center and Nessus Scanners

H-90. The administrator should download the latest system image from the Department of Defense Patch Repository Website before installing. Installing both supports the Security Center which controls and consolidates vulnerability scan data from multiple Nessus scanners across the network. This allows centralized viewing, analysis, and prioritization of cybersecurity risks.

Setting up Scan Zones and Nessus Scans

H-91. Scan zones should align with the subnets allocated across the local domain. Administrators must assign which scanner will cover each zone.

BEST PRACTICES

H-92. When establishing a network baseline, daily scanning is likely necessary to achieve compliance. Once an acceptable baseline is achieved, weekly Assured Compliance Assessment Solution scans may be sufficient, subject to the network administrator's battle rhythm and operating tempo.

Plug-Ins

H-93. Plug-ins are snippets of code that determine what is picked up in a scan. Administrators should download updated plug-ins weekly. When uploading plug-ins to Security Center it is better to check for updated .tar files rather than downloading all plug-ins. When pushing updates from Security Center in a bandwidth-limited environment, it is generally a best practice to ensure automatic updates are activated on only one scanner at a time and to update each subordinate scanner individually.

Enabling and Disabling Automatic Updates

H-94. Enabling automatic updates helps ensure compliance with cybersecurity standards and minimizes the amount of time the network is exposed to a potential exploit. Automatic updates keep the system up to date with the latest security patches and detection capabilities.

Checking Compliance

H-95. The vulnerability summary checks cybersecurity compliance across multiple scans. It also allows administrators to identify trends, such as an increase or decrease in the number of vulnerabilities identified over time. Using Assured Compliance Assessment Solution, units can proactively assess their cybersecurity posture against security technical implementation guides. These guides provide a framework of best practices and security controls that organizations should implement to mitigate risks effectively.

Exporting Vulnerability Lists

H-96. Administrators can export vulnerability lists as .csv files to give consolidated lists and groups of computers to subordinate echelons to employ multiple patches on a single restart. Firewalls must be adjusted to allow scanning on port 8834 throughout the network. This allows Security Center to communicate with Nessus Scanners.

H-97. Factory service representative-managed command and control information systems are problematic to patch. Quarterly updates are often delayed, which may leave multiple unpatched vulnerabilities on the system until the next update.

Enforcing Subordinate Cybersecurity Compliance

H-98. A useful technique to enforce compliance in subordinate units is calling them periodically to check their progress and help them through any issues. This may seem obvious but is often overlooked.

PATCH MANAGEMENT

H-99. Patch management encompasses the systematic process of updating software, drivers, and firmware on network devices. This practice addresses security vulnerabilities, resolves software issues, adds new

features, and ensures compliance with cybersecurity standards. Prioritizing patch management enhances security, improves system performance, and reduces risk of cyber incidents.

BEST PRACTICES

H-100. By adhering to patch management best practices, units can minimize vulnerabilities, strengthen security, and ensure the continued integrity of their network infrastructure. Best practices for patch management include—

- **Source verification**—administrators must obtain patches and updates exclusively from trusted sources. These include official vendor websites, the Defense Information Systems Agency, or authorized distribution channels like the patch quarterly disc.
- **Thorough testing**—before deploying patches or updates across the network, administrators must conduct rigorous testing in a controlled environment. Testing should verify that the patch does not introduce new issues or conflicts with existing software.
- **Performance validation**—after successful testing, administrators should have a designated system operator evaluate the performance of the patched system. This step ensures that the patch does not negatively affect system functionality or stability.
- **Baseline image update**—once a patch has been thoroughly tested and approved for deployment, administrators should update the unit's baseline image. This image serves as a template for configuring new devices or restoring existing devices to a known secure state.
- **Distribution strategy**—various tools and methods exist for automating and streamlining the patch deployment process. Administrators should select a patch distribution solution that aligns with their unit's specific environment and requirements.

PATCH MANAGEMENT STEPS

H-101. The steps in patch management are—

- Verifying Windows Server Update Service configuration.
- Configuring the System Center Configuration Manager server
- Setting up a test workstation.

Verifying Windows Server Update Service Configuration

H-102. The Windows Server Update Service server should point to the Defense Information Systems Agency update service server. The Windows Server Update Service server should come pre-configured and not require any adjustment.

Note. Patches pulled by the Windows Server Update Service server are designed to be distributed through the System Center Configuration Manager server and cannot be accessed manually.

Configuring the System Center Configuration Manager Server

H-103. The System Center Configuration Manager server is the preferred method to distribute patches across a domain. Patch distribution should be pre-scheduled. In a limited bandwidth environment, units should maintain an SOP for manually pulling and distributing system patches. A best practice is to conduct system patching outside periods of peak activity.

Setting Up a Test Workstation

H-104. Network administrators should designate one workstation per enclave as a test environment to verify new patches before deploying them across the network. This will allow network administrators to determine whether additional configuration changes are needed to maintain network functionality. If additional configuration changes are required, those instructions can be included as a part of the update to ensure patched systems work properly.

MANUAL PATCHING IN A BANDWIDTH-LIMITED ENVIRONMENT

H-105. If network bandwidth is insufficient to support using Windows Server Update Service and System Center Configuration Manager, network administrators will likely need to patch systems manually. This involves downloading patches individually from the Defense Information Systems Agency patch repository and copying those patches to a local shared drive for further distribution. This method requires administrators to apply patches system by system. This method is slower and labor intensive, but if properly managed it can be effective.

WINDOWS DEPLOYMENT SERVICE CONFIGURATION

H-106. Windows Deployment Service allows administrators to centrally manage and deploy standardized images to minimize the risk of rogue software installations. A Windows Deployment Service server allows a unit to centrally manage its image repositories, capture updated system images, and distribute them to subordinate units.

PRINTER ACCESS CONTROL

H-107. Administrators should establish access controls on network shared printers. Printer access control limits access to networked printers to a list of defined users. Implementing access control through password or common access card login prevents unauthorized access to printing functions. This prevents unauthorized users printing and removing sensitive documents to which they should not have access. Applying access controls to printers also prevents unauthorized network access via printer vulnerabilities.

DEFAULT PASSWORDS

H-108. A default password is a preconfigured password typically used for initial setup of a system. Many systems, including major communications assemblages and command and control information systems, come with default passwords and user and administrator accounts configured. Using default passwords on networked devices or consoles presents a significant network vulnerability. Army password standards require changing the passwords on routers and system consoles from the factory default. This includes changing from the default passwords provided by program managers during equipment fielding. Since default passwords are widely known, threats or the opposing force will try them first in their attempts to infiltrate the network. Administrators and users must change all default passwords on network and endpoint devices before connecting them to the network.

Appendix I

Army Integrated Reprogramming Cycle

As currently implemented, electromagnetic warfare reprogramming cannot be implemented within a tactically relevant timeframe. The Cyber Center of Excellence led a comprehensive doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy assessment to define a future state Army integrated reprogramming cycle. This appendix defines the future state reprogramming cycle.

OVERVIEW

I-1. The modern electromagnetic operational environment is more dynamic than ever. Rapid advances in communications and noncommunications technologies contribute to the pace of change. One of the newest challenges is the widespread employment of software-defined radios. Enemy electromagnetic warfare systems have also advanced, making the electromagnetic operational environment a challenging maneuver space where the commander must maintain situational understanding and be able to control electromagnetic signatures associated with command and control systems, radars, and EW systems.

I-2. Electromagnetic attack effects must include advanced techniques beyond brute-force jamming to increase survivability and lethality of Army personnel and systems. The increasingly capable threat throughout the electromagnetic operational environment requires a responsive EW reprogramming enterprise that supports tactical maneuver with software-defined emitter detection and effects delivery capabilities as close to combat speed as possible.

I-3. The future Army integrated reprogramming cycle is a modified version of the joint reprogramming cycle outlined in JP 3-85. The Army integrated reprogramming cycle reflects a consolidated Army electromagnetic countermeasures development and delivery process. Figure I-1 illustrates the Army integrated reprogramming cycle for the development of electromagnetic countermeasures.

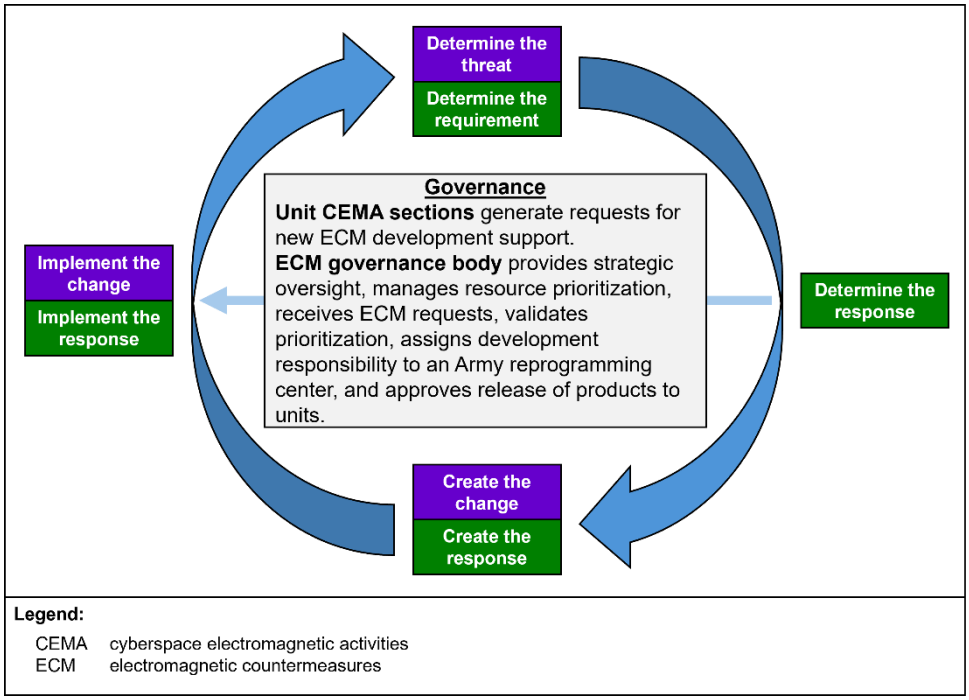


Figure I-1. Army integrated reprogramming cycle

PHASES

I-4. The Army integrated reprogramming cycle follows the process in JP 3-85, with minor adjustments to support imitative, manipulative, or simulative electromagnetic attack. The purple cycle phases identified in Figure I-1 are the joint naming convention and the green phases are the naming convention used to support the Army electromagnetic warfare reprogramming enterprise. The Army integrated reprogramming cycle aligns electromagnetic countermeasures development as a subprocess within the scope of EW reprogramming, eliminating the need for new policies and allowing development to occur within existing EW reprogramming authorities.

I-5. The Army integrated reprogramming cycle consists of four phases:

- Determine the requirement.
- Determine the response.
- Create the response.
- Implement the response.

DETERMINE THE REQUIREMENT

I-6. Staffs develop and maintain an accurate description of the operational environment, specifically threat systems and tactics, techniques, and procedures through intelligence preparation of the operational environment. Maintaining an accurate description of the environment requires the fusion of known electromagnetic data with the collection, analysis, and validation of threat signature changes.

I-7. Intelligence preparation of the operational environment (see chapter 4) is a collaborative staff effort led by the intelligence staff. The staff continually updates intelligence preparation of the operational environment products (including the electromagnetic order of battle) to support situational understanding and assist commanders and staff in identifying relevant aspects within their assigned area or area of interest, such as threat signals of interest that can affect mission accomplishment. The commander and staff's understanding of intelligence preparation of the operational environment and the electromagnetic order of battle help in developing high-payoff and high-value targets. Defining the electromagnetic order of battle requires—

- Identifying transmitters and receivers in an area of interest.
- Determining their geographic locations or range of mobility.
- Characterizing their signals.
- Determining their roles in the threat's broader organizational order of battle where possible.

I-8. Threat use of software-defined radios and agile electromagnetic attack capabilities require continual updates to the electromagnetic order of battle. When EW and SIGINT teams detect unidentified signals in their assigned areas, those signals require analysis to identify their characteristics. This contributes to a current, accurate electromagnetic order of battle and allows EW personnel to identify requirements for new or updated electromagnetic countermeasures.

DETERMINE THE RESPONSE

I-9. Once commanders and staff understand the situation and mission, they develop courses of action to generate response options that will drive the production of operation plans or orders. The CEMA section generates cyberspace and EW options to support proposed courses of action. If the CEMA section determines an existing electromagnetic countermeasure is not sufficient or a new countermeasure is needed, they perform additional analysis to determine whether a proposed new countermeasure will provide the emitter detection or effects delivery capability necessary to achieve the commander's objectives for a given target or set of targets.

I-10. CEMA staff at echelon using the Electromagnetic Warfare Planning and Management Tool will review the electromagnetic countermeasures arsenal to determine whether an electromagnetic countermeasure has been developed for a target and that the electromagnetic attack system it was developed for meets their operational requirement. If no countermeasure is available, the CEMA staff submits an operational change request (see appendix E) to request development of an electromagnetic countermeasure to support their fielded EW system and establish the priority (routine, urgent, or emergency) of the request. CEMA sections

forward the operational change request through their chain of command to the theater army CEMA section for approval and processing.

CREATE THE RESPONSE

I-11. The create the response phase consists of—

- Developing and testing an electromagnetic countermeasure.
- Cataloging the countermeasure and placing it within the electromagnetic countermeasures arsenal for use by EW community.

I-12. The electromagnetic countermeasures arsenal provides detailed information on electromagnetic countermeasure techniques, EW systems, and threat signal characteristics to support modeling and simulation, mission planning, and course of action development. The electromagnetic countermeasures arsenal also provides the capability to store and deliver electromagnetic countermeasures to fielded EW systems via the Electromagnetic Warfare Planning and Management Tool.

I-13. Electromagnetic countermeasure developers must determine whether enough threat system data is available to develop a countermeasure. The signal of interest can be complex and may require reverse engineering to determine whether an effective electromagnetic countermeasure can be developed to affect the target.

I-14. The electromagnetic countermeasure developer will conduct a vulnerability assessment that consists of—

- Signal analysis.
- Reverse engineering.
- Protocol and specification review.

I-15. Once developers discover a vulnerability to the threat system, they develop an electromagnetic countermeasure to exploit the vulnerability. If the vulnerability assessment fails to expose an obvious weakness, an electromagnetic countermeasure may still be created through experimentation or trial and error. By leveraging previously developed electromagnetic countermeasures known to be effective against similar signals of interest, a baseline capability can be quickly established and modified to tailor the countermeasure to the target in question. Developers can then evaluate tactics, techniques, and procedures for deploying these countermeasures through physical testing, modeling, and simulations and predict combat effectiveness against the threat system.

I-16. Depending on the urgency of the request, developers may not have enough time to generate a carefully tailored countermeasure for the threat capability. In these cases, they may opt to quickly develop an interim capability or tactics, techniques, and procedures to detect the signal of interest and deliver a brute force effect while continuing to develop and refine a more advanced technique.

I-17. The developer tests the electromagnetic countermeasure at a test range to validate tactics, techniques, and procedures, combat effectiveness, and required safety certification for employment. When testing and validating new countermeasures, tactics, techniques, and procedures, developers must consider the risk tolerance of the mission—

- Electromagnetic protection and defensive electromagnetic attack techniques carry a low risk tolerance for mission failure. Systems that protect personnel and equipment require stringent testing and evaluation processes.
- Electromagnetic attack techniques allow a higher level of accepted risk. Systems designed to deny, disrupt, or destroy threat systems may not require extended testing and evaluation before employment.
- Advanced electromagnetic attack techniques (electromagnetic deception, electromagnetic intrusion, electromagnetic manipulation, or electromagnetic spectrum-enabled cyberspace attack) require extensive testing and evaluation to predict their combat effectiveness.

I-18. Once a countermeasure is approved, the electromagnetic countermeasure file and tactics, techniques, and procedures for employment are packaged and placed in the electromagnetic countermeasures arsenal. A reprogramming message is then sent to all theater CEMA staff.

IMPLEMENT THE RESPONSE

I-19. Upon receipt of the reprogramming message, the CEMA staff will download the electromagnetic countermeasure file and supporting products to complete the mission. The CEMA sections determine the need for a countermeasure and review the electromagnetic countermeasures arsenal. The CEMA section, using an EW planning tool like Electromagnetic Warfare Planning and Management Tool, downloads a countermeasure file with supporting tactics, techniques, and procedures. The CEMA section verifies the new electromagnetic countermeasure effect can be employed withing their delegated electromagnetic attack control authority.

I-20. The CEMA section disseminates files and associated tactics, techniques, and procedures to the EW team with the mission task. The team installs the file and adjusts the systems for executing the mission. The CEMA section then submits a unit loading message (see appendix E) to document implementation of the reprogramming action.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
AR	Army regulation
ARCYBER	United States Army Cyber Command
ATP	Army techniques publication
CECOM	United States Army Communications-Electronics Command
CEMA	cyberspace electromagnetic activities
CERF	cyber effects request format
CEWO	cyber electromagnetic warfare officer
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
DA	Department of the Army
DAI	Dynamic Address Resolution Protocol Inspection
DODI	Department of Defense instruction
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network-Army
EMCON	emission control
EW	electromagnetic warfare
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-39	assistant chief of staff, information plans and operations
G-6	assistant chief of staff, signal
HF	high frequency
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-6	communications, computers, and cyberspace directorate of a joint staff
JP	joint publication
METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations
MIJIFEEDER	meaconing, intrusion, jamming, and interference feeder
NETCOM	United States Army Network Enterprise Technology Command
NIST SP	National Institute of Standards and Technology special publication

INSCOM	United States Army Intelligence and Security Command
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
SIGINT	signals intelligence
SOP	standard operating procedure
TC	training circular
VHF	very high frequency
USCYBERCOM	United States Cyber Command
UHF	ultrahigh frequency

SECTION II – TERMS

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

ARFOR

(Army) The Army component and senior Army headquarters of all Army forces assigned or attached to a combatant command, subordinate joint force command, joint functional command, or multinational command. (FM 3-94)

assessment

Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (JP 3-0)

combat information

A report that is gathered by or provided to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence before being used to support decision making. (FM 2-0)

combined arms

The synchronized and simultaneous application of arms to achieve an effect greater than if each element was used separately or sequentially. (ADP 3-0)

commander's critical information requirement

Specific information identified by the commander as being essential to facilitate timely decision making. (JP 3-0)

convergence

An outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area. (FM 3-0)

crisis

An emerging incident or situation involving a possible threat to the United States, its citizens, military forces, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, or military importance that commitment of military forces and resources is contemplated to achieve national and/or strategic objectives. (JP 3-0)

cyberspace attack

Actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires. (JP 3-12)

cyberspace defense

Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures. (JP 3-12)

cyberspace domain

(Army) The interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum. (FM 3-0)

*** cyberspace electromagnetic activities**

The planning, integration, and synchronization of cyberspace and electromagnetic warfare operations as part of a combined arms approach through the operations process. **Also called CEMA.**

defensive cyberspace operations

Missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity. (JP 3-12)

defensive cyberspace operations-internal defensive measures

A defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace. (JP 3-12)

defensive cyberspace operations-response actions

A defensive cyberspace operations mission executed external to the defended network or portion of cyberspace without the permission of the owner of the affected system. (JP 3-12)

delay

When a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on enemy forces without becoming decisively engaged. (ADP 3-90)

Department of Defense information network

The set of information capabilities and associated processes owned or leased by the Department of Defense for collecting, processing, storing, disseminating, and managing information, whether interconnected or stand-alone. **Also called DODIN.** (JP 6-0)

Department of Defense information network-Army

An Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide. **Also called DODIN-A.** (ATP 6-02.71)

destroy

A tactical mission task that physically renders an enemy force combat ineffective until it is reconstituted. (FM 3-90)

disintegrate

To disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations. (ADP 3-0)

disrupt

A tactical mission task in which a unit upsets an enemy's formation or tempo and causes the enemy force to attack prematurely or in a piecemeal fashion. (FM 3-90)

electromagnetic attack

Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-85).

electromagnetic compatibility

The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. (JP 3-85)

electromagnetic hardening

Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (JP 3-85)

electromagnetic interference

Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (JP 3-85)

electromagnetic intrusion

The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (JP 3-85)

electromagnetic jamming

The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-85)

electromagnetic masking

The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

electromagnetic probing

Intentional radiation designed to be introduced into the devices or systems of an adversary for the purpose of learning the functions and operational capabilities of the devices or systems. (JP 3-85)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

electromagnetic pulse

A strong burst of electromagnetic radiation caused by a nuclear explosion, energy weapon, or by natural phenomenon, that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 3-85)

electromagnetic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 3-85)

electromagnetic support

Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 3-85)

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. **Also called EW.** (JP 3-85)

electromagnetic warfare reprogramming

The deliberate alteration or modification of electromagnetic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. (JP 3-85)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. **Also called EMCON.** (JP 3-85)

enemy

A party identified as hostile against which the use of force is authorized. (ADP 3-0)

essential element of friendly information

A critical aspect of a friendly operation that, if known by a threat, would subsequently compromise, lead to failure, or limit success of the operation and therefore should be protected from enemy detection. (ADP 5-0)

execution

The act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation. (ADP 5-0)

exfiltration

The unauthorized transfer of information from a system. (NIST SP 800-53)

fix

A tactical mission task in which a unit prevents the enemy from moving from a specific location for a specific period. (FM 3-90)

force projection

The ability to project the military instrument of national power from the United States or another theater in response to requirements for military operations. (JP 3-0)

friendly force information requirement

Information the commander and staff need to understand the status of friendly force and supporting capabilities. (JP 3-0)

guarded frequencies

A list of time-oriented, enemy frequencies that are currently being exploited for combat information and intelligence or jammed after the commander has weighed the potential operational gain against the loss of the technical information. (JP 3-85)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects. (TC 7-100)

information activity

A collection of tasks linked by purpose to affect how humans and automated systems derive meaning from, use, and act upon, or are influenced by, information. (ADP 3-13)

information advantage

A condition when a force holds the initiative in terms of situational understanding, decision making, and relevant actor behavior. (ADP 3-13)

information collection

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations. (FM 3-55)

informational considerations

Those aspects of the human, information, and physical dimensions that affect how humans and automated systems derive meaning from, use, act upon, and are impacted by information. (FM 3-0)

insider threat

A threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the department; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace. (AR 381-12)

intelligence preparation of the operational environment

The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (FM 2-0)

interdict

A tactical mission task where a unit prevents, disrupts, or delays the enemy's use of an area or route in any domain. (FM 3-90)

joint restricted frequency list

A time and geographically oriented listing of TABOO, protected, and guarded functions, nets, and frequencies and limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. (JP 3-85)

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

multidomain operations

The combined arms employment of joint and Army capabilities to create and exploit relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders. (FM 3-0)

network enterprise center

The facility that provides and acquires telecommunications and information management services on Army installations. (ATP 6-02.71)

neutralize

A tactical mission task in which a unit renders the enemy incapable of interfering with an operation. (FM 3-90)

offensive cyberspace operations

Missions intended to project power in and through cyberspace. (JP 3-12)

operational environment

The aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operations process

The major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. (ADP 5-0)

priority intelligence requirement

The intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support. (JP 2-0)

protected frequencies

Friendly, generally time-oriented, frequencies used for a particular operation, identified and protected to prevent them from being inadvertently jammed by friendly forces while active electromagnetic warfare operations are directed against hostile forces. (JP 3-85)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

security area

That area occupied by a unit's security elements and includes the areas of influence of those security elements. (ADP 3-90)

setting the theater

The broad range of activities continuously conducted to establish conditions for the successful execution of operations in a theater. (FM 3-0)

suppress

A tactical mission task in which a unit temporarily degrades a force or weapon system from accomplishing its mission. (FM 3-90)

synchronization

The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 2-0)

system

A functionally, physically and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole. (JP 3-0)

TABOO frequencies

Any friendly frequency of such importance that it must never be deliberately jammed or interfered with by friendly forces including international distress, safety, and controller frequencies. (JP 3-85)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

threat warning

The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 2-0)

wartime reserve modes

Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to, or misunderstood by, opposing commanders before they are used but could be exploited or neutralized if known in advance. (JP 3-85)

This page intentionally left blank.

References

All URLs were last accessed on 5 September 2025.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. August 2025.

FM 1-02.1. *Operational Terms*. 28 February 2024.

FM 1-02.2. *Military Symbols*. 23 January 2025.

RELATED PUBLICATIONS

These documents are cited in this publication.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/doctrine.

Chairman of the Joint Chiefs of Staff issuances are available online: https://www.jcs.mil/library/.

DOD issuances are available online: https://www.esd.whs.mil/dd/dod-issuances/.

CJCSI 6510.01F. *Information Assurance (IA) and Support to Computer Network Defense (CND)*. 9 February 2011.

CJSCM 3320.01D. *Joint Electromagnetic Spectrum Operations*. 24 January 2025.

CJCSM 6510.01B. *Cyber Incident Handling Program*. 10 July 2012.

DODI 8530.01. *Cybersecurity Activities Support to DoD Information Network Operations*. 7 March 2016.

DODI 8530.03. *Cyber Incident Response*. 9 August 2023.

JP 2-0. *Joint Intelligence*. 26 May 2022.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-04. *Information in Joint Operations*. 14 September 2022.

JP 3-12. *Joint Cyberspace Operations*. 19 December 2022.

JP 3-22. *Foreign Internal Defense*. 17 August 2018.

JP 3-55. *Joint Operations Security*. 20 February 2025.

JP 3-57. *Joint Civil-Military Operations*. 2 April 2025.

JP 3-60. *Joint Targeting*. 20 September 2024.

JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.

JP 5-0. *Joint Planning*. 1 July 2025.

JP 6-0. *Joint Communications*. 4 December 2023.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 3-0. *Operations*. 21 March 2025.

ADP 3-13. *Information*. 27 November 2023.

ADP 3-37. *Protection*. 10 January 2024.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

AR 380-5. *Army Information Security Program*. 25 March 2022.

AR 381-12. *Counterintelligence Awareness and Reporting*. 13 June 2025.

AR 525-24. *U.S. Army Cyberspace and Electromagnetic Warfare Operations*. 12 July 2023.

ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5/STTP 3-9002. Multi-Service Tactics, Techniques, and Procedures for Multi-Service Brevity Codes. 25 April 2025.

ATP 2-01. (U) *Collection Management*. 17 August 2021.

ATP 2-01.3. *Intelligence Preparation of the Operational Environment*. 1 March 2019.

ATP 2-22.6. (U) *Signals Intelligence*. 9 January 2024.

ATP 2-33.4. *Intelligence Analysis*. 10 January 2020.

ATP 3-04.1. *Aviation Tactical Employment*. 7 May 2020.

ATP 3-05.2. *Foreign Internal Defense*. 19 August 2015.

ATP 3-09.32/MCRP 3-31.6/NTTP 3-09.2/AFTTP 3-2.6. *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower*. 29 November 2023.

ATP 3-12.3. *Electromagnetic Warfare Techniques*. 30 January 2023.

ATP 3-12.4. *Electromagnetic Warfare Platoon*. 9 January 2023.

ATP 3-21.20. *Infantry Battalion*. 28 December 2017.

ATP 3-60.1/MCRP 3-31.5/NTTP 3-60.1/AFTTP 3-2.3/STTP 3-9001. *Multi-Service Tactics, Techniques and Procedures for Dynamic Targeting*. 28 March 2025.

ATP 3-72/MCRP 10-10E.9/NTTP 3-72.1/AFTTP 3-2.65. *(U) Operations in a Nuclear Environment*. 7 March 2022.

ATP 5-0.1. *Army Design Methodology*. 1 July 2015.

ATP 5-0.3/MCRP 5-10.1/NTTP 5-01.3/AFTTP 3-2.87. *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment*. 7 February 2020.

ATP 6-01.1. *Knowledge Management*. 11 March 2024.

ATP 6-02.53. *Techniques for Tactical Radios and Retransmission*. 31 July 2025.

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 16 October 2019.

ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 14 August 2025.

ATP 6-02.75. *Techniques for Communications Security*. 18 May 2020.

FM 2-0. *Intelligence*. 1 October 2023.

FM 3-0. *Operations*. 21 March 2025.

FM 3-11. *Chemical, Biological, Radiological, and Nuclear Operations*. 10 April 2025.

FM 3-14. *Army Space Operations*. 30 October 2019.

FM 3-16. *The Army in Multinational Operations*. 15 July 2024.

FM 3-53. *Military Information Support Operations*. 4 January 2013.

FM 3-55. *Information Collection*. 3 May 2013.

FM 3-57. *Civil Affairs Operations*. 28 July 2021.

FM 3-84. *Legal Support to Operations*. 1 September 2023.

FM 3-90. *Tactics*. 1 May 2023.

FM 3-94. *Armies, Corps, and Division Operations*. 23 July 2021.

FM 4-0. *Sustainment Operations*. 14 August 2024.

FM 5-0. *Planning and Orders Production*. 4 November 2024.

FM 6-0. *Commander and Staff Organization and Operations*. 16 May 2022.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

FM 7-0. *Training*. 14 June 2021.

TC 3-12.2.4.1. *Analytic Support to Defensive Cyberspace Operations*. 17 January 2024.

TC 3-12.2.90. *Mission Thread Defense*. 5 February 2024.

TC 3-12.2.98. *Hunt Operations*. 2 February 2024.

TC 7-100. *Hybrid Threat*. 26 November 2010.

TC 7-100.2. *Opposing Force Tactics.* 9 December 2011.

OTHER PUBLICATIONS

National Institute of Standards and Technology (NIST) special publications are available at: https://www.nist.gov/publications.

Most acts and public laws are available at https://uscode.house.gov/.

NIST SP 800-53r5. *Security and Privacy Controls for Information and Systems*. September 2020.

NIST SP 800-61r3. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*. April 2025.

Title 10, United States Code. *Armed Forces*.

Title 32, United States Code. *National Guard*.

Title 44, United States Code. *Public Printing and Documents*. Section 3552. *Definitions*.

Title 50, United States Code. *War and National Defense; and Appendix*.

WEBSITES

Cyber Lessons and Best Practices Website. https://cybercoelessonslearned.army.mil. (Requires DOD-approved certificate login).

Department of Defense Patch Repository Website (Defense Asset Distribution System [DADS]). https://patches.csd.disa.mil. (Requires DOD-approved certificate login.).

Office of Management and Budget Memorandum M-23-03, Fiscal Year 2023. *Guidance on Federal Information Security and Privacy Management Requirements*. https://www.fpc.gov/resources/omb/.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, Department of the Army Forms are on the Army Publishing Directorate Website: https://armypubs.army.mil.

Department of Defense forms are available online. https://www.esd.whs.mil/directives/forms/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DD Form 1972. *Joint Tactical Airstrike Request.*

RECOMMENDED READINGS

These documents contain relevant supplemental information.

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 1-01. *Doctrine Primer*. 31 July 2019.

This page intentionally left blank.

Index

Entries are by paragraph number.

A

A2/AD. *See* antiaccess and area denial

ACAS. *See* Assured Compliance Assessment Solution

advantages
  human. 5-73, 5-109
  information. 1-11, 5-72, 5-108
  physical. 5-71, 5-105
  relative. 1-10, 5-70

AIWOC. *See* Army Information Warfare Operations Center

antiaccess and area denial. 5-115

ARAT-PO. *See* Army Reprogramming Analysis Team Program Office

ARCYBER. *See* United States Army Cyber Command

armed conflict. 1-32, 5-99

Army Information Warfare Operations Center. F-36

Army National Guard. F-19

Army Reprogramming Analysis Team Program Office. F-48

assessment. B-87

Assured Compliance Assessment Solution. H-87

B

brigade. 5-93, 5-146

C

camouflage net masking. 3-46

CEMA. *See* cyberspace electromagnetic activities

CERF. *See* cyber effects request format

change control board. H-30

CISA. *See* Cybersecurity and Infrastructure Security Agency

CISCO Security Manager. H-36

close operations. 5-134

CMF. *See* Cyber Mission Force

collection management. 4-69

combat information. 4-74

combat training centers. G-11

combatant command. 5-30

combined arms. 1-6

competition. 1-29, 5-28
  activities. 5-44

consolidation of gains. 5-56, 5-94

convergence. 5-2

corps. 5-91, 5-142

counterreconnaissance. 5-21

CPB. *See* cyber protection brigade

crisis. 1-30, 5-59
  roles. 5-88

CTC. *See* combat training centers

cyber battalion. F-44

Cyber Combat Mission Force. F-26

cyber effects request format. C-22

cyber events. A-48
  categories. A-50

cyber incident
  analysis. A-9, A-18, A-45
  major. A-53
  recovery. A-29
  reporting. A-7, A-21
  response. A-11, A-24

cyber incident handling. A-1

cyber incidents. A-48

Cyber Mission Force. F-25

Cyber National Mission Force. F-29

cyber protection brigade. F-43

Cyber Protection Force. F-28

Cyber Threat Intelligence Center. A-67

cybersecurity. 5-18, H-1

Cybersecurity and Infrastructure Security Agency. A-69

cyberspace attack. 2-27

cyberspace defense. 2-7
  missions and functions. 2-16

cyberspace domain. 1-62

cyberspace electromagnetic activities. 4-1
  roles. 4-5

cyberspace exploitation. 2-24

cyberspace offense. 2-20

cyberspace security. 5-17

cyberspace surveillance and reconnaissance. 2-23

D

data exfiltration, 159

DCDC. *See* DOD Cyber Defense Command, *See* Defense Information Systems Agency

DCO. *See* defensive cyberspace operations

deep operations. 5-131

default passwords. H-108

defense. 5-119

Defense Information Systems Agency. F-31

Defense Intelligence Agency. F-10

defensive cyberspace operations. 2-8, 5-19
  internal defensive measures. 2-11, 5-112
  response actions. 2-15, 5-113
  support requests. C-13

denial-of-service. D-52

Department of Defense Cyber Crime Center. A-65

Entries are by paragraph number.

Department of Defense information network. 2-2
Department of Defense information network-Army. 2-4
Department of Defense organizations. F-4
Department of Homeland Security. F-3
Department of Justice. F-2
deployment. 5-78
deployment, contested. 1-37, 5-75
DHS. *See* Department of Homeland Security
DIA. *See* Defense Intelligence Agency
direction finding. 3-55
DISA. *See* Defense Information Systems Agency
division. 5-92, 5-144
DOD Cyber Defense Command. A-62
DODIN. *See* Department of Defense information network
DODIN-A. *See* Department of Defense information network-Army
DOJ. *See* Department of Justice

E

EA. *See* electromagnetic attack
EARF. *See* electromagnetic attack request format
early entry. 1-38
effects. 4-94
  cyberspace. 4-59
  electromagnetic spectrum. 4-59
effects requests
  cyberspace. C-10
  electromagnetic attack. C-1
electromagnetic attack. 3-3, 5-4
electromagnetic attack request format. C-6
electromagnetic compatibility. 1-140
electromagnetic countermeasures. 3-5
electromagnetic deception. 3-6
electromagnetic environmental effects. 1-138
electromagnetic hardening. 3-47
electromagnetic interference. 1-141
electromagnetic intrusion. 3-14
electromagnetic jamming. 3-15
electromagnetic masking. 3-44
electromagnetic protection. 3-37, 5-20
electromagnetic radiation hazards. 1-145
electromagnetic reconnaissance. 3-53
electromagnetic spectrum. 1-66
electromagnetic support. 3-49, 5-15
electromagnetic warfare. 3-1
electromagnetic warfare forces. 3-73
  brigade. 3-76
  division. 3-74
electromagnetic warfare reprogramming. 3-57
EMCON. *See* emission control
EMI. *See* electromagnetic interference
emission control. 3-38, 4-33
EMS. *See* electromagnetic spectrum
enabling operations. 5-9
Enterprise Security Manager. H-66
EP. *See* electromagnetic protection
ES. *See* electromagnetic support
ESM. *See* Enterprise Security Manager
EW. *See* electromagnetic warfare
extended deep operations. 5-132

F

force projection. 5-75
force protection. 5-45
fort to port. 5-82
frequency deconfliction. 4-51

H

hazards. 1-137
  atmospheric weather. 1-153
  electromagnetic pulse. 1-143
  space weather. 1-149
HBSS. *See* Host Based Security System
Host Based Security System. H-83
humanitarian assistance. 5-55
hunt operations. 2-19, 5-12

I

information activities
  attack. 1-25
  enable. 1-14
  influence. 1-24
  inform. 1-23
  protect. 1-19
information collection. 4-67
information warfare. 1-124
integrating processes. 4-62
intelligence preparation of the operational environment. 4-63, B-6
intelligence, support to. 4-53
IPOE. *See* intelligence preparation of the operational environment

J

jamming. *See* electromagnetic jamming, D-17
joint forcible entry. 5-116
joint integration. 4-101, 5-74
  cyberspace operations. 4-102
  electromagnetic spectrum. 4-103
  targeting. 4-103
joint planning. 4-108
joint spectrum interference resolution. D-41
joint tactical airstrike request. C-3
JSIR. *See* joint spectrum interference resolution

K

knowledge management. 4-99

L

logs and alerts. H-64

M

main battle area. 5-125
malware. D-57
MDEB. *See* multi-domain effects battalion

Entries are by paragraph number.

MDMP. *See* military decision-making process
MDO. *See* multidomain operations
MDTF. *See* multi-domain task force
message formats
  electromagnetic warfare. E-1
  electromagnetic warfare reprogramming. E-6
military decision-making process. 4-32, B-1
  step 1—receipt of mission. B-8
  step 2—mission analysis. B-11
  step 3—course of action development. B-27
  step 4—course of action analysis. B-42
  step 5—course of action comparison. B-48
  step 6—course of action approval. B-52
  step 7—orders production. B-55
mission thread defense. 2-18
mobilization. 5-77
multi-domain effects battalion. F-46
multidomain operations. 1-5
multi-domain task force. 5-36, F-45

N

National Cyber Investigative Joint Task Force. A-68
National Geospatial-Intelligence Agency. F-14
National Guard Bureau. F-17
National Security Agency. A-66, F-7
NEC. See network enterprise center
Nessus Scanner. H-90
NETCOM. *See* United States Army Network Enterprise Technology Command
network enterprise center. F-40
network hardening. H-1
  device configuration. H-41
  file server resource manager. H-10
  folder redirection. H-21
  group policy. H-16
  layer 2 security. H-42
  organizational unit. H-2
  print servers. H-15
  read-only domain controller. H-22
  security access. H-6
  shared drives. H-14
  test environment. H-28
network monitoring. H-56
NGIA. *See* National Geospatial-Intelligence Agency
NSA. *See* National Security Agency
nuclear deterrence. 5-53

O

offense. 5-128
operation order. B-58
operation plan. B-58
operational environment. 1-57
  congested. 1-40
  contested. 1-43
operational framework. 5-130
operations process. 4-18
  assessment. 4-57
  execution. 4-48
  planning. 4-20
  preparation. 4-46
operations security. 5-67
operations, close. 5-124
operations, deep. 5-121
operations, rear. 5-135
operations, rear. 5-127
OPLAN. *See* operation plan
OPORD. *See* operation order
OPSEC. *See* operations security
organizations, national. F-1

P

patch management. H-99
personal electronic devices. D-85
phishing. D-74
protection. 4-60

R

RCC. See regional cyber center
reception, staging, onward movement, and integration. 5-85
reconnaissance. 5-10
regional cyber center. F-39
relative advantages. 5-103
reprogramming. I-1
reprogramming cycle. I-4
Reserve Components. F-16
risk management. 4-97
RSOI. *See* reception, staging, onward movement, and integration
running estimate. B-2

S

sanctuary. 1-115
security area. 5-126
security assistance. 5-48
Security Center. H-90
security cooperation. 5-46
Security Onion. H-81
security operations. 5-16
security, endpoint. H-82
setting the theater. 1-34, 5-29
SIGINT. *See* signals intelligence
signals intelligence. 3-63
social engineering. D-67
SolarWinds. H-31
systems analysis. 1-154
  output. 1-167
  process. 1-157
systems warfare. 1-117

T

targeting. 4-77
  deliberate. 4-91
  dynamic. 4-92
  guidance. 4-78
  joint. 4-113
  process. 4-84
  restrictions. 4-87
targeting coordination board. B-83
terrain masking. 3-45
theater army. 5-33, 5-90, 5-140
threat. 1-72
  activities. 1-73
    cyberspace. 1-75
    electromagnetic spectrum. 1-88
  hybrid. 1-119
  insider. 1-134
  non-state. 1-131
  peer. 1-95
    tactics. 1-114
  state. 1-92
    China. 1-99

Entries are by paragraph number.

Iran. 1-107
North Korea. 1-111
Russia. 1-103
threat warning. 3-54
threat, persistent. 1-33
training
classroom. G-6
field training exercise. G-10
home station. G-5
institutional. G-3
lane. G-9
transitions. 5-58, 5-95, 5-137

U

United States Army Cyber Command. A-64, F-35
United States Army Network Enterprise Technology Command. F-38
United States Army Reserve. F-21
United States Cyber Command. A-63, F-22
USCYBERCOM. *See* United States Cyber Command,

See United States Cyber Command

W

wartime reserve modes. 3-48
working groups. 4-40, B-72
assessment. B-87
cyberspace electromagnetic activities. 4-42
information collection. B-73
protection. B-85
targeting. B-79

FM 3-12

17 September 2025

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:



MATTHEW L. SANNITO
Administrative Assistant
to the Secretary of the Army
2525310

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.



PIN: 201561-000